# *Understanding the Individual Level and Macro Level Causes of Economic Cybercrime Victimisation in the UK: A Contextual Vulnerabilities Approach to Examine Cybercrime Victimisation*

NACI AKDEMIR

# Understanding the Individual Level and Macro Level Causes of Economic Cybercrime Victimisation in the UK: A Contextual Vulnerabilities Approach to Examine Cybercrime Victimisation

**(Volume I and II)**

**Naci AKDEMIR**

A thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy


Department of Sociology

Durham University

2019

**Understanding the Individual Level and Macro Level Causes of Economic Cybercrime Victimisation in the UK: A Contextual Vulnerabilities Approach to Examine Cybercrime Victimisation**

Naci Akdemir

## Abstract

This thesis applying a mixed methods research paradigm discerns the individual and macro level factors facilitating economic cybercrime victimisation in the UK. Understanding and exploring the adverse impacts of economic cybercrime victimisation on victims' online lifestyles, psychological well-being and protection motivation are other goals of this research. To these ends, semi-structured interviews were conducted with thirty-two victims of economic cybercrime, ten non-victim control group participants and ten cybercrime experts.

The extant cybercrime victimisation studies utilised Lifestyle Routine Activities Theory (LRAT), the latest version of the Opportunity Theories of the Victimisation Perspective, as a theoretical framework. However, the applicability of LRAT to cybercrime research is questionable (Yar, 2005) since the theory was originally proposed to explain traditional crime victimisation occurring in the physical world. This thesis critically evaluates the transposition of key LRAT concepts to cybercrime research and proposes The Contextual Vulnerabilities Approach to better understand the causes of economic cybercrime victimisation.

Protection Motivation Theory (PMT) and Approach-Avoidance Paradigm were also utilised as a conceptual framework while examining the adverse impacts of victimisation experiences on Internet users' behavioural adaptation and security intentions. The Integrated Cyber Victimisation Model (ICVM) was built based on the empirical findings of this thesis to examine cybercrime victimisation holistically and understand the adverse consequences of victimisation.

Past cybercrime victimisation research utilising LRAT as a theoretical framework explicitly put the onus of the victimisation on victims' shoulders. The findings of this thesis suggest that most victims faced economic cybercrime victimisation due to the congruence of the contextual factors that are beyond their controls. Technological vulnerabilities and data breaches of large companies holding personal information of the Internet users are macro vulnerabilities identified. Fear of crime, perceived severity, perceived vulnerability and self-efficacy emerged as the cognitive factors affecting Internet users' protection motivation and behavioural adaptation.

**Table of Contents**

Abstract ..... ii

Table of Contents ..... iii

List of Tables ..... xv

List of Figures ..... xviii

Declaration ..... xx

Statement of Copyright ..... xx

Acknowledgements ..... xxi

Chapter 1 Introduction ..... 1

1.1 Introduction ..... 1

1.1.1 Definition of Cybercrime ..... 3

1.1.2 Three Generations of Cybercrime ..... 6

1.1.3 Typology of Cybercrime ..... 8

1.2 Economic Cybercrime ..... 9

1.2.1 Card-not-present Fraud ..... 11

1.2.2 Online Banking Fraud ..... 12

1.2.3 Identity Fraud ..... 14

1.3 Modus Operandi of Online Perpetrators ..... 15

1.3.1 Phishing ..... 15

1.3.2 Hacking ..... 17

1.3.3 Malware Infection....18
1.4 Synopsis of Cybercrime Victimisation Literature....19
1.4.1 Development of Victimology....19
1.4.2 Shared Responsibility....21
1.4.3 Victimhood....22
1.4.4 Opportunity Theories of Victimisation....25
1.4.5 Correlates of Cybercrime Victimisation....26
1.4.5.1 Online Activities....27
1.4.5.2 Demographics of Internet Users....29
1.4.6 Consequences of Cybercrime Victimisation....29
1.4.6.1 Emotional Reactions....30
1.4.6.2 Behavioural Responses....32
1.5 Research Aims, Objectives and Research Questions....32
1.6 Key Contributions and Implications....35
1.7 Engaging with Cybercrime and Cyber Victimology....37
1.8 The structure of the Thesis....38
Chapter 2 Theoretical Framework....42
2.1 Introduction....42
2.2 Opportunity Theories of Victimisation....43
2.2.1 Lifestyle Exposure Theory....44
2.2.2 Routine Activities Theory....45

2.2.3 The Opportunity Model of Predatory Victimisation ..... 46
2.2.4 Structural-Choice Theory of Victimisation (LRAT) ..... 48
2.2.5 Assessment of Theoretical Evolution of LRAT ..... 49
2.2.5.1 Transformation of Conceptual Elements of LRAT ..... 50
2.2.6 Critique of Opportunity Theories of Victimisation ..... 53
2.3 Application of LRAT to Cybercrime Studies ..... 54
2.3.1 Operationalisation of LRAT concepts in Cybercrime Studies ..... 56
2.3.2 Conceptual Pitfalls of Transposing LRAT Elements to Cyber Space ..... 61
2.3.2.1 The Distinction between Proximity and Exposure to Motivated Offender ..... 61
2.3.2.2 Target Suitability and Target Attractiveness ..... 62
2.3.2.3 Spacio-temporality of the Events ..... 64
2.4 Protection Motivation Theory ..... 67
2.5 Approach and Avoidance Coping Paradigm ..... 72
2.6 Summary ..... 75
Chapter 3 Cybercrime Victimisation ..... 77
3.1 Introduction ..... 77
3.2 Correlates of Cybercrime Victimisation ..... 77
3.2.1 Exposure and Proximity to Motivated Offender ..... 78
3.2.2 Target Suitability and Target Attractiveness ..... 79
2.2.3 Absence of a Capable Guardian ..... 83
2.3.3.1 Computer Integrity Crimes ..... 84

2.3.3.2 Computer Content Crimes....85
2.3.3.3 Computer Assisted Crimes....85
3.3 Precursors of Economic Cybercrime Victimisation....87
3.3.1 Phishing....87
3.3.1.1 Email Phishing....88
3.3.1.2 Website Phishing....93
3.3.2 Malware Infection....94
3.3.3 Hacking....95
3.4 Economic Cybercrime Victimisation....97
3.4.1 Card-not-present Fraud....97
3.4.2 Online Banking Fraud....98
3.4.3 Online Identity Fraud....99
3.5 Emotional and Behavioural Responses to Victimisation Experiences....102
3.5.1 Fear of Crime....103
3.5.1.1 Fear of Crime versus Concern....104
3.5.1.2 Fear of Crime versus Perceived Risk of Victimisation....104
3.5.1.3 Fear of Crime versus Anxiety....105
3.5.2 Fear of Cybercrime....106
3.5.2.1 Personal Traits....107
3.5.2.2 Social Determinants....109
3.5.2.3 Psychological Factors....109

3.5.3 Consequences of Fear of Cybercrime ..... 110
3.5.3.1 Security intention ..... 110
3.5.3.2 Behavioural change ..... 111
3.6 Summary ..... 112
Chapter 4 Methodology ..... 113
4.1 Introduction ..... 113
4.2 The Rationale for Utilising a Mixed Methods Research Paradigm ..... 113
4.3 Research Design and Analytic Strategy ..... 118
4.4 Design of Quantitative Phase of Research ..... 122
4.4.1 Sample Size ..... 125
4.4.2 Operationalisation ..... 126
4.4.3 Definitions of Outcome Variables ..... 126
4.4.4 Operationalisation of Response Variables ..... 131
4.4.5 Contextual Vulnerabilities Elements ..... 137
4.5 Analytic Strategy of Quantitative Phase of the Research ..... 138
4.5.1 Univariate Analysis: ..... 139
4.5.2 Bivariate Analysis: ..... 139
4.5.3 Multivariate Analysis: ..... 141
4.5.3.1 Analytic Procedure: ..... 142
4.6 Reflexive Account of the Qualitative Phase of Research ..... 144
4.6.1 Reliability and Validity ..... 145

4.6.2 Sampling ..... 148
4.6.2.1 Defining the Sample Universe ..... 148
4.6.2.2 Sample Size ..... 149
4.6.2.3 Devising a Sampling Strategy ..... 150
4.6.2.4 Sample Sourcing ..... 152
4.6.3 Ethical Issues and Obtaining Ethics Approval ..... 160
4.6.4 Interview Guide ..... 160
4.6.5 Conducting Semi-Structured Interviews ..... 160
4.6.6 Pilot Study ..... 166
4.7 Analytic Procedure: Content Analysis ..... 169
4.7.1 Data Preparation ..... 170
4.7.2 Data Display ..... 176
4.7.3 Conclusion Drawing ..... 177
4.8 Summary ..... 178
Chapter 5 Quantitative Results ..... 179
5.1 Introduction ..... 179
5.2 Descriptive Statistics: ..... 181
5.2.1 Outcome Variable: ..... 181
5.2.2 Response Variables: ..... 182
5.3.3 Control Variables: ..... 186
5.3.3.1 Gender: ..... 186

5.3.3.2 Age: ..... 187
5.3.3.3 Education Level: ..... 187
5.3.3.4 Household Income: ..... 188
5.3 Online Lifestyle Correlates of Economic Cybercrime Victimisation ..... 189
5.3.1 Bivariate Analyses ..... 190
5.3.1.1 Operationalisation of the LRAT Concepts ..... 191
5.3.1.2 The Results of Bivariate Analyses ..... 193
5.3.1.2 Absence of Capable Guardianship ..... 195
5.3.1.3 Control Variables ..... 198
5.3.2 Multivariate Analysis Results ..... 200
5.3.2.1 Binary Logistic Regression Results ..... 200
5.3.2.2 Three-way Cross-tabulation Results ..... 205
5.4 Discerning the Determinants of Economic Cybercrime through the Lenses of the Contextual Vulnerabilities Approach ..... 221
5.4.1 Technological Vulnerabilities ..... 221
5.4.1.1 Descriptive Statistics ..... 224
5.4.1.2 Bivariate Analysis: ..... 225
5.4.1.3 The Impact of Age on Electronic Device Related Risk of Victimisation ..... 228
5.5 Fear of Cybercrime ..... 232
5.5.1 Gender Differences in Fear of Cybercrime ..... 233
5.5.2 Age Differences in Fear of Cybercrime ..... 235
5.6 Summary ..... 236

Chapter 6 Becoming an Online Target ..... 239
6.1 Introduction ..... 239
6.2 The Determinants of being a Phishing Attack Target ..... 241
6.2.1 Voluntary Personal Information Disclosure ..... 243
6.2.2 Involuntary Personal Information Disclosure ..... 248
6.3 The Determinants of being a Hacking Attack Target ..... 250
6.3.1 Deviant Online Behaviour ..... 250
6.4 Summary ..... 253
Chapter 7 Experiencing Victimisation ..... 256
7.1 Factors Affecting Internet Users' Decision-Making Processes ..... 256
7.1.1 Email Phishing ..... 257
7.1.1.1 External Vulnerabilities ..... 258
7.1.1.2 Internal Vulnerabilities ..... 262
7.1.2 Website Phishing ..... 264
7.2 Correlates of Economic Cybercrime Victimisation ..... 269
7.2.1 Online Lifestyle Correlates ..... 269
7.2.2 Contextual Vulnerabilities ..... 271
7.2.2.1 Individual and Behavioural Vulnerabilities ..... 271
7.2.2.2 Socio-cultural (Context Specific) Vulnerabilities ..... 275
7.2.2.3 Macro Vulnerabilities ..... 279
7.3 Summary ..... 290

Chapter 8 Consequences of Economic Cybercrime Victimisation .....292
8.1 Introduction.....292
8.2 Psychological Effects of Victimisation Experience.....295
8.2.1 Emotional Responses.....295
8.2.2 Fear of Crime.....299
8.3 Impact of Victimisation on Internet Users' Online Lifestyles.....302
8.3.1 Initial Threat Appraisal.....303
8.3.2 Consecutive Coping Appraisals.....304
8.4 Summary.....320
Chapter 9 Discussion.....321
9.1 Introduction.....321
9.2 Economic Cybercrime Victimisation Process .....321
9.3 Being Targeted Online.....322
9.3.1 Exposure to Phishers .....322
9.3.2 Proximity to Hackers' Tools.....326
9.4 Occurrence of Victimisation.....327
9.4.1 Phishing .....328
9.4.1.1 Email Phishing .....328
9.4.1.2 Website Phishing.....331
9.4.2 Unauthorised Access to Online Financial Accounts and Credit Card Information
……..333
9.4.2.1 Technological Vulnerabilities .....334

9.4.2.2 Online Deviance ..... 339
9.4.2.3 Virtual Hot Spots of Crime ..... 342
9.5 Dealing with Consequences of Economic Cybercrime Victimisation ..... 343
9.5.1 Emotional Responses ..... 343
9.5.2 Fear of Crime ..... 345
9.5.2.1 Social Determinants of Fear of Cybercrime ..... 346
9.5.2.2 Demographic Characteristics ..... 347
9.5.2.3 Psychological Factors ..... 348
9.5.2.4 Behavioural Responses ..... 350
9.5.3 Behavioural Responses ..... 351
9.5.3.1 Impact of Phishing Victimisation Experience on Behavioural Responses ..... 351
9.5.3.2 Impact of Hacking Victimisation Experience on Behavioural Response ..... 354
9.6 Evaluating the Applicability of LRAT to Economic Cybercrime Victimisation ..... 356
9.6.1 Proximity to Motivated Offender ..... 357
9.6.2 Exposure to Motivated Offenders ..... 359
9.6.3 The absence of Capable Guardianship ..... 362
9.7 Summary ..... 364
Chapter 10 Conclusion ..... 366
10.1 Introduction ..... 366
10.2 Summary of Findings ..... 369
10.2.1 Being a Target of an Online Attack ..... 369

10.2.2 Process of Becoming a Victim ..... 371
10.2.3 Contextual Vulnerabilities Approach ..... 372
10.2.3.1 Individual and Behavioural (Micro Level) Vulnerabilities ..... 373
10.2.3.2 Macro Vulnerabilities ..... 374
10.2.3.3 Socio-cultural (Context Specific) Vulnerabilities ..... 377
10.2.4 Impacts of Victimisation ..... 380
10.2.5 Applicability of LRAT to Economic Cybercrime Victimisation ..... 382
10.3 Integrated Cyber Victimisation Model ..... 384
10.3.1 Being Targeted Online ..... 384
10.3.2 Threat Assessment ..... 386
10.3.3 Consequences of Victimisation ..... 388
10.4 Significance of Research and Original Contributions to Cybercrime Victimisation Literature ..... 391
10.5 Implication of Research Findings for Policy and Policing Economic Cybercrime ..... 393
10.6 Limitations of the Thesis and Recommendations for Future Research ..... 398
Appendices ..... 401
Appendix 1: Ethical Approval Letter From Durham University ..... 401
Appendix 2: Participant Information Sheets ..... 403
Appendix 3: Request Letter ..... 409
Appendix 4: Consent Form ..... 410
Appendix 5: Interview Guides ..... 411
Appendix 6: Poster and Flier ..... 420

Appendix 7: Coding Outcome Variables ..... 421

Appendix 8: Glossary ..... 427

Bibliography ..... 430

**List of Tables**


Table 1.1 Classification of Cybercrime……10

Table 1.2 Summary of Victim Typologies……20

Table 2.1 Operationalisation of Reyns et al. (2011)……..59

Table 4.1 Descriptive Statistics of Online Banking Victimisation……..128

Table 4.2 Exposure to Motivated Offender……133

Table 4.3 Proximity to Motivated Offender……134

Table 4.4 Online Guardianship……...135

Table 4.5 Demographic Characteristics……..137

Table 4.6 Electronic Devices Used to Access the Internet……..138

Table 4.7 Sampling Criteria……153

Table 4.8 Summary of the Interviews Conducted……...159

Table 4.9 Coding Process of the Negative Life Events Category……174

Table 4.10 Coding Process of the Contextual Vulnerabilities Concept……175

Table 5.1 Economic Cybercrime Victimisation……..181

Table 5.2 Frequency of Variables Representing Proximity and Exposure to Motivated Offender……..……..…..183

Table 5.3 Frequency of Variables Representing Guardianship Measures ……...……...……..……184

Table 5.4 Frequency of Internet Usage……...185

Table 5.5 Frequency of Variables Representing Electronic Devices Used to Access the Internet…..……..……186

Table 5.6 Economic Cybercrime Across Gender Categories……..187

Table 5.7 Economic Cybercrime Across Age Categories…….……..187

Table 5.8 Economic Cybercrime Across Education Categories……...……..188

Table 5.9 Economic Cybercrime Across Household Income Categories……..…..188

Table 5.10 Response Variables……...……..192

Table 5.11 Response Variables of Online Guardianship Measures ……...…….....193

Table 5.12 Cross-tabulation Results for the relationship between Online Activities and Experiencing Economic Cybercrime Victimisation……194

Table 5.13 The Relationship between Frequency of Internet Usage and Economic Cybercrime……...……..195

Table 5.14 Cross-tabulation Results for the Relationship between Guardianship Measures and Experiencing Economic Cybercrime……197

Table 5.15 The Relationship between Demographic Characteristics of the Internet Users and Economic Cybercrime……..199

Table 5.16 Binary Logistic Regression Analysis……...……..202

Table 5.17 Binary Logistic Regression Analysis……..204

Table 5.18 Sample Bivariate Analysis Outputs……208

Table 5.19 Cross-tabulation Results for the Relationship between Guardianship Measures and Experiencing Economic Cybercrime……209

Table 5.20 Cross-tabulation Results for the Relationship between Guardianship Measures and Experiencing Economic Cybercrime……209

Table 5.21 The Relationship between Using the Internet to Access Online Financial Activities and Experiencing Economic Cybercrime……211

Table 5.22 Three-way Cross-tabulation Table Controlling Age……...212

Table 5.23 Three-way Cross-tabulation Controlling Age……214

Table 5.24 Three-way Cross-tabulation Table Controlling Gender……..215

Table 5.25 Three-way Cross-tabulation Controlling Gender……...….216

Table 5.26 Three-way Cross-tabulation Table Controlling Education Level……..…….217

Table 5.27 Three-way Cross-tabulation Controlling Education Level……..218

Table 5.28 Three-way Cross-tabulation Table Controlling Household Income……219

Table 5.29 Three-way Cross-tabulation Controlling Household Income……..220

Table 5.30 Categorisation of Electronic Devices Used to Access the Internet into Risk Groups……223

Table 5.31 The Relationship between Electronic Device Used to Access the Internet and Experiencing Various Forms of Economic Cybercrime……..……...227

Table 5.32 The Relationship between Electronic Devices Used to Access the Internet, Guardianship Measures and Experiencing Loss of Money Through Virus Infection……..227

Table 5.33 The Relationship between Using the Internet to Access Online Banking or Managing Services and Experiencing Online Banking Fraud after Controlling Most Frequently Used Device to Access the Internet……..231

Table 5.34 Fear of Crime……..232

Table 5.35 Gender Differences in Fear of Crime……..233

Table 5.36 Impact of Previous Economic Cybercrime Victimisation on Gender Differences in Fear of Cybercrime……..234

Table 5.37 Age Differences in Fear of Crime……...235

Table 5.38 Impact of Previous Economic Cybercrime Victimisation on Age Differences in Fear of Cybercrime…….236

Table 7.1 Demographics of Phishing Victims…….264

Table 7.2 The Relationship between Low Internet Self-efficacy and Website Phishing……..266

Table 7.3 Password Management……...273

Table 7.4 Security Measure Avoidance……..276

Table 7.5 Socio-cultural Vulnerabilities……..…...278

Table 7.6 Preference of Electronic Devices Used for Financial Purposes……...283

Table 7.7 The Relationship between Type of Device for Financial and Type of Victimisation……...283

Table 7.8 Free Public Wi-Fi Usage……...……..284

Table 8.1 Fear of Economic Cybercrime……...……..300

Table 8.2 Coping Strategy Adaption for Elderly Phishing Victims…….310

Table 8.3 Coping Strategy Adaption for Hacking Victims……..313

Table 8.4 Coping Strategy Adaption for Repeat Victims……315

**List of Figures**


Figure 1.1 Online Banking Usage in the UK……..13

Figure 1.2 Online Banking Fraud in the UK……...13

Figure 2.1 Historical Transformation of LRAT Concepts……..52

Figure 2.2 PMT Conceptual Framework……69

Figure 3.1 Classification of Phishing Attempts……..87

Figure 4.1 Mixed Methods Quantuum……...……..120

Figure 4.2 Visual Model of Research Design……...121

Figure 4.3 The Statistical Procedure to Obtain Online Banking Variable……128

Figure 4.4 Syntax Editor Screenshot….……...129

Figure 4.5 Statistical Procedure to Obtain Loss of Money Through Virus Infection Variable……...129

Figure 4.6 Statistical Procedure to Obtain Online Identity Fraud Variable……..130

Figure 4.7 Statistical Procedure to Obtain the Card-not-present Fraud Variable……..131

Figure 4.8 Online Guardianship Measures……...135

Figure 4.9 The Cyber Victimisation Coping Model ……168

Figure 4.10 Data Analysis Process……170

Figure 4.11 Data Analysis Process……176

Figure 5.1 Economic Cybercrime Victimisation……..181

Figure 5.2 Cybercrime Across Gender Categories……...187

Figure 5.3 Economic Cybercrime Across Age Categories……...187

Figure 5.4 Economic Cybercrime Across Education Levels……...….188

Figure 5.5 Economic Cybercrime Across Household Income……..……..188

Figure 5.6 Economic Cybercrime Victimisation Across Age Categories……...214

Figure 5.7 Relative Risk Controlling Age……214

Figure 5.8 Economic Cybercrime Controlling Gender……..……..216

Figure 5.9 Relative Risk Controlling Gender……...216

Figure 5.10 Economic Cybercrime Controlling Education Level……..218

Figure 5.11 Relative Risk Controlling Education Level…….218

Figure 5.12 Economic Cybercrime Controlling Household Income…….…….221

Figure 5.13 Relative Risk Controlling Household Income……..……..221

Figure 5.14 Frequency of Electronic Device Usage……..…….……224

Figure 6.1 Process of being a Target of an Online Attack……..……..255

Figure 7.1 Phishing Victimisation Process…….…….268

Figure 8.1 The Cyber Victimisation Coping Model……...…..294

Figure 8.2 The Cyber Victimisation Coping Model…….……316

Figure 9.1 Process of Economic Cybercrime Victimisation…….322

Figure 9.2 Online Advertisement Sample……..……..324

Figure 10.1 Decision-making Process…….…..387

Figure 10.2 Decision-making Process……...389

Figure 10.3 Integrated Cyber Victimisation Model…….……..390

## Declaration

I declare that this is my own work and has not been submitted for the award of a higher degree anywhere else.

## Statement of Copyright

**Acknowledgements**

First and foremost, I would like to express my utmost gratitude to my primary supervisor Dr Christopher Lawless and secondary supervisor Professor Fiona Measham for providing their expertise and guidance throughout the process of this doctoral research. Without their unwavering support and encouragement, I feel as though this thesis could have never been completed.

Additionally, I would like to express my appreciation to Dr Ivan Hill for his continuous encouragement, invaluable advice and academic support. His support has benefited this thesis greatly.

I also would like to thank Professor Vikki Boliver for sharing her expertise on the statistical methodology.

I am also very grateful to the Turkish Gendarmerie General Command for their support and accrediting me as a candidate to pursue this postgraduate degree. I particularly would like to express my deepest gratitude to the President of Turkish Gendarmerie and Coast Guard Academy, Major General Huseyin Kurtoglu for providing me with the opportunity to continue my postgraduate study at Durham University. Without his invaluable support and trust, it would be impossible to complete my doctoral research.

I would like to thank Postgraduate research administrator Sarah Fiona Jackson and staff and members of Sociology Department for always being welcoming, supportive and friendly.

I am grateful to Durham International Women Group, Age UK County Durham, Durham Constabulary and Durham County Council for their assistance and guidance in the early stages of this research. In no particular order: Dave Sampson, Glenn Maleary, Tony Murray, Christine Fletcher, George Barber and Peter Dawson for creating a network.

Particular thanks to Bulent Sungur for his friendship, encouragement and sharing the ups and downs of this postgraduate journey.

Finally, I would like to thank all of my participants who shared their experiences, opinions and thoughts. I am very grateful for their courage and openness.

Most importantly, I would like to thank my wife Eda, my son Atakan and my daughter Elanaz for their endless love and support throughout all of my endeavours.

This thesis has been dedicated to my wife, Eda who is always in my heart. Thank you for your love, inspiration and support.

# Chapter 1 Introduction

## 1.1 Introduction

This chapter outlines the background of this mixed-methods doctoral thesis, which examines the determinants and impacts of economic cybercrime victimisation at an individual level in the UK. This chapter initially provides background information about economic cybercrime and the modus operandi of online perpetrators. It then presents a synopsis of cybercrime victimisation studies. The chapter provides research aims, objectives and research questions before concluding with a presentation of the structure of the thesis.

The invention and proliferation of the Internet may be considered as one of the most influential technological advancements of this century (Mowery and Simcoe, 2002; Weekes, 2003). The Internet can be utilised for a wide array of purposes ranging from communication to trading. The integration of mobile technologies to the Internet has also boosted the omnipresence of the Internet in our daily lives (Holt and Bossler, 2016). It is estimated that approximately 89% of adult people have access to the Internet in the UK in 2018 (Office for National Statistics, 2018).

The unprecedented intrusion of the Internet into every facet of our lives also gave rise to new opportunities for the commission of traditional crimes in the last two decades (Grabosky, 2001; Pease, 2001). Child pornography, identity theft, illicit drug trading and fraud are examples of physical world crimes that prosper from the opportunities the new environment, cyberspace, offers (Clarke, 2004). For example, cryptomarkets, which are websites that provide anonymity to its users through encryption (Martin, 2014), appear to

provide a safe environment for illicit drug trading (Masson and Bancroft, 2018; Aldridge, 2019).

The borderless global nature of the Internet has also created unparalleled opportunities for criminals to commit a crime in large volumes while remaining *relatively anonymous* (Levi, 2001; Koops, 2010) since attaining absolute online anonymity is hard to reach task (Savage, 2016; Bancroft and Scott Reid, 2017). Online perpetrators now have the chance to access numerous individuals who are physically beyond their reach (Wall, 2008b). Additionally, the Internet empowers individuals to conduct large scale online attacks without depending on someone else (Goldsmith and Brewer, 2015). This ability to conduct online attacks individually was fostered with the introduction of the websites offering tutorials on handling online attacks or freely distributed software that assists online criminal acts. The advent of the Internet has not only boosted the execution of traditional crimes in cyberspace; it has also given rise to new forms of cybercrimes, namely true cybercrimes. True cybercrimes are a new genre of crimes that cannot be committed without networked Internet technologies (Wall, 2007). Malware infection and spamming[1] are the most vivid examples of this new genre of cybercrimes (Wall, 2008a). This genre of cybercrime is dependent on the existence of the networked Internet technologies; it vanishes when the networked Internet technologies are removed from the equations of the crime (Wall, 2007).

Empirical research suggests that economic cybercrime is on the rise and it poses a significant threat to citizens, business and government (Yuan et al., 2014; Levi et al., 2015; Levi, 2017). The Crime Survey for England and Wales 2017/2018 demonstrates that 4.2% of participants experienced bank or credit account fraud. While more than 2.2 million bank account and credit account fraud incidents were reported, approximately 1.95 million

[1] Technical terms used in this thesis are defined in the Glossary (Appendix Eight).

individuals were victimised in 2017 (Office for National Statistics, 2018). The Annual Fraud Indicator (AFI) report prepared by UK Fraud Costs Measurement Committee with the help of Experian, Centre for Counter Fraud Studies, University of Portsmouth and Crowe Clark Whitehill, illustrates that identity fraud against individuals cost approximately £1.344 billion to the UK economy (AFI, 2017). This cost soars to £5.4 billion when identity fraud against business is taken into consideration (Action Fraud, 2017). However, despite its adverse impacts on individuals, society and private companies, there is a dearth of theoretically informed empirical research on economic cybercrime victimisation (Hernandez-Castro and Boiten, 2014; Reyns et al., 2014; Dusabe, 2016). To address this knowledge gap, this thesis aims to explore economic cybercrime victimisation patterns, the causes of becoming a victim and to understand the effects of economic cybercrime victimisation on the Internet users' online lifestyles and safeguarding measures.

### 1.1.1 Definition of Cybercrime

It is generally considered that there is a lack of agreement around a standard definition of cybercrime in the literature (Wall, 2008a; Anderson et al., 2013; Williams and Levi, 2015). This section of the chapter provides definitions of cybercrime provided by various sources.

The Council of Europe Cybercrime Convention (ETS No. 185), which is also known as The Budapest Convention, is one of the first international initiatives to create a shared understanding of cybercrime (Wall, 2013a), though the convention caused controversy regarding its imbalance between public liberties and power delegated to governments about surveillance, search and seizure of computers (Taylor, 2002). Rather than providing an umbrella definition, this convention highlights the importance of deterrence. The Convention defines the scope of the deterrence as "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such

systems, networks and data by providing for the criminalisation of such conduct" (The Council of Europe Convention on Cybercrime, 2001, p. 2), and presents sub-categories of cybercrime within four titles. A number of cybercrimes were defined within these four categories. However, this approach received criticism, as it does not include some sorts of cybercrime like stalking, extortion (Brenner, 2007), online identity theft and spamming (Clough, 2014).

The Commission of the European Communities (C.E.C.) report defines cybercrime as "criminal acts committed using electronic communications networks and information systems or against such networks and systems" (European Commission, 2007, p. 2). In comparison with the Council of Europe's broad definition, the C.E.C perceives cybercrime in a narrow sense. This definition again excludes the cases related to illicit online activities.

The United Nations is another important international actor that dealt with cybercrime related issues. The United Nations manual on the prevention and control of computer-related crime (1994) uses the terms of computer crime and computer-related crime interchangeably. This manual did not provide any clear definition but emphasised the fact that traditional crimes such as theft, fraud and forgery can be associated with computer crime. The manual also stated establishing a distinction between illicit and unlawful activities was mandatory (UN Manual, 1994). The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (2000) was another significant occasion where cybercrime related issues were discussed. During the workshops two cybercrime definitions were formed:

a) "any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them."

b) "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network" (UN Congress, 2000, p. 5). While the former

defines the cybercrime in a narrow sense as computer crime, the latter describes it in a broader sense as a computer-related crime.

A definition of cybercrime can also be found in the Commonwealth of Independent States Agreement (2001). The act without referring the term cybercrime defines[2] it as "a criminal act of which the target is computer information" (as cited in Akhgar et al., 2016, p. 298). This definition focuses on crimes against computers and leaves out the occasions where computers or networked technologies are used to commit crimes online.

The Shanghai Cooperation Organization (SCO) Agreement[3] provides a definition of cybercrime in its Annex as "the use of information resources and (or) the impact on them in the informational sphere for illegal purposes", however, agreement prefers the term information offences (as cited in Malby et al., 2013, p. 12). This definition also focuses on crimes related to information technologies and omits offences and illicit activities against individuals.

With regards to academic efforts to define cybercrime, while some scholars (i.e. Thomas and Loader, 2000; Gordon and Ford, 2006; Koops, 2010; Kshetri, 2010; Casey, 2011; Pathak, 2016b) strived to create a definition of cybercrime, some others (Gordon and Ford, 2006; Wall, 2007; Brenner, 2010) preferred to provide a typology of cybercrime. Firstly, the two most popular definitions of cybercrime will be examined, and then the typology of cybercrime will be presented.

A search on academic databases such as Google Scholar and ProQuest was conducted to find out the most popular definition of cybercrime. The search result indicated that the

[2] The original language of the Commonwealth of Independent States Agreement is Russian. Thus, it is cited from another source.
[3] Due to unavailability of the English version of the Shanghai Cooperation Organization (SCO) Agreement, it is cited from another source.

definitions provided by Thomas and Loader (2000) and Gordon and Ford (2006) were the most frequently cited definitions in academic papers related to cybercrime. Thus, these two definitions will be juxtaposed with each other. Thomas and Loader (2000, p. 3) define cybercrime as *"computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks"* whereas Gordon and Ford (2006, p. 14) define it as *"any crime that is facilitated or committed using a computer, network, or hardware device"*. While the former definition involves illicit behaviours that are not defined as delinquent, the latter refers to only specific actions that are a crime. In this aspect, the description provided by Thomas and Loader (2000) covers a wide range of activities ranging from illicit ones like distributing Internet users' personal information (Gercke, 2012) or illegal ones such as spamming (Wall, 2005). Furthermore, the latter definition not only includes actions mediated through networked technologies but it also covers the crimes to be committed via hardware devices, though, the former does not include activities facilitated with devices like iPads or smartphones (Blanco Hache and Ryder, 2011; Dolliver and Poorman, 2018) or memory sticks containing malware (Gercke, 2012).

### 1.1.2 Three Generations of Cybercrime

Gordon and Ford (2006) argue that cybercrimes cover a wide array of actions, which represents a continuum ranging from entirely technological crimes to conventional crimes. Similarly, given the definitional complexities caused by the versatile nature of cybercrime, which is fuelled by networked technologies, Wall (2007) offers a chronological evolutionary account of cybercrime. It is generally accepted that networked technologies created new opportunities for the conduit of crime (Wall, 2005). Thus, the transformation test was offered to perceive the opportunities created by networked technologies (Wall, 2010a). This test

assumes that the removal of the networked technologies from the equation of the crime reveals the cyber nature of the crime.

The first-generation cybercrime consists of crimes that are entirely traditional, and networked technologies are utilised to either gather information to commit a crime or create a channel of communication (Wall and Williams, 2007). When the networked technologies are removed from the crime, it persists. This generation of cybercrime is dubbed as cyber-assisted crimes (Levi et al., 2015; Levi et al., 2017). The use of a computer to access the building plan in a bank robbery can be an example of the first-generation cybercrime. The first-generation cybercrime is also named as low-end cybercrime to emphasise the slight impact of the networked technologies in the commission of the crime.

The second-generation cybercrime is hybrid cybercrime, which is the outcome of the integration of traditional crimes and networked technologies (Wall, 2007). The networked technologies become an environment for the commission of the traditional crimes for this type of crimes (Wall, 2008b). (Levi et al., 2015) and (Levi et al., 2017) as cyber-enabled crimes. Hacking, large-scale frauds, identity theft and online pornography are examples of this generation (Wall, 2005). The crime persists after the removal of networked technologies, but most of the opportunities such as the chance of conducting large-scale attacks or accessing the individuals living in remote locations would be lost.

The last generation of cybercrime is considered by some to be the ‘true’ cybercrime, which is entirely technological and can happen in cyberspace. The crime vanishes after the removal of networked technologies (Wall, 2005). This generation of cybercrime is also called cyber-dependent crimes due to its dependence on cyberspace (Levi et al., 2015; Levi et al., 2017). Ransomware, which is a type of cybercrime committed through encrypting files or folders that are present in the computer, is a vivid example of a true cybercrime. This crime

cannot be committed in the absence of the networked technologies since the phases requiring the distribution of malware and the encryption of the files are cyber-dependent. For this reason, the third-generation cybercrime is sui generis and rests at the high-end of the spectrum (Wall, 2007). Phishing, denial of services and spamming are the other examples of the third-generation cybercrime (Wall, 2015).

### 1.1.3 Typology of Cybercrime

The classification of cybercrime is another controversial issue in cybercrime literature. Several scholars and institutions (The Council of Europe Convention on Cybercrime, 2001; Gordon and Ford, 2006; Wall, 2007; Higgins and Wolfe, 2009; Brenner, 2010) provided a typology of cybercrime. Table 1.1 illustrates the typologies of cybercrime provided by several authors. As can be seen from the table, three typologies presented by The Council of Europe Convention on Cybercrime (2001), Wall (2007) and Brenner (2010) generally overlap. These typologies were created from a law perspective. This approach similarity might be the reason for the overlap between these typologies. It appears that Wall (2007) gathered the cybercrimes classified under Title 3 and Title 4 of the under one heading as computer-related offences. While Brenner's (2010) first two categories, target cybercrimes and tool cybercrimes, displays similarity with Wall's (2007) first two categories, computer-integrity crimes and computer-assisted crimes, Brenner's (2010) last category corresponds Wall's first-generation cybercrime.

Although the typology presented by Higgins and Wolfe (2009) was based on the opportunities that each category of cybercrime created for different offending groups, cybercrimes that were included into categories generally overlap with those of Wall (2007). Gordon and Ford (2006) suggested a two-category typology of cybercrime. They argue that cybercrime presents a continuum where technology-based crimes rest at one end and people-based crimes rest at the other end. The crimes like phishing, hacking and identity theft are

considered as Type I cybercrime, which is entirely automated. The crimes that involve human element were classified as Type II cybercrime.

This thesis applies Wall's (2007) classification since this classification is widely accepted in cybercrime literature (Yar, 2005; Lagazio et al., 2014).

## 1.2 Economic Cybercrime

There appears to be no consensus in the literature around the terminology that covers financial crimes committed via networked Internet technologies. **Economic cybercrime** (Maurushat, 2010; Levi et al., 2015) **financial cybercrime** (Marshall, 2010; Lagazio et al., 2014), **online financial crime** (Akhgar and Arabnia, 2013) and **online economic crime** (Knapp, 2004; Pamplin, 2014) are the terms used to describe the financially motivated online crimes. This thesis uses the term 'economic cybercrime' to describe the financial crimes committed via networked Internet technologies since this term is widely accepted in recent cybercrime studies (i.e. Pathak, 2016a; Martellini et al., 2017; Mattern, 2017; Papantoniou, 2017; Ray and Kaushik, 2017; Williams and Levi, 2017).

Levi et al. (2015, p. 9) describe the scope of economic cybercrime as *"obtaining, or initiating a dialogue to obtain, data, goods and/or money by deception, misrepresentation or straightforward fraud from individuals, businesses and government through the medium of the Internet."* As can be seen, economic cybercrime is an umbrella term encompassing a wide range of financially motivated online crimes including money laundering or financing of terrorism (Menon and Guan Siew, 2012).

Table 1.1
*Classification of Cybercrime*

| **Convention on Cybercrime (2001** | **Wall (2007)** | **Brenner (2010)** | **Higgins (2009)** | **Gordon and Ford (2006)** |
|---|---|---|---|---|
| Title 1<br>Offences against the confidentiality, integrity and availability of computer data and systems<br><br>*Hacking | Computer-integrity crimes<br>(Crimes against the machines)<br><br>*Cyber-trespass<br>*Hacing/Cracking | Target cybercrimes<br><br>*Hacking<br>*Malware infection | Cyber community<br><br>*Hacking<br>*Cracking | Type I Cybercrime<br><br>*Phishing<br>*Hacking<br>*Identity Theft |
| Title 2<br>Computer-related offences<br><br>*Computer related forgery and fraud | Crimes-assisted or related offenses<br>(Crimes using the machines)<br><br>*Cyber-deceptions<br>*Fraud | Tool cybercrimes<br><br>*Fraud | Cyber fraud | Type II Cybercrime<br><br>*Cyberstalking<br>*Extertion<br>*Blackmail |
| Title 3<br>Content-related offences<br><br>*Child Pornography | Content-related offenses<br>(Crimes in the machines)<br>Cyber-obscenity<br>Cyber-violence/harm | Computer incidental<br><br>*Real world crimes using computers | Cybermarkets<br><br>*Digital pricacy<br>*Cyberpornography | |
| Title 4<br>Offences related to infringements of copyright and related rights<br><br>*Digital piracy | | | | |

The FBI[4] has identified twenty-three types of fraud bearing a cyber element at one point. Similarly, Action Fraud UK[5] provides a number of online frauds like advance fee fraud, identity fraud or bank card fraud. Furthermore, as Levi et al. (2015) clearly illustrate, economic cybercrime may occur at three levels: individual, business and government. This breadth of scope is beyond the capability of a doctoral research. Hence, this thesis focuses on financially motivated online crimes that target individuals. The types of online frauds to be examined by this thesis will be limited to card-not-present fraud, online banking fraud, and online identity fraud.

### 1.2.1 Card-not-present Fraud

The increased use of the Internet for commercial purposes has created new frontiers for traditional payment methods. Payment cards, which are mainly categorised as credit cards, debit cards and charge cards (Schneider, 2011; Turban et al., 2015), have become the primary payment method for online purchases, especially for the business-to-customer e-commerce (Anderson et al., 2018; Banka, 2018). The latest report released by the UK Card Association illustrates that the number of card purchases and card spending displayed a record in the UK in 2017. According to this report, 1.4 billion card transactions occurred, and £58.0 billion were spent during these transactions (The UK Cards Association Card Expenditure Report, 2017).

This popularity of payment cards created new opportunities for perpetrators. While the earlier versions of the credit card fraud were mostly offline, the criminal intention migrated to cyberspace due to a myriad of opportunities emanating from cyberspace (Wall, 2007). Fraudsters utilised the physical world methods like skimming, which involves copying the information embedded in the magnetic strip of the card to another card during automated teller

[4] Please see FBI's website https://www.fbi.gov/scams-and-safety/common-fraud-schemes to see full list.
[5] Please see Action Fraud's website https://www.actionfraud.police.uk/fraud-az-online-fraud to see full list.

machines (ATM) transactions besides processing the card with pin entry devices at shops or restaurants (Jewkes, 2009; Kraemer-Mbula et al., 2013; Reurink, 2016) or dumpster diving of credit card information (Lease and Burke, 2000; Granger, 2001) to clone the payment card. However, the introduction of the precautions such as the use of the personal identification number (PIN) and installation of chips into plastic cards as well as the introduction of the card validation codes (CVC2) decreased the offline credit card fraud dramatically in the UK (Wall, 2010b; Reyns and Henson, 2016).

These precautions applied to prevent credit card fraud in the physical world have transformed credit card fraud to card-not-present fraud, which Levi (2017, p. 14) names as "transitional crimes". Card-not-present fraud (CNP) is the unauthorised use of payment cards in the absence of a physical card (Montague, 2010). Card-not-present fraud does not only encompass payment cards, but it also involves new forms of digital payment methods such as e-wallet, a pre-paid electronic card that is linked with the users' bank account, or other online payment methods (i.e. PayPal or Shopify). These new digital payment methods are devised to both decrease the transaction costs and alleviate the risks inherent to payment cards (Şeitan et al., 2010; Sudarno, 2012).

### 1.2.2 Online Banking Fraud

Internet banking has provided many advantages such as ease of use, instant access to the accounts at any time regardless of the geographical locations and decreased costs for both banks and customers. Online banking fraud covers unauthorised, illegal access to customers' online bank accounts and fund transfers to third parties (McGuire and Dowling, 2013; Levi et al., 2015). As Figure 1.1 illustrates, online banking usage is on the rise in the UK, and approximately 69% of the adult British population use online banking (Office for National Statistics, 2018). Parallel to this increase in online banking usage, online banking fraud losses

elevated steadily from 2011 to 2015, where it reached a peak of £133.5 million. However, the losses decreased to £101.8 million in 2016 (Figure 1.2).

Figure 1.1
*Online Banking Usage in the UK*

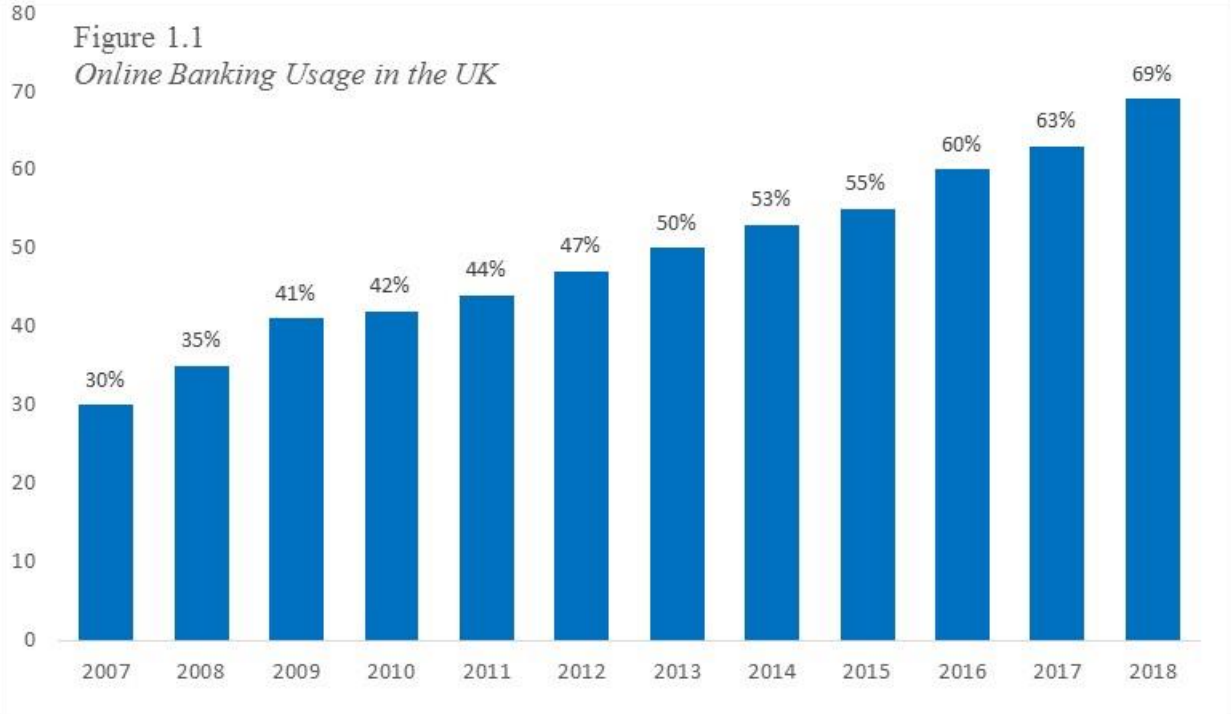
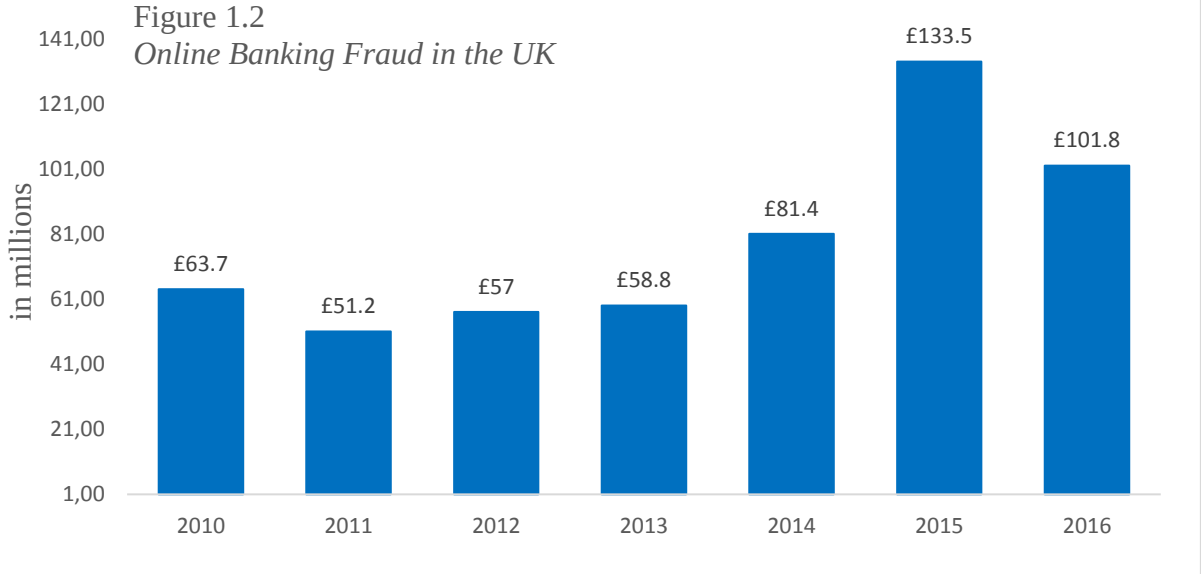



Figure 1.2
*Online Banking Fraud in the UK*



### 1.2.3 Identity Fraud

Identity fraud is another significant online threat for Internet users (Smith, 2010; Kraemer-Mbula et al., 2013; Wall, 2013d; Levi et al., 2015; Levi, 2016). According to the Credit Industry Fraud Avoidance System (Cifas)[6] 174,523 identity fraud cases were reported in 2017, which means a 125% rise when compared to 2007. Moreover, 95% of these cases involved the impersonation of the victims (Cifas, 2018). Though it may be defined differently in other identity-related studies, identity theft covers the actions of "acquiring and then unlawfully using the personal and financial account information to acquire goods and services in someone else's name" (McQuade, 2006, p. 69) in economic cybercrime context. As Brenner (2010) highlights, identity theft does not involve the action of depriving the rightful owner of one's personal information. Rather, it is the copying of personal identifying information that is labelled as identity theft (McGuire and Dowling, 2013). On the one hand, identity theft refers to the impersonation of somebody to commit a crime or establish a new life (Pontell and Geis, 2007; Reurink, 2016). On the other hand, it involves unauthorised access to and use of personal identifying information for financial gain (Copes et al., 2010; Smith, 2010; Holt and Turner, 2012).

It appears that identity theft and identity fraud has been used interchangeably in cybercrime literature (Sproule and Archer, 2007). However, while identity theft refers to misappropriation of victims' personal identifying information, identity fraud involves the application of acquired information for financial gain (Kraemer-Mbula et al., 2013; Reyns and Henson, 2016). Wall (2010b) classifies identity theft as input fraud as it provides the required information for the commission of the output fraud namely identity fraud.

[6] Cifas is a not-profit membership organisation aimed to reduce fraud related crimes in the UK.

## 1.3 Modus Operandi of Online Perpetrators

Information is the primary target that fraudsters strive to access (Newman and Clarke, 2003). The information gained from various sources may be utilised to conduct online attacks aiming financial gain. Phishing, hacking and malware infection are the most effective methods that online perpetrators adapt to defraud Internet users into yielding their personal or financial information as well as to gain unauthorised access to Internet users' computers or online accounts (Wall, 2013b; Williams, 2015).

### 1.3.1 Phishing

The term phishing was first used around 1995 after a notorious America Online (AOL) accounts' hack, where naïve Internet users were manipulated into divulging their login information (Purkait, 2012; Gupta et al., 2017). Early hackers coined the term phishing by replacing the letter f in fishing with *'ph'* as a sign of respect to hacking tradition since phone phreaking, which is one of the earliest means of stealing personal information via telephone lines, is considered to be the initial form of hacking (Lynch, 2005; Jaishankar, 2008). Phishing can be conducted via unsolicited emails conveying socially engineered messages to coerce Internet users into yielding personal information or bogus websites mimicking reputable traders.

There can be found many different definitions of the phishing in the literature. When these definitions are examined it can be observed that whereas the aim, which is the theft of personal and financial information, is quite common; the means of achieving deception and identity theft differ. On the one hand, some phishing definitions (Arachchilage and Love, 2014; Yeboah-Boateng and Amanor, 2014; Arachchilage et al., 2016) attribute the success of phishing attacks to the skilful use of social engineering attacks, where socially tailored messages exploit human weaknesses. For instance, Khonji et al. (2013, p. 2092) defines

phishing as “a type of computer attack that communicates socially engineered messages to humans via electronic communication channels in order to persuade them to perform certain actions for the attacker’s benefit.”

On the other hand, some other definitions (Qi and Yang, 2006; Whittaker et al., 2010) perceive the ability of electronic communications to acquire personal information as a source of success. For instance, Myers (2007, p. 1) defines phishing attacks as “attempts to fraudulently retrieve legitimate users’ confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organisation in an automated fashion”.

Technical subterfuge, which is highlighted in phishing most definitions, is another aspect of phishing attempts. Almomani et al. (2013, p. 2070) define phishing attempts as the schemes that “rely on malicious code or malware after users click on a link embedded in the email”. This kind of attack mainly depends on the ability of the malicious code to exploit the security deficiencies of targeted computers. As can be seen, all these definitions stress various aspects of phishing attacks. The Anti-Phishing Working Group (APWG) provides a more comprehensive definition of identity theft stressing both sociological and technical aspects of phishing. APWG defines phishing as “a criminal mechanism employing both social engineering and technical subterfuge to steal consumers’ identity data and financial account credentials” (APWG Report, 2017).

Phishing studies researching the susceptibility of Internet users indicate that urgency cues and fear appeals are utilised to exploit weaknesses in individuals’ decision-making systems (Wang et al., 2012; Chen et al., 2017). Urgency cues are messages indicating scarcity, time limitation or a warning aim to coerce receivers to focus on the urgency conveying messages to elicit their compliance (Vishwanath et al., 2011). Fear appeals are the online communications informing receivers about an imminent threat or a significant problem besides

providing a solution to overcome the mentioned problem (Witte, 1992). The disproportionate focus on urgency cues and anxiety provoked by fear appeals have been found to lead email users to make spurious decisions based on heuristic decision-making process rather than systematic decision making-system (Luo et al., 2013).

Failure to capture the impact of social vulnerabilities on Internet users' decision making-system when they are exposed to an email phishing attempt is one of the shortcomings of previous phishing studies. This shortcoming of extant research will be addressed in this thesis through an examination of victimisation processes of email users. Lack of empirical research on the antecedents of website phishing is another limitation of past phishing studies. Although an increasing number of phishing websites threatens online commerce (GlobalSign, 2017; Palmer, 2017), there is a dearth of empirical research on the factors leading Internet users to be a victim of website phishing. Much of the empirical research is directed on providing technical solutions to fake website detection (i.e. Zahedi et al., 2015; Jain and Gupta, 2017; Rao et al., 2018). A small body of consumer fraud victimisation indicates purchasing from non-secure websites as a risk factor for consumer fraud victimisation (Reisig and Holtfreter, 2013; van Wilsem, 2013a). However, these studies failed to account for the factors facilitating website phishing victimisation. This thesis, therefore, aims to discern factors rendering Internet users susceptible to website phishing.

### 1.3.2 Hacking

Hacking is unauthorised access to computers or computer systems with the aim of damaging, altering or stealing data (Wall, 2001). Hackers utilise both technical subterfuge like malware infection or social engineering to access the target computer systems (Hutchings, 2013; Reyns and Henson, 2016). Although the initial hackers were motivated by more naïve ends like curiosity or finding out the deficiencies in computer systems to perfect them, the

recent hackers have been motivated by more criminal intent such as financial gain or terrorism (Holt, 2007; Choi, 2008; Koops, 2010). Wall (2015) explains this shift in hacker stereotype with the increased commercialisation of the Internet and the myriad opportunities arising from this application of the Internet.

Cybercrime victimisation studies (Bossler and Holt, 2009; Holt and Copes, 2010; van Wilsem, 2013b; Reyns, 2015; Leukfeldt and Yar, 2016) researched the antecedents of becoming a hacking victim. The results of these empirical studies suggested participating in online forums, sharing personal information on social media, pirating media and accessing adult content as a risk factor for hacking victimisation. Additionally, the relationships between hacking and online harassment (van Wilsem, 2013b), identity theft (Reyns and Henson, 2016) and malware infection (Chu et al., 2012) have been researched. The results of these studies indicate a mutual relationship between hacking victimisation and these forms of cybercrime victimisation.

### 1.3.3 Malware Infection

Perpetrators utilise malware infection either to acquire personal information or to harm targeted computer systems (Holt and Bossler, 2013). According to a recent Internet security report, 1 in every 3,207 emails contained malware. Moreover, 7.8% of emails contained malicious URLs used to divert Internet users into bogus websites in 2018 (Symantec, 2019). The word malware is the combination of the words malicious and software, which encompasses keyloggers[7], computer viruses and other types of malicious codes (Ena, 2008). Malware can be disseminated through infected files, programs or websites (Choi, 2008; Bossler and Holt, 2009). The main difference between malware infection and phishing is their modus operandi.

[7] Keylogger can software or hardware that is utilised to capture key strokes to retrieve Internet users' personal information.

While malware infection occurs through digital means, phishing may happen both through social engineering and technical means (Jansen and Leukfeldt, 2015).

Malware infection may also be utilised to conduct scareware attacks. Scareware is also a malicious software aimed to coerce Internet users to either purchase fake security software or pay some money to get rid of the threat displayed on a computer screen (Halgas, 2016). Scareware is successful in exploiting vulnerabilities that arose from the lack of Internet skills (Shahzad and Lavesson, 2011).

Malware infection is found to be associated with various forms of cybercrime victimisation. The results of the past empirical research indicate that malware infection is the precursor of online identity theft (Holt and Turner, 2012; Paek and Nalla, 2015), online banking fraud (Jansen and Leukfeldt, 2015, 2016) and hacking (Chu et al., 2012). The results of these studies suggest that malware infection facilitates cybercrime victimisation.

## 1.4 Synopsis of Cybercrime Victimisation Literature

### 1.4.1 Development of Victimology

Though criminologists' interest in discerning the causes of crime dates to the early works of Lombroso at the end of eighteen-century (Becker and Wetzell, 2006), scholars' focus on victims and victimisation is relatively recent (Sparks, 1982). Thus, it may be suggested that victimisation as a concept is understudied and victims of crime are largely neglected (Walklate, 2012). Initial victimisation studies focused on discerning the roles of victims in the occurrence of victimisation and creating a typology of victims in 1940s (Eigenberg and Garland, 2008). Von Hentig (1941, p. 303) who examines the relationship between victims and perpetrators propose that there are "born victims, self-harming and self-destroying through the medium of a pliable outsider Later Von Hentig (1948) created a victim typology categorising individuals

into risk groups based on their biological, social and psychological attributes (Meier and Miethe, 1993). Thus, he aimed to distinguish groups who are prone to victimisation. Mendelsohn (1968) is known as one of the founders of victimology since he is the first to use the term victimology at a conference held in Bucharest in 1947 (Wilson, 2009). Mendelsohn (1968) created another typology of victims based on their culpability in occurrence the offences (Miers, 1989). Mendelsohn (1968) offered a spectrum of victim typology ranging from the completely innocent victim to the most guilty and imaginary victim (Daigle, 2017). Schafer (1968) is another scholar who proposed a typology of victims. He categorised victims' according to their responsibilities in the occurrence of victimisation. Schafer (1968) argues that victims have functional responsibility for both abstaining from provoking offenders and protecting themselves actively (Quinney, 1972). Table 1.2 summarises the categorisation of the initial victimologists, who are a group of theorists embracing theoretical assumptions around victimology.

Table 1.2
*Summary of Victim Typologies*

| | **von Hengtig (1948)** | **Mendelsohn (1968)** | **Schafer (1968)** |
|---|---|---|---|
| **Criteria** | Being Prone to Victimisation | Culpability of Victim | Functional Responsibility |
| **Typology** | a) Young<br>b)Female<br>c) Old<br>d) Immigrant<br>e) Depressed<br>f) Mentally defective or deranged<br>g) The acquisitive<br>h) Dull normal<br>i) Minority<br>j) Wanton<br>k) The lonesome and heartbroken<br>l) Tormentor<br>m) The blocked, exempted, and fighting | a) Completely innocent victim<br>b) Victim with minor guilt<br>c) Victim as guilty as offender or a voluntary victim<br>d) Victim more guilty than offender<br>e) Most guilty victim<br>f) Simulating or imaginary victim | a) Unrelated victims—no responsibility<br>b) Provocative victims—share responsibility<br>c) Precipitative victims—some degree of victim responsibility<br>d) Biologically weak victims—no responsibility<br>e) Socially weak victims—no responsibility<br>f) Self-victimizing—total responsibility<br>g) Political victims—no responsibility |

### 1.4.2 Shared Responsibility

Initial academic works aiming to create victim typologies based on the victims' role in the occurrence of crime events gave rise to two contested concepts: victim precipitation and victim facilitation. It is (Wolfgang, 1957, 1958) who introduced the term victim precipitation to denote the extent to which a victim contributes to the occurrence of a crime (Meier and Miethe, 1993). Wolfgang (1957, p. 2) argues that "the role of the victim is characterised by his having been the first in the homicide drama to use a physical force directed against his subsequent slayer". Thus, in some cases, it is the victim who initiated his/her ensuing homicide victimisation. Amir (1971) is another scholar who put undue responsibility and culpability onto victims on crime. Based on empirical research on rape incidents, he asserted that 19% of forcible rape victims somehow precipitated their victimisation (Timmer and Norman, 1984; Koss and Dinero, 1989). Amir (1971) argues that offenders' interpretations of victims' attitudes, clothing or "bad" reputation is more important than victims' actual behaviours for the occurrence of a victimisation event (Berger and Searles, 1985). He also proposes that the lack of significant protest against the offenders' actions may also be interpreted as the presence of consent (Miethe, 1985; Muehlenhard and MacNaughton, 1988). Amir's (1971) assertions rightfully received criticism not only for blaming rape victims and justifying offenders' actions to some extent but also for the methodological pitfalls in reaching the conclusions (Koss and Dinero, 1989). Though he utilised police reports in his analysis and did not conduct any interviews with victims of crime, he asserted a broadly generalised relationship between victims' behaviours and being a victim of rape (Fattah, 1979).

It worth noting a conceptual difference between the initial conceptualisation of victim precipitation provided by Wolfgang (1957) who conceive the victim as the initiator of the crime events, and Amir's (1971) suggestion of victim involvement at any phase of a crime event.

Wolfgang (1957) argued that victims precipitate their victimisation by conducting initial assault; however, contemporary scholars argue that victim precipitation may happen at any phase of victimisation (Eigenberg and Garland, 2008).

Victim facilitation is another concept that puts the onus of victimisation on victims to some extent. Victim facilitation denotes victims' inadvertent contributions to the occurrence of crime events (van Wyk and Benson, 1997). It may be perceived "as a catalyst in a chemical reaction that, given the right ingredients and conditions, speeds up the interaction" (Karmen, 2012, p. 124). In that sense, the concept of victim facilitation affixes less responsibility to victims when compared to victim precipitation (Daigle, 2017). Victim facilitation is more echoed in victimisation studies utilising opportunity theories of victimisation as a theoretical framework (Timmer and Norman, 1984; Titus and Gover, 2001; Homant, 2010).

### 1.4.3 Victimhood

The preceding sections outlined the development of victimology; this section examines the concept of the victim, the term ascribed to individuals by either wider society or themselves. The word victim, which is the derivation of Latin word *victima,* meaning sacrificial animal, has changed its connotation in the course of the time (Van Dijk and Sarkeshikian, 2013). Today, the concept of victim encompasses a wide range of targets such as environment, household or individuals (Fisher and Reyns, 2009). This thesis limits the scope of the victimisation to crime victimisation.

Karmen (2012, p. 501) defines a victim as "a person who suffers physical, emotional, and/or financial harm because of illegal activity" and victimization as "an asymmetrical relationship that is abusive, painful, destructive, parasitical, and unfair." This definition of victim leaves out some elements such as the individuals' guilt or responsibility in the occurrence of crime event or the victimiser. Bayley (1991) argues that victims should be

innocent, and they must not contribute to their victimisation. For instance, a burglar who received harm as a result of his criminal attempt should not be considered as a victim. So, anyone who contributes to his/her victimisation may not be regarded as a victim. However, Fattah (2003, p. 763) criticizes such approaches taken against the groups what he names as "socially expendable" groups including ethnic, religious or sexual minorities and prisoners as well as dissidents and troublemakers in totalitarian societies. He argues that member of these groups might not receive the victim status and the pity or sympathy of society due to their beliefs, lifestyles or political stances.

Kauzlarich et al. (2001, p. 176) define victims from radical victimology aspect as "individuals or groups of individuals who have experienced economic, cultural, or physical harm, pain, exclusion, or exploitation because of tacit or explicit state actions or policies which violate the law or generally defined human rights." As can be seen, the role of the state and its policies in the formation of the victim are stressed more than setting the criteria that shape the concept of victim or victimhood.

Feminist victimology, which is affected victim-blaming discourse, perceives victimhood as acceptance of individual responsibility in the commission of the crime events especially in the cases of women battering and rape (Convery, 2006; Cunniff Gilson, 2016). Acceptance of victim status is seen as defying innocence of individuals receiving harm from third parties. Lamb (1999, p. 109) proposes that an alternative version of the victim definition should be "the one that recognizes agency as well as passivity, strength as well as vulnerability, resistance as well as dissociation." In this vein, feminist scholars generally prefer the term survivor in favour of the victim as while the term victim connotes permanent injury (Armstrong, 1987), weakness, passivity and vulnerability (Phillips, 2000), the word survivor encompasses active confronting strategies, strength and agency (Dunn, 2005; Stringer, 2014).

Barry (1984, pp. 46-7) asserts that "surviving is the other side of being a victim. It involves will, action, initiative on the victim's part."

In response to these discourses about the definitions of the victim, constructivist victimology argues that being a victim is a socially constructed status, which is formed through the intersection of several factors such as the culture, law and self-identity (Dunn, 2008). (Strobl, 2004, 2010) proposes five *universal* criteria for the victimological concept of the victim:

(1) Identifiable single event: This criterion leaves out the situations where individuals claim themselves as the victim of factors such as globalization or climate change.

(2) Negative evaluation: Individuals should perceive their experiences as something negative with regard to the harm they received to be considered a victim.

(3) Uncontrollable event: The victim should not be responsible for the occurrence of the event lead to harm.

(4) Attribution to a personal or social offender: This criterion again excludes the events like natural disasters. The victimiser should be a human actor.

(5) Violation of socially shared norm: This criterion highlights the social acceptance of violation. So, any harm that is not socially accepted may not lead to assigning victim status to a person.

Labelling or assigning victim status is viewed as a social process where the individual who received the harm and the wider society interacts (Holstein and Miller, 1990; Miers, 1990). Both individuals who suffered harm or injury and society should identify him/her as a victim to be labelled or called as a victim. The harm experienced by individuals should comply with the norms of society. Strobl (2010, p. 6) names this status as "actual victim" who are more likely to receive public sympathy and special treatment (Convery, 2006). Acceptance of victim

identity or status may also empower individuals to take actions both to overcome adverse psychological and social outcomes in the aftermath of victimisation and pursue legal procedures to draw the attention of criminal justice system (Dunn, 2008). In sum, construed victim identity is the outcome of the assessment and the interpretation of the meaning of harm received in the broader context of specific society (Zaykowski, 2015).

However, some individuals deny the status of the victim as they attach negative connotations, such as being perceived as helpless or weak (Leisenring, 2006). Spalek (2016, p. 10) argues that "If the stereotype of the victim as "passive" and "helpless" is perpetuated in dominant representations of victimhood, during a time when individual strength is valued in society, then both males and females may increasingly refuse to situate themselves in terms of victimhood."

Miers (1990) argues that the harm received is the precondition of victimisation. This doctoral research set the financial loss experienced as a recruiting criterion. Internet users' who experienced financial loss as a consequence of online actions were considered to be potential participants. However, the harm received may not be limited to financial loss. Non-financial harms such as emotional effects of victimisation experiences might have also rendered Internet users' as victims of economic cybercrime. Thus, the semi-structured interview guide included questions exploring participants perceptions of naming their negative experiences as victimisation.

### 1.4.4 Opportunity Theories of Victimisation

Opportunity theories of victimisation are a series of victimisation theories rooted in works of Hindelang et al. (1978) and Cohen and Felson (1979). Lifestyle-Exposure Theory (Hindelang et al., 1978), Routine Activities Theory (Cohen and Felson, 1979), The Opportunity Model of Predatory Victimisation (Cohen et al., 1981) and Structural-Choice Theory of

Victimisation (Miethe and Meier, 1990, 1994) are generally named as opportunity theories of victimisation due to their focus on criminal structural opportunities created by people's lifestyles and routine activities (Maxfield, 1987; Meier and Miethe, 1993; Miethe and McDowall, 1993).

Lifestyle-Exposure Theory (LET) is one of the first systematic attempts to explain the causes of victimisation (Maxfield, 1987; Meier and Miethe, 1993). This theory was proposed to explain and understand violent victimisation across demographic strata of the population. The central premise of LET is that individuals' lifestyles increase the risk of being victimised by exposing them to potential offenders (Hindelang et al., 1978). Similarly, Routine Activities Theory (RAT) proposes that individuals' routine activities create opportunities for the commission of a crime (Cohen and Felson, 1979). A crime occurs when a suitable target, motivated offender converges in the absence of a guardian capable of deterring the threat (Cohen and Felson, 1979). These two theories and other variations of these opportunity theories of victimisation implicitly propose that individuals facilitate their victimisation.

### 1.4.5 Correlates of Cybercrime Victimisation

Though still in its infancy, the last decade has seen a proliferation of interest in cybercrime victimisation (Holt and Bossler, 2016; Stalans and Finn, 2016). Besides theoretical and conceptual works of (Grabosky, 2001; Levi, 2001; Castells, 2002; Newman and Clarke, 2003; Yar, 2005; Wall, 2007), which provided an invaluable framework for our greater understanding of cybercrime and cyberspace, a growing body of empirical attempts have been made to discern the correlates of cybercrime victimisation. Online correlates of *malware infection* (Bossler and Holt, 2009; Holt and Bossler, 2013; Leukfeldt, 2015), *phishing victimisation* (Hutchings and Hayes, 2008; Leukfeldt, 2014), *online identity theft victimisation* (Paek and Nalla, 2015; Williams, 2015), *online harassment victimisation* (Marcum et al., 2010;

Marcum, 2011; Reyns et al., 2011; Reyns et al., 2016), *hacking victimisation* (Choi, 2008; Choi et al., 2016) *multiple forms of cybercrime victimisation* (Ngo and Paternoster, 2011; van Wilsem, 2013b; Reyns et al., 2015) *and online fraud victimisation* (Pratt et al., 2010; van Wilsem, 2013a; Policastro and Payne, 2014) have been researched.

#### 1.4.5.1 Online Activities

As it was noted above, opportunity theories of victimisation assumed individuals' lifestyles and routine activities as risk-enhancing factors for traditional crimes. Cybercrime studies researching the impact of normal or legitimate online activities on the risk of victimisation have found that online shopping (Marcum et al., 2010; Pratt et al., 2010; Reyns, 2013), Internet banking (Hutchings and Hayes, 2008; Reyns, 2013, 2015) and online social activities (i.e. using chatrooms, visiting Internet forums) (Marcum et al., 2010; van Wilsem, 2011, 2013b) were associated with cybercrime victimisation.

Besides legitimate online activities, a number of empirical studies reported deviant online activities as a risk factor for cybercrime victimisation. Prior to presenting the results of empirical research, a definition of cyber-deviance will be provided. Providing a standard definition of deviancy and accounting for the causes of deviant behaviour is one of the most contested issues in criminological history (Gottfredson and Hirschi, 1990; Holt and Bossler, 2008). Approaches aiming to define deviance may be categorised into two general groups: absolutist perspective and (objectivist position) sociological perspective (Goode, 2015). The absolutist perspective presumes the existence of higher authorities that set unalterable moral standards to be complied with (Little, 2007). This aspect of deviance conceives deviance as a dichotomous phenomenon like good and bad since the absolute standards are introduced by the law of nature or God (Hills, 1977; Perrin, 2001). The advocates of the objectivist position of deviance assume that deviance is socially constructed; thus it is highly subjective and displays

changes over different cultures, times and places (Melossi, 1994; Bereska, 2013).

Cybercrime literature is also been interested in defining cyber deviance (Holt and Bossler, 2016). Online deviance or cyber-deviance is defined as "a transcendence of rules, values or morals set out by a particular community" (Williams, 2000, p. 97) or "behaviour that may not be illegal, but violates norms and beliefs of the larger culture" (Holt and Bossler, 2016, p. 7).

Operationalisation of deviance is another significant issue. Studies researching traditional crimes conceptualised illicit drug use, excessive alcohol consumption and delinquent peer involvement as deviant behaviours (Finkelhor and Asdigian, 1996; Osgood et al., 1996; Lanier and Henry, 1998; Mustaine and Tewksbury, 1998; Vazsonyi et al., 2002). Cybercrime literature also tends to label some online activities transcending values of the online community as deviant. Viewing or downloading online pornography (Hox and Boeije, 2005; Bossler and Holt, 2010; Ngo and Paternoster, 2011; Wall, 2017), pirating and sharing pirated media (Bossler and Holt, 2010; Ngo and Paternoster, 2011; Donner et al., 2014; David, 2017), hacking (Bossler and Holt, 2010; Ngo and Paternoster, 2011; Donner et al., 2014), free streaming (Birmingham and David, 2011; Kirton and David, 2013; Pursiainen, 2016; Wong, 2016) and downloading software illegally (Donner et al., 2014; Paek and Nalla, 2015) were assumed as deviant or illegal online behaviours in cybercrime studies.

With regard to the impact of engaging with online deviance and on the risk of victimisation, the results of empirical studies suggested an association between online deviant activities and the risk of experiencing cybercrime victimisation. For instance, recent evidence suggests accessing adult content or engaging with digital piracy as a significant antecedent of becoming a victim of malware infection (Bossler and Holt, 2009; Holt and Bossler, 2013). Opening unknown email attachments or downloading free games was found to be associated

with increased risk of online identity theft victimisation (Ngo and Paternoster, 2011; Reyns, 2013).

#### 1.4.5.2 Demographics of Internet Users

Opportunity theories of victimisation assumed that demographic characteristics of individuals have an effect on the chances of being a victim through influencing individuals' behaviours (Hindelang et al., 1978). Cybercrime studies utilising opportunity theories of victimisation as a theoretical framework have researched the effect of demographics (i.e. age, gender, education level and annual household income) on the risk of experiencing cybercrime victimisation. The results of empirical studies generally suggested being young (Pratt et al., 2010; Ngo and Paternoster, 2011; Paek and Nalla, 2015; Choi et al., 2016; Leukfeldt and Yar, 2016) and female increased the odds of facing cybercrime victimisation (Bossler and Holt, 2009; Holt and Bossler, 2013; Choi et al., 2016). Previous research also indicated that Internet users with higher education levels were more likely to be a victim of cybercrime (Pratt et al., 2010; van Wilsem, 2011, 2013a, 2013b; Paek and Nalla, 2015). Likewise, annual household income was also associated with an increased risk of victimisation Empirical evidence suggested that Internet users' with higher annual household income were more likely to be a victim of cybercrime (Pratt et al., 2010; van Wilsem, 2011, 2013a, 2013b; Paek and Nalla, 2015).

### 1.4.6 Consequences of Cybercrime Victimisation

Emotional reactions and behavioural responses are two significant adverse outcomes of victimisation experiences (Yin, 1980; Skogan, 1986).

#### 1.4.6.1 Emotional Reactions

Fear of crime, "an emotional response to a danger or threat of an actual or potential criminal incident" (Henson and Reyns, 2015, p. 92), is one of the most significant adverse psychological outcomes of victimisation experiences. It is argued that factors having an impact on the presence of fear of crime can be summarised into three groups as demographic characteristics (gender and age), social determinants (direct and indirect victimisation experiences) and psychological factors (perceived risk and perceived severity) (Yin, 1980; Skogan, 1986).

Fear of traditional crime studies suggested the prevalence of fear of crime among females (Warr, 2000; May et al., 2010; van Eijk, 2017). Fear of cybercrime studies yielded inconsistent results with regard to the presence of gender differences in fear of cybercrime. Research on fear of online interpersonal cybercrime (i.e. cyberstalking or cyberbullying) suggested female Internet users were more fearful when compared to male Internet users (Henson et al., 2013; Pereira et al., 2016; Virtanen, 2017). However, there seem to be no gender differences for malware infection or online identity theft (Roberts et al., 2013; Yu, 2014). Age is another demographic characteristic that is found to be associated with fear of crime. Fear of crime literature assumed older people as being more fearful than younger individuals' due to their physical vulnerability to thwart an attack (Ortega and Myles, 1987; Moore and Shepherd, 2006). Fear of cybercrime studies suggested no age differences in fear of cybercrime (Henson et al., 2013; Roberts et al., 2013; Yu, 2014).

Previous victimisation experience (direct victimisation experience) and interactions about crime events (indirect victimisation experiences), which are conceptualised as social determinants of fear of crime (Yin, 1980), have found to foster fear of traditional crime (Silverman and Kennedy, 1985; Russo and Roccato, 2010; Sironi and Bonazzi, 2016).

Likewise, cybercrime studies indicated an association between prior cybercrime experience, interactions about cybercrime such as media news related to notorious cybercrime incidents and fear of cybercrime (Alshalan, 2006; Henson et al., 2013; Yu, 2014).

Psychological factors, perceived risk and perceived severity, were also assumed to be antecedents of fear of crime (Ferraro and Grange, 1987; Vitelli and Endler, 1993). Although initial fear of crime studies conceptualised fear of crime as one concept, recent fear of crime literature tends to examine fear of crime and perceived risk of victimisation separately (Ferraro, 1995; Rountree and Land, 1996; Rengifo and Bolton, 2012). It is argued that the perceived risk of victimisation is a cognitive process where the likelihood of becoming a victim is evaluated (LaGrange et al., 1992). However, fear of crime is a set of emotional reactions to prior criminal victimisation or indirect experiences (LaGrange and Ferraro, 1989). Nonetheless, empirical research has illustrated the interconnectedness of these two concepts (Kanan and Pruitt, 2002; Cook and Fox, 2011). It is suggested that perceived risk and perceived severity of victimisation exacerbate fear of crime (Rader, 2004; Wyant, 2008).

Emotional responses to victimisation experiences are not limited to fear of crime. Research on white collar crime suggests anger, anxiety and depressive disorder as the psychological outcomes of fraud victimisation (Titus et al., 1995; Piquero et al., 2007). It is argued that anger is more prevalent than fear of crime (Ditton et al., 1999). Cybercrime victimisation studies also indicate annoyance and stress as the feelings experienced in the aftermath of cyberstalking (Short et al., 2015), identity theft (Dinisman and Moroz, 2017) and cyberbullying (Dredge et al., 2014).

#### 1.4.6.2 Behavioural Responses

Cybercrime literature suggests that prior adverse online experiences cause changes in Internet users' online lifestyles and security intentions (Forsythe et al., 2006; Chang and Wu, 2012). Previous cybercrime victimisation studies have found that Internet users with high perceived risk and fear of crime were less likely to purchase goods online (Reisig et al., 2009; Henson et al., 2013). Internet security studies also indicate that prior adverse online experiences intensity security intentions. Internet users who felt vulnerable due to prior victimisation experiences preferred to install security software (Chen et al., 2016; Tsai et al., 2016) or tend to comply with password guidelines (Mwagwabi et al., 2014).

## 1.5 Research Aims, Objectives and Research Questions

The main aims of this thesis are to explore and examine the factors that facilitate the occurrence of economic cybercrime victimisation as well as to understand the impacts of economic cybercrime victimisation on individuals' behavioural and security adaptations. Previous cybercrime victimisation studies examined online correlates of some forms of economic cybercrime separately. For instance, credit card fraud victimisation (Bossler and Holt, 2010; Holtfreter et al., 2010) and online banking fraud victimisation (Jansen and Leukfeldt, 2015, 2016) have been researched separately. However, economic cybercrime victimisation has not been examined holistically. This thesis aims to examine and understand economic cybercrime victimisation process and how victimisation experiences influence Internet users' online lifestyles.

Previous cybercrime victimisation studies heavily focused on discerning the relationship between online lifestyles/online routine activities and the risk of cybercrime victimisation. Extant research was descriptive in nature. Hence, little is known about *why* and *how* some Internet users experienced victimisation and *why* some online activities are

associated with the risk of cybercrime victimisation. This gap in the literature may be the outcome of quantitatively driven research methodology of previous research. Mixed methods approach that harmonised quantitative and qualitative research methods in one single research was adapted to address this gap in the literature. The causes and impacts of economic cybercrime victimisation were examined through statistical analysis of Crime Survey for England and Wales (CSEW) (2014/2015) (Office for National Statistics, 2016a)and qualitative analysis of semi-structured interviews conducted with victims of economic cybercrime victims and non-victim control group participants. Police reports pertaining to economic cybercrime incidents happened in a Northeast city in 2015 were also included in the qualitative analysis.

Applicability of Lifestyle Routine Activities Theory (LRAT) as a theoretical framework to cybercrime studies is a highly contested debate (Ngo and Paternoster, 2011; Holt and Bossler, 2014). LRAT, which is the latest model of opportunity theories of victimisation, was originally proposed to account for the victimisation in the physical world. This theory has increasingly been utilised to examine the causes of cybercrime victimisation. Empirical studies yielded controversial results about the applicability of LRAT to cybercrime. Whereas the results of (Choi, 2008; Reyns et al., 2011; Reyns et al., 2016) yielded support, the results of (Bossler and Holt, 2009; Marcum et al., 2010; Holt and Bossler, 2013; van Wilsem, 2013b; Leukfeldt and Yar, 2016) suggested partial support. Yet, (Ngo and Paternoster, 2011) and (Policastro and Payne, 2014) found no empirical support of the applicability of theory to cybercrime victimisation. Thus, testing applicability of LRAT to economic cybercrime victimisation is another aim of this thesis.

**Thesis Objectives;**

a) To explore factors that render some Internet users as targets of online attacks;
b) To examine the decision-making process of Internet users when they face an online threat;
c) To explore factors increasing the risk of being a victim of economic cybercrime;
d) To explore the impact of technological vulnerabilities on the risk of becoming a victim of economic cybercrime;
e) To identify and understand the emotional and behavioural impacts of economic cybercrime victimisation on individuals' online lifestyles;
f) To test the applicability of LRAT as a theoretical framework to economic cybercrime victimisation and address the theoretical shortcomings of LRAT in economic cybercrime victimisation context.

**Thesis Research Questions;**

**Central research question**

What are the factors that facilitate economic cybercrime victimisation at the individual level in the UK?

**Research question 1**

What are the factors renders Internet users susceptible to be the target of an online attack?

**Research question 2**

What factors affect Internet users' decision making-system when they face an online threat?

**Research question 3**

How technological vulnerabilities impact the chance of being a victim of economic cybercrime?

**Research question 4**

What are the emotional responses to economic cybercrime victimisation and how these emotional responses impact victims' behavioural and security intentions?

**Research question 5**

Can Lifestyle Routine Activities Theory provide a sound theoretical framework to explain the economic cybercrime victimisation in cyberspace?

## 1.6 Key Contributions and Implications

Discerning the factors facilitating cybercrime victimisation is a growing area of interest in the field of cyber criminology. Previous research examining the factors that render Internet users vulnerable to online threats mainly focused on the individual level factors. This doctoral research explored the impact of both individual and macro-level factors on the risk of experiencing economic cybercrime victimisation. While laptop computers used away from secure Internet connections, public access computers and free Wi-Fi connections emerged as technological vulnerabilities that enhanced the likelihood of victimisation, data breaches of large companies holding personal information of Internet users, security flaws of online shopping websites and mobile applications appeared as macro-level factors affecting the risk of victimisation. These findings offer some critical insight into criminological research examining the causes of cybercrime victimisation. First, this thesis illustrated that besides individual-level factors such as Internet users' online behaviours, macro-level factors might successfully be integrated into cybercrime victimisation models. Future cybercrime studies may explore the effect of macro variables like mobile application usage on the risk of cybercrime victimisation in depth. The Integrated Cyber Victimisation Model (ICVM), the novel and innovative contribution of this thesis, may serve as a base for future cybercrime victimisation studies while researching the impact of macro-level factors on the risk of

victimisation. Second, findings highlighting the role of macro-level factors in the occurrence of economic cybercrime victimisation shifts the onus of responsibility from Internet users to macro-level actors (governments, online traders or security companies) who are responsible for providing a safer online environment. These actors should devise effective policies to regulate cyberspace rather than labelling Internet users as the weakest chain in Internet security.

The findings of this research pertaining to the causes of fear of economic cybercrime illustrated that although economic cybercrime victims experienced financial losses, the risk of possible misuse of personal information caused higher levels of fear of crime and concern when compared to direct financial loss. Perceived severity of potential misuse of personal and financial information seemed to modify behavioural and psychological responses to economic cybercrime victimisation. This finding provides an opportunity to challenge and advance our understanding of the causes of fear of cybercrime. Although extant research examines the impact of economic cybercrime in materialistic means (amount of financial loss), the results of this thesis suggest that non-materialistic harm should also be included in research exploring the cost of economic cybercrime. A more discourse analytic approach may be applied to understand how individuals form cybercrime victim identity

Research findings regarding the impact of economic cybercrime victimisation on behavioural and security adaptation suggested that older participants were more likely to adopt online avoidance behaviours such as stopping using online financial services than approach behaviours like applying safeguarding measures to tackle with adverse effects of the victimisation experiences. Application of online avoidance behaviours appeared to have negative impacts on the quality of lives of older participants who were living alone. Low Internet self-efficacy seemed to affect Internet users' adaptation decisions. This finding stresses the need for educational programs aiming to increase the Internet skills of older Internet users.

Older Internet users should be informed about possible online threats and how to deal with those online threats. Future fear of cybercrime victimisation may explore age differences in behavioural and security adaptations of Internet users.

Password fatigue emerged as one of the reasons for becoming a hacking victim. Participants who used the same passwords for different online accounts appeared to be more likely to be a victim of economic cybercrime through hacking of financial and personal accounts. Many online platforms require Internet users to create online accounts, which are associated with passwords. Interviews suggested that most of the participants experienced difficulties in managing user names and passwords. Administrators of online platforms might consider applying biometric recognition systems as a means of authentication to prevent the risks posed by password fatigue.

## 1.7 Engaging with Cybercrime and Cyber Victimology

I had worked as a law enforcement officer as a member of Turkish Gendarmerie General Command for twelve years before beginning my postgraduate education at Durham University. Turkish Gendarmerie, which is a police force with military status in Turkey, is responsible for maintaining public order, safety and security in mostly rural areas. Crime prevention and executing judicial services are two major duties of Turkish Gendarmerie General Command. I had dealt with several types of crimes ranging from organised crimes to burglary; however; economic cybercrime cases were the hardest ones to deal with. This difficulty mainly arose from the lack of expertise and coordination between bodies responsible for policing online economic crimes. I always felt uneasy with the fact that most of the cyber perpetrators could not be prosecuted. These conditions made me apply for a postgraduate programme in Criminology. While doing my master's degree at Durham University, I had the opportunity to read cybercrime literature and thanks to Professor David Wall and Professor

Maggie O'Neil's inspiring ideas about cybercrime and criminological research, I decided to apply for a post as a PhD student at Durham University.

My Master's Degree dissertation was about Card-not-present Fraud Victimisation in the UK. The dissertation process enabled me to engage with cybercrime literature in depth. My Master's dissertation and the initial literature review conducted during my PhD research indicated that economic cybercrime victimisation is a significant issue, which has numerous adverse impacts on individuals. Since the majority of cybercrime studies were quantitatively driven, the voices of victims were not echoed in their results. These factors lead me to conduct mixed-methods research examining the economic cybercrime victimisation process and understand the impacts of victimisation on victims' online lifestyles.

## 1.8 The structure of the Thesis

This thesis is divided into three parts which are composed of ten chapters including this Introduction Chapter. The first part of the thesis aims to illustrate the significance of research and provide background information to research questions. This part consists of the Introduction Chapter, two Literature Review Chapters and Methodology Chapter. The second part of the thesis presents the results of the Quantitative analysis of CSEW 2014/2105 and findings of the qualitative analysis. This part is comprised of one quantitative results chapter and three qualitative findings chapters. The last part of the thesis discusses the results and findings of this thesis.

Chapter Two presents a theoretical and conceptual framework utilised in this thesis to address research questions. The chapter starts with presenting the historical evolution of Lifestyle Routine Activities Theory (LRAT). It then goes on discussing the conceptual shortcomings of transposition of LRAT to cybercrime environment before outlining the

empirical evidence about the applicability of LRAT to cybercrime. It finishes with reviewing the empirical studies researching behavioural and emotional impacts of cybercrime victimisation. This section of the chapter also presents two other conceptual frameworks, Protection Motivation Theory and Coping Strategies that will be utilised while examining the decision-making process of Internet users when they face an online threat and effects of victimisation experiences on Internet users' online lifestyles.

Chapter Three is the second literature review chapter. This chapter reviews the results of previous cybercrime victimisation studies. The chapter initiates with presenting controversies in cybercrime literature and then continues to review the results of relevant empirical studies.

Chapter Four is the Methodology Chapter. This chapter illustrates the research design and methodology utilised to address the research questions. The chapter begins by providing a rationale for utilising a mixed-methods research paradigm while examining the correlates and impacts of economic cybercrime victimisation at the individual level in the UK. The chapter then explains the design of the quantitative and qualitative phases of research. The chapter concludes by providing a reflexive account of the research process.

Chapter Five is the first empirical chapter. This chapter presents and discusses the results of a quantitative analysis of CSEW 2014/2015. The chapter initially provides descriptive statistics of variables used in statistical analysis. After providing an overview of variables, bivariate and multivariate analysis results aiming to discern online correlates of economic cybercrime victimisation are presented. The applicability of LRAT to economic cybercrime victimisation is also tested in this section of the chapter. The chapter concludes with demonstrating analysis results exploring the impacts of technological vulnerabilities on the risk of economic cybercrime victimisation.

Chapter Six, which is the second empirical chapter, is the first qualitative findings chapter. This chapter illustrates the factors that render Internet users a target of an online attack. While the first section of the chapter presents the determinants of being a target of phishing attempts, the second part of the chapter illustrates the causes of being a target of hacking attacks.

Chapter Seven is the second qualitative findings chapter. This chapter examines the factors leading to economic cybercrime victimisation. The first part of the chapter examines the factors impacting Internet users' decision-making process when they face an online threat. The findings suggest possible causes of email phishing and website phishing victimisation are presented in this section. The second part of the chapter examines the impact of contextual vulnerabilities on the chance of being a victim of economic cybercrime. The last part of the chapter illustrates the findings pertaining to testing applicability of LRAT to economic cybercrime victimisation.

Chapter Eight is the last qualitative findings chapter. This chapter displays findings pertaining to the impacts of economic cybercrime faced in the aftermath of victimisation experiences. Whereas the first section of the chapter presents findings related to adverse psychological effects of victimisation experiences, the second section of the chapter provides the effects of victimisation experiences on Internet users' behavioural adaptations.

Chapter Nine is the Discussion Chapter. This chapter blends and discusses the quantitative analysis results and qualitative findings to explore factors leading to economic cybercrime victimisation and understand impacts of victimisation on individuals' online lifestyles.

Chapter Ten is the Conclusion Chapter. This chapter draws the findings of this thesis together and presents a contextual vulnerability approach, which is one of the original

contributions of this thesis. It then goes on to explain the Integrated Cyber Victimisation Model proposed by the thesis to address the theoretical shortcomings of LRAT. The penultimate section discusses the novel contribution of this thesis to our understanding of economic cybercrime victimisation. It then goes on discussing implications of the findings for policy making and governance of the Internet. The last section of the chapter presents the limitations of this doctoral thesis and provides recommendations for future research.

# Chapter 2 Theoretical Framework

## 2.1 Introduction

This first literature review chapter provides an overview of the theoretical and conceptual frameworks that informed the research design of this doctoral thesis. This chapter is composed of four sections. The first section of the chapter introduces opportunities theory of victimisation. This first section deals with a historical account of the development of Lifestyle Routine Activities Theory (LRAT). LRAT is the last version of the theories, which are known as opportunity theories of victimisation (Miethe and Meier, 1990). This theory provides a systematic approach to examine the factors that create suitable conditions for the occurrence of a victimisation event (Wooldredge et al., 1992). The chapter then goes on to discuss the theoretical shortcomings of applying LRAT to cybercrime studies. LRAT was initially proposed to account for the victimisation in the physical world; however, during the last decade it has been increasingly applied as a theoretical framework in cybercrime studies. Due to the inherent complexities of cyberspace, the applicability of LRAT to cyberspace is questioned (Yar, 2005). This second section of the chapter will critically evaluate this highly contested debate in the literature. The penultimate section of the chapter introduces the Protection Motivation Theory (PMT). Rogers (1975) proposed PMT to evaluate individuals' behavioural reactions to fear-provoking messages. This thesis utilised the conceptual elements of PMT to examine economic cybercrime victims' decision-making processes when they experienced an online attack. This is one of the first applications of PMT in an economic cybercrime victimisation research. The last section of the chapter introduces Approach-Avoidance Paradigm (Lazarus and Folkman, 1984; Roth and Cohen, 1986), which was utilised a conceptual framework while examining the adverse impacts of economic cybercrime

victimisation on Internet users' behavioural adaptations and security intention. This use of Approach-avoidance paradigm was also one of the first applications of the theory in cybercrime victimisation literature.

## 2.2 Opportunity Theories of Victimisation

Lifestyle Exposure Theory (LET), and Routine Activities Theory (RAT) are two significant criminological theories that stimulated scholars' perspectives related to the occurrence of victimisation by shifting academic attention from the causes of offending behaviour to the criminal opportunities created by individuals' lifestyles and routine activities for the occurrence of a crime (Maxfield, 1987). Although opportunity theories of victimisation were initially proposed to account for predator victimisation such as burglary and theft, these theories have been applied as a theoretical framework to research other types of offences as well. Risk of violent victimisation (Sampson and Wooldredge, 1987; Lauritsen et al., 1991; Miethe and Meier, 1994; Rountree et al., 1994; Pratt and Turanovic, 2016), burglary victimisation (Peguero and Popp, 2012; Ariel and Partridge, 2017), sexual harassment, sexual assault and rape (Tseloni et al., 2004; Tillyer and Eck, 2009; Quick et al., 2018), offending behaviour (Finkelhor and Asdigian, 1996; Madensen and Eck, 2008), deviant behaviour (Maume Jr, 1989; Osgood et al., 1996), child abuse and domestic violence (Mustaine and Tewksbury, 2002; Pauwels and Svensson, 2011; Maimon and Browning, 2012) and cybercrime (i.e. Holtfreter et al., 2008; Pratt et al., 2010; Holt and Bossler, 2013; Williams and Levi, 2015) are the example of application of opportunity theories of victimisation.

As noted earlier, opportunity theories of victimisation are a series of theories. Lifestyle Exposure Theory (LET), Routine Activities Theory (RAT), The Opportunity Model of Predatory Victimisation and Structural Choice Theory of Victimisation (LRAT) are the variations of opportunity theories of victimisation. The first part of this section introduces the

historical development of the aforementioned theories and the second part of the section present a critique of opportunity theories of victimisation.

### 2.2.1 Lifestyle Exposure Theory

LET is the first version of the opportunity theories of victimisation. LET posits that individuals' lifestyles and demographic characteristics influence the chances of becoming a victim (Hindelang et al., 1978). Lifestyle is defined as "routine daily activities, both vocational activities (e.g., work, school, keeping house) and leisure activities" (Hindelang et al., 1978, p. 613). LET proposes that role expectations which are heavily influenced by demographic characteristics affect individuals' lifestyles (Miethe and Meier, 1994). Age, marital status, family income, race and gender are demographics proposed to impact lifestyles via imposing constraints to individuals. Besides demographic characteristics, structural constraints, which can be financial, familial or educational, are also assumed to define individuals' lifestyles (Hindelang et al., 1978). Individuals acquire skills and behaviours through adaptation of both structural constraints and role expectations. These learnt attitudes and skills are later transformed into lifestyles (Hindelang et al., 1978).

Hindelang et al. (1978, p. 617) argue that variations in lifestyles impact the risk of exposure to offenders at particular times and places since "victimisation is not randomly distributed across time and space". It is proposed that victimisation occurs more frequently in public places at night. The more time spent outside of the home settings, the more likely individuals face victimisation due to an increased chance of interacting with offenders at risky places and risky times (Mustaine and Tewksbury, 2000b). For instance, the amount of time spent at public places at night increases the odds of interacting with would be offenders. It is suggested that young persons, single individuals, males and those with high-income levels are more likely to face victimisation as individuals with these demographic characteristics are more

likely to spend time away from household settings. Moreover, it is assumed that people share more time with those having similar demographic characteristics (Hindelang et al., 1978). Thus, shared demographic characteristics such as age, gender, ethnicity, family income and marital status increase the odds of victimisation due to peer involvement (Maxfield, 1987).

### 2.2.2 Routine Activities Theory

Routine Activities Theory (RAT) is another systematic approach aimed to account for victimisation. Cohen and Felson (1979) proposed RAT to explain these unexpected crime trends in the US after World War II. Official crime statistics pertaining to the period between 1960 and 1975 illustrated significant increases in the crime rates for robbery, rape, aggravated assault, homicide as well as property crimes in the US (Cohen and Felson, 1979). However, statistics related to the welfare of US citizens at this period displayed improvement in employment, education and family income rates. These discrepancies in statistics presented a sociological paradox since it was expected that increased prosperity would lead to decreased crime rates (Eck, 1995). It is argued that enhanced welfare changed individuals' daily routine activities, which in turn increased the criminal opportunity for the "direct-contact predatory violations", namely illegal actions against persons or properties with the intention of damaging them (Cohen and Felson, 1979, p. 589). Motivated offender, suitable target and absence of a capable guardianship are proposed to be three minimal elements of a crime. Should the temporal and spatial convergence of these elements be impeded, the occurrence of a crime would be prevented (Finkelhor and Asdigian, 1996). It is individuals' legal daily routine activities that prepare suitable conditions for the tempo-spatial convergence of these three minimal elements (Cohen and Felson, 1979).

Although RAT does not deny the significance of motivated offender, it presumes motivated offender as a given fact since RAT assumes that structural changes in routine

activities create opportunities for a crime regardless of changes in offending intention (McNeeley, 2015). Routine activities, which can be work, social interaction, leisure and childrearing, are defined as "any recurrent and prevalent activities which provide for basic population and individual needs, whatever their biological or cultural origins." (Cohen and Felson, 1979, p. 593). It is argued that these daily routine activities separate individuals from their safe home settings or leave their goods unguarded (Miethe et al., 1987). RAT emphasises the significance of the time of the daily routine activities for the temporal convergence of suitable target and motivated offender (Cohen and Felson, 1979). For instance, going out to bars at night both leave the houses unguarded and increase target suitability of individuals' by increasing their visibility and accessibility (Tewksbury and Mustaine, 2001).

### 2.2.3 The Opportunity Model of Predatory Victimisation

Cohen et al. (1981) later proposed a new version of RAT. This approach which is dubbed as "the opportunity model of predatory victimisation" (Cohen et al., 1981, p. 507) is considered as the subset of opportunity theories of victimisation since it synthesised the lifestyle concept of LET with three minimum crime elements of RAT (Sampson and Wooldredge, 1987). This new model was formed according to the outcomes of an empirical study aimed to build a bridge between demographic characteristics such as age, income and ethnicity and risk of experiencing predatory victimisation like burglary and theft (Cohen et al., 1981). This approach conceives five concepts, exposure, proximity to potential offenders, the attractiveness of suitable targets, guardianship and definitional properties of specific crimes, as the risk factors acting as mediating factors on the likelihood of occurrence of victimisation (Sampson, 1987).

Cohen et al. (1981) explicitly stated that this approach borrowed the lifestyle element of LET proposed by (Hindelang et al., 1978). Lifestyle is presented as the proxy of exposure

and guardianship in this model of victimisation. Exposure is defined as "visibility and accessibility of persons or objects to potential offenders" while proximity is explained as "physical distance" between individuals' residents and places where potential motivated offenders are found (Cohen et al., 1981, p. 507). It is argued that there is a positive relationship between exposure, proximity and risk of victimisation. The more individuals expose themselves through their activities which determine their lifestyles, the more likely they face victimisation (Cohen et al., 1981). People residing in close proximity to the population of offenders also increase the risk of victimisation by enabling potential offenders to acquire more information about their lifestyle patterns and security measures applied to protect their residents (Meier and Miethe, 1993). The target attractiveness concept encompasses two attributes: value and inertia of persons or objects. Persons or objects having more value and less inertia (less physical resistance like small weight or size) to potential attacks are hypothesised to be more attractive targets (Cohen et al, 1981). For instance, a mobile phone can be considered as a more attractive target when compared to a desktop computer or a TV due to its inertia, which means that it is less resistant to removal and easy to carry or hide.

Definitional properties of specific crimes denote attributes of that impose some limitations or present some difficulties for offenders to implement their criminal intentions (Cohen et al., 1981). The distinction between larceny and burglary regarding the difficulties they pose to potential offenders may be an example of this concept. Offenders require more information for the commission of burglary when compared to larceny. Hence, potential offenders who act rationally would seek less attractive targets should they have no substantial information about lucrative targets (Collins et al., 1987).

### 2.2.4 Structural-Choice Theory of Victimisation (Lifestyle Routine Activities Theory)

Miethe and Meier (1990) integrated three approaches of criminal opportunity (Lifestyle-exposure, Routine Activities Theory and Opportunity Model) into one single model what they called Structural-Choice Model. However, this approach is mostly referred to as Lifestyle Routine Activities Theory (LRAT) in the literature. Miethe and Meier (1990) simplified the elements of the theory to four concepts: proximity to motivated offenders, exposure to risky situations, target attractiveness and absence of capable guardianship. It is proposed that these four concepts are the necessary conditions for the occurrence of an offence. Thus, the absence of any of these elements would prevent victimisation (Sampson and Lauritsen, 1990).

The omission of definitional properties of specific crimes and classification of the conceptual elements as structural and choice components are two fundamental distinctions between Cohen et al.'s (1981) approach and Miethe and Meier's (1990) model. Miethe and Meier (1990) argue that individuals' lifestyles and daily routine activities create opportunity structure for criminal intention since persons' lifestyles and daily routine activities are proposed to increase their exposure to offenders at risky times and places. Miethe and Meier (1990) further posit that attractiveness of potential targets and degree of capable guardianship impact offenders' target selection decisions given that offenders act rationally. Thus, while proximity and exposure elements are conceptualised as opportunity structure component of the model, target attractiveness and absence of a capable guardianship are hypothesised as choice features of the model (Meier and Miethe, 1993).

### 2.2.5 Assessment of Theoretical Evolution of LRAT

LET and RAT are two cornerstone theories that provided the foundation for the criminal opportunity approach. Although there are some minor conceptual variations between these theories and following variations of these theories, it is generally proposed that LET and RAT are similar theories explaining the same phenomenon with different terminology (Maxfield, 1987; Meier and Miethe, 1993; Eck, 1995; Choi, 2008). Initially, these conceptual similarities and differences will be documented, and then integration of these concepts in the LRAT perspective will be evaluated.

The main similarity between these two theories is their victim centred opportunity perspectives related to the occurrence of a crime (Maxfield, 1987; Miethe and Meier, 1990; Meier and Miethe, 1993). Both theories propose that individuals' lifestyles and routine activities create opportunities for criminal victimisation. However, while LET put more emphasis on the role of demographic characteristics of individuals on the risk of victimisation, RAT highlights the significance of tempo-spatial convergence of three elements for the creation of criminal opportunity. Furthermore, both theories downplay offender motivation and focus on risk enhancing patterns of daily routine activities (Finkelhor and Asdigian, 1996; Mustaine and Tewksbury, 1998). It is argued that motivated offenders are always present. Thus, emphasis should be put on risk enhancing lifestyles, routine activities and demographic characteristics (Osgood et al., 1996). The assumption of the rationality of offenders while selecting their targets is another shared characteristic of these two theories (Clarke, 1995; Holtfreter et al., 2010). Rational offenders calculate the benefit and risk of their actions, and they may choose a less attractive target should they perceive the presence of a guardian capable of deterring the offence (Miethe and Meier, 1994).

One of the main differences between LET and RAT is their perception of the occurrence of victimisation. Whereas LET takes the risk posed by risky behaviours using drugs or peer involvement into account while assessing the probability of facing victimisation, RAT is more concerned with normal daily activities that lead the convergence of three minimum elements for the occurrence of victimisation (Pratt and Turanovic, 2016). Their assumption regarding the occurrence of crime is another important distinction between these two theories. LET is proposed to explain differential risks posed by individuals' lifestyles and demographic characteristics; however, RAT aims to account for the causes of changes in crime rates (Miethe and Meier, 1994).

#### 2.2.5.1 Transformation of Conceptual Elements of LRAT

As it is outlined above, LRAT is a product of a process starting with the introduction of LET. This section summarises the conceptual transformation of LRAT elements (Figure 2.1). The ideas presented in LET was groundbreaking since crime and victimisation were examined through offending intention prior to the introduction of LET (Eck, 1995; Tillyer and Eck, 2009; Pratt and Turanovic, 2016). RAT is generally perceived as the extension of LET as it borrowed routine activities concept from LET (Maxfield, 1987; Finkelhor and Asdigian, 1996). Cohen and Felson (1979) added a suitable target and absence of capable guardianship as the other criminal opportunity creating elements. They proposed that a suitable target has four attributes which are value, inertia, visibility and accessibility. Visibility and accessibility are seen as the function of routine activities since they increase the probability of intersecting with potential offenders at risky places and times. Value and inertia are hypothesised to increase the desirability of the object or persons.

Later, Cohen et al. (1981) divided suitable target elements as exposure which is the outcome of visibility and accessibility of targets and target attractiveness referring symbolic value and desirability of objects or persons. This categorisation of four attributes appears to be more practical since one concept (suitable target) had different dimensions which would make it difficult to operationalise in empirical studies. It would be a hard task to assess whether it was visibility and accessibility or value and inertia that made objects or persons more suitable targets. Moreover, Cohen et al. (1981) introduced proximity to the motivated offender concept in their new model although Cohen and Felson (1979) used the term proximity to explain unexpected high victimisation rates among unemployed people. They argued that the geographical proximity of unemployed individuals to the high concentration of would-be offenders could be the reason for the increased risk of being targeted. However, they did not use proximity as a conceptual component of the RAT. Cohen et al. (1981) posit that proximity to motivated offenders, which denotes living in areas close to places where potential offenders are mostly found, increases the risk of victimisation.

Miethe and Meier (1990) suggested a structural-choice model as a remedy to operationalisation problems occurred in empirical studies applied LET and RAT. They proposed four elements: proximity, exposure, target attractiveness and absence of a capable guardianship as minimal requirements of a crime. They omitted the concept of definitional properties of specific crimes from their model. Although authors did not provide any reason for the omission of this concept, difficulties in the operationalisation of this concept may be a possible explanation of the removal of definitional properties of specific crimes from the equation of victimisation process

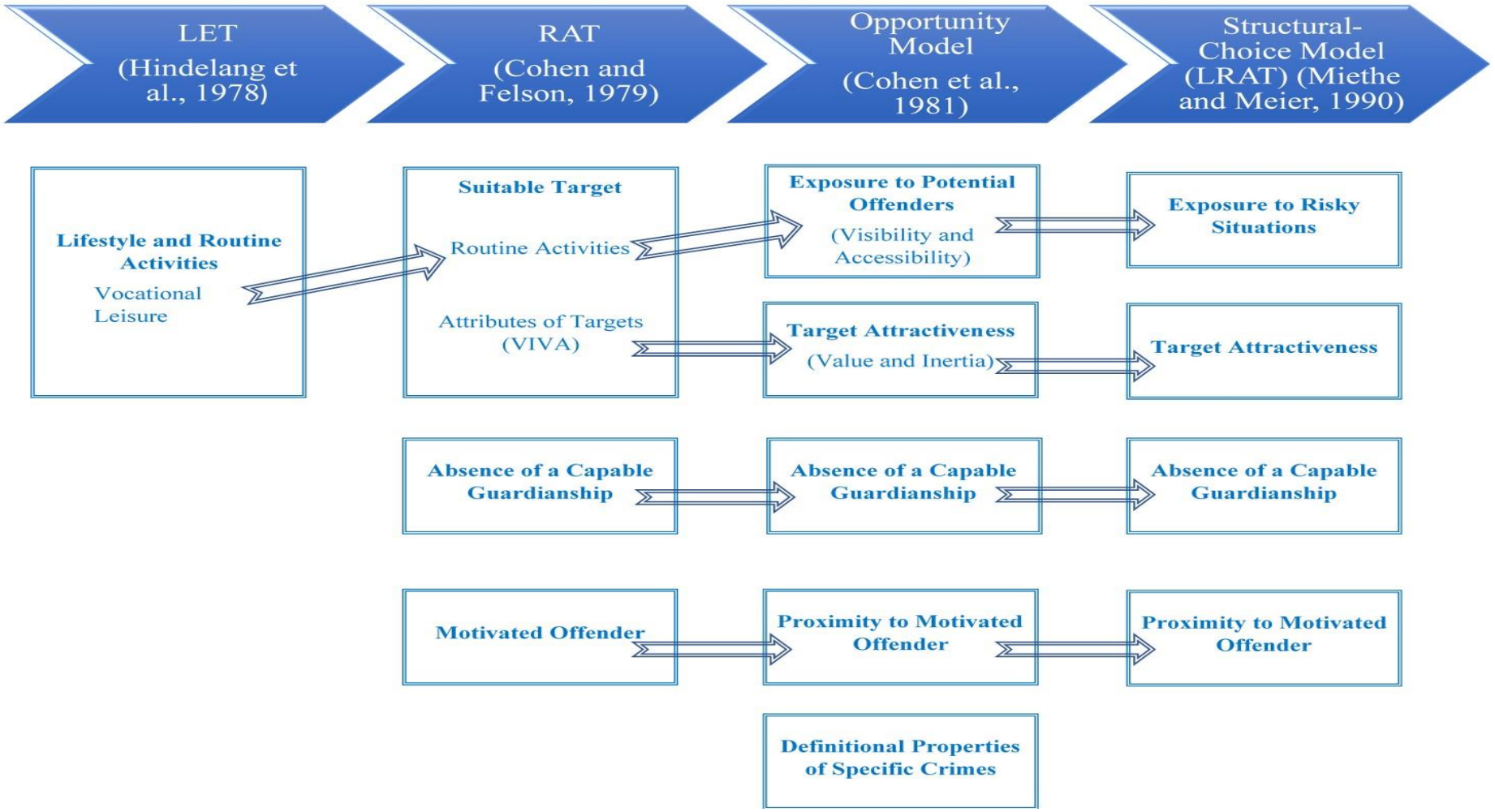



Figure 2.1: *Historical Transformation of LRAT Concepts*

### 2.2.6 Critique of Opportunity Theories of Victimisation

It may be argued that opportunity theories of victimisation challenged the way scholars perceived the criminal victimisation and the introduction of LET and RAT stimulated criminological thinking (Osgood et al., 1996; Mustaine and Tewksbury, 1998; Tillyer and Eck, 2009). Whereas this approach received praise for its novel contribution to criminological thinking, it has also been subject to criticism. This section of the chapter documents the conceptual limitations of opportunity theories of victimisation.

It is argued that main postulate of opportunity theories which states that crime is the outcome of the convergence of three elements: motivated offender and suitable target in the absence of a capable guardianship presents an unfalsifiable tautology (Walklate, 1989; Pratt and Turanovic, 2016). This formulation of victimisation is just a mere description of crime events, and there is nothing special with this formulation (Sutton, 2014). However, I would argue that although criminal opportunity theories are descriptive in nature, they still offer a valuable systematic approach to crime events. Examining the contribution of each element to crime events would provide significant insight into our understanding of criminal victimisation.

The vagueness of the lifestyle concept and failure in distinguishing between risky and non-risky routine activities were other criticisms directed to opportunity theories (Meier and Miethe, 1993). Tittle (2018) further argues that theory does not tell exactly which daily routine activities or which combination of these activities lead to victimisation.

Ambiguity around the relative importance of each conceptual component of theory in the commission of a crime is another criticism directed to opportunity theories approach. It is argued that theory posits convergence of three elements as a minimal requirement of predatory victimisation; however, each component should not have equal impact on the chance of experiencing victimisation (Miethe et al., 1987; Finkelhor and Asdigian, 1996). For instance,

is its absence of a capable guardianship or symbolic value of an object that makes it a more suitable target of an attack? Opportunity theories do not clearly state which elements of theories create more opportunities for criminal victimisation.

Lastly, the lack of focus on offenders has also received criticism. It is argued that opportunity approach downplays the role of offenders in the commission of a crime (Meier and Miethe, 1993). These theories propose that crime rates may display changes regardless of the total number of offenders in a society (Akers, 1999; Tillyer and Eck, 2009). It is the shifts in criminal opportunities created by individuals' lifestyles and routine activities that cause variance in crime rates. Another point to be highlighted with regards to offending is that this approach implicitly states that every individual may commit an offence should the opportunity arises (Bohm and Vogel, 2010). Clarke and Felson (1998, p. 1) later explicitly pronounce this assumption with the well-known phrase "opportunity makes thief".

This section of the chapter introduced the historical development of opportunity theories of victimisation. The next section will critically evaluate the applicability of the last version of opportunity theories of victimisation, LRAT, to cybercrime.

## 2.3 Application of LRAT to Cybercrime Studies

Even though opportunity theories of victimisation were proposed to explain the causes of predatory victimisation, it has been applied to many types of victimisation including cybercrime. Although some scholars (Grabosky and Smith, 2001; Pease, 2001) discussed the virtue of some concepts of RAT for cybercrime in their works, it is Grabosky (2001) who explicitly proposed RAT as a theoretical framework for cybercrime studies. He argues that technology advances rapidly; however, basic tenets of human motivation like lust, revenge, power, adventure and greed do not change. Three elements proposed to account for the victimisation of conventional terrestrial crimes may be utilised to explain the causes of

victimisation in cyberspace. A review of the literature indicates that RAT has gained considerable attention of scholars researching cybercrime after Yar's (2005) seminal work where he systematically examined the conceptual problems of applicability of RAT to cybercrime. Since then many cybercrime studies applied opportunity theories of victimisation as a theoretical framework.

The applicability of LRAT as a theoretical framework to cybercrime studies is one of the contested debates in cybercrime victimisation literature (Paek and Nalla, 2015; Holt and Bossler, 2016). Opportunity theories of victimisation have been applied as theoretical frameworks while examining *online fraud victimisation* (Pratt et al., 2010; van Wilsem, 2013a; Policastro and Payne, 2014), *online identity theft victimisation* (Paek and Nalla, 2015; Williams, 2015), *phishing victimisation* (Hutchings and Hayes, 2008; Leukfeldt, 2014), *hacking victimisation* (Choi, 2008; Choi et al., 2016), *malware infection* (Bossler and Holt, 2009; Holt and Bossler, 2013; Leukfeldt, 2015), *online harassment victimisation* (Marcum et al., 2010; Marcum, 2011; Reyns et al., 2011; Reyns et al., 2016) and *multiple forms of cybercrime victimisation* (Ngo and Paternoster, 2011; van Wilsem, 2013b; Reyns et al., 2015). The results of these empirical studies yielded mixed results about the applicability of LRAT to cybercrime as well as the theoretical power of theory in explaining victimisation in cyberspace. Whereas results of some studies (Choi, 2008; Reyns et al., 2011; Reyns et al., 2016) supported the application of theory, results of some other studies (Ngo and Paternoster, 2011; Policastro and Payne, 2014) lent no support to the application of theory to cybercrime. On the other hand, some other studies (Bossler and Holt, 2009; Marcum et al., 2010; Holt and Bossler, 2013; van Wilsem, 2013b) yielded partial support for the applicability of LRAT to cybercrime which means that while some elements of theory fail to account for victimisation in cyberspace other elements explain cyber victimisation successfully.

The first part of this section examines the operationalisation of opportunity theories of victimisation in cybercrime victimisation studies. The second part of this section critically reviews the debate pertaining to shortcomings of utilising conceptual elements of LRAT in cybercrime victimisation analysis.

### 2.3.1 Operationalisation of LRAT concepts in Cybercrime Studies

As noted earlier, although opportunity theories of victimisation share similar approaches to the causation of victimisation events, their conceptual frameworks display differences. A review of the literature indicates that scholars aiming to understand victimisation phenomenon through the lenses of criminal opportunity utilised different versions of this theoretical approach. Likewise, cybercrime studies utilising opportunity theories as theoretical frameworks applied different versions of this theoretical perspective. While some cybercrime victimisation studies (i.e. Hutchings and Hayes, 2008; Bossler and Holt, 2009; Pratt et al., 2010; Marcum, 2011) applied RAT as a theoretical framework, some others (i.e. Ngo and Paternoster, 2011; Policastro and Payne, 2014; Maimon et al., 2015) utilised LRAT to account for cybercrime victimisation. Some scholars preferred to utilise LRAT with other theories to increase the predictive power of their studies. For instance, Self-control Theory and RAT (Holtfreter et al., 2008; van Wilsem, 2011, 2013a, 2013b) or Protection Motivation Theory (PMT) and RAT (Jansen and Leukfeldt, 2016) are utilised in tandem to account for cybercrime victimisation.

Choi (2008) utilised the LRAT perspective to create a Structural Model of computer-crime victimisation. However, as he treated the RAT as the extension of LET, he did not operationalise four conceptual elements of LRAT. Self-reports from a sample of college students (N=204) were utilised to run Structural Equation Model tests. Online lifestyle and digital guardianship concepts were operationalised to construct the proposed model of

victimisation. Online lifestyle was operationalised with three measures: normal vocational and leisure activities, risky vocational activities and risky leisure activities. Online activities like visiting unknown websites, downloading free MP3 or software and clicking icons without consideration were used as proxy measures of risky online lifestyle. Three digital guardianship measures: using antivirus software, anti-spy software and firewall were utilised to measure the effectiveness of guardianship. Three variables, frequency of victimisation, total hours lost due to victimisation experience and total financial loss, were used as a proxy of computer-crime victimisation. Research findings indicated the presence of a relationship between computer-crime victimisation, an online lifestyle and guardianship measures. His model suggested that while risky online lifestyle increased the odds of victimisation, guardianship measures decreased the risk of being a victim.

Choi's (2008) study is one of the first studies adapting opportunity theories approach to cybercrime. Demonstrating the relationship between two main LRAT concepts (online lifestyle and guardianship) and the risk of victimisation was the major contribution of his study to cybercrime victimisation literature. However, this study has some significant limitations to be documented. Although the Choi (2008) utilised RAT as a theoretical framework, he did not operationalise suitable target concept of this theory. His Cyber-Routine Activities model presented an abridged model of RAT. Moreover, he did not deal with conceptual issues with regards to the transposition of RAT's concept to cybercrime studies. Lastly, he used a limited number of online activities as a proxy of the online lifestyle. Utilising a sample of college students, which limited generalisability of research findings, was another shortcoming of the study.

Later Choi et al. (2016) utilised the same dataset collected in 2007 to examine the relationship between demographic characteristics of Internet users and the risk of computer

crime victimisation. Age, gender and ethnicity were the demographics examined through the Structural Model of Victimisation. The results of this study indicated the presence of gender difference at online lifestyles of Internet users. Males were found to be more likely to engage with risky online activities. However, no gender difference was identified pertaining to digital guardianship. A negative association was identified between age and security measure application. Older Internet users used fewer security measures. However, it should be noted that this study utilised college students as the sample universe. Thus, the generalisability of this finding is questionable. Their study suggested no significant relationship between race and risk of victimisation. Since Choi et al. (2016) utilised the same dataset in their analysis above mentioned limitations are applicable to this study.

Reyns et al. (2011) proposed Cyberlifestyle-Routine Activities Theory. A sample of college students (N=974) was utilised to research cyberstalking victimisation. This study may be considered as the most successful application of LRAT to cybercrime victimisation analysis, since all four concepts of LRAT, online exposure to motivated offenders, online proximity to motivated offenders, online target attractiveness and online guardianship, were operationalised in this study. Moreover, online/electronic deviant lifestyle is also included this proposed cyber version of LRAT. Demographic characteristics and risky offline activities were added as control variables in the study. Due to a large number of variables, the operationalisation of this study is illustrated with a table (Table 2.1).

Table 2.1

*Operationalisation of Reyns et al. (2011)*

| |
|---|
| **Dependent variable** |
| Unwanted contact |
| Harassment |
| Sexual advances |
| Threats of violence |
| Cyberstalking victimization |
| **Independent variable** |
| **Online exposure** |
| Time spent online (Number of hours per day) |
| Number of social networks |
| Number of updates to social network (Number of updates to social networks per day) |
| Number of photos online |
| Use AOL Instant Messenger |
| **Online proximity** |
| Add stranger |
| Number of friends (Natural log of the number of friends online) |
| Friend service |
| **Online guardianship** |
| Profile(s) set to private |
| Use profile tracker |
| Deviant peers (Mean level of peer deviance) |
| **Online target attractiveness** |
| Composite measure (Mean level of target attractiveness) |
| Gender |
| Relationship status |
| Sexual orientation |
| Online deviance (Mean level of online deviance) |
| **Control variables** |
| Age |
| Non-White |
| Offline risky activities |

The results of this study suggested LRAT as a suitable theoretical framework for cybercrime victimisation. While online exposure and proximity had the weakest association with cyberstalking victimisation, online target attractiveness and guardianship had a stronger relationship with victimisation. Online deviance had the most significant impact on the risk of experiencing cyberstalking victimisation.

This study which integrated LRAT approach with Self-control Theory (Gottfredson and Hirschi, 1990) has important contributions to cybercrime literature. Previous studies utilising opportunity approach as a theoretical framework failed to operationalise at least one component of LRAT. However, Reyns et al. (2011) operationalised all components of LRAT. This study successfully addressed all criticism related to applicability of LRAT to cybercrime. Integrating Self-control theory with LRAT is another significant contribution of this study. LRAT generally focused on the impact of normal routine activities on the risk of victimisation. This study incorporated the effect of deviant online activities to opportunity theories of victimisation. However, it should be noted that this is not the first study that incorporated online deviance to opportunity theories of crime. Previous cybercrime studies also examined the impact of cyber deviance on the risk of online harassment (Holt and Bossler, 2008; Bossler and Holt, 2010), malware infection (Bossler and Holt, 2009) and computer virus infection (Choi, 2008).

This part of the section reviewed the key studies to illustrate the operationalisation of LRAT concepts in cybercrime victimisation studies. This part of the section discusses the conceptual problems of utilising LRAT concepts in empirical cybercrime victimisation research.

### 2.3.2 Conceptual Pitfalls of Transposing LRAT Elements to Cyber Space

As stated earlier, LRAT posits that motivated offender, suitable target and absence of a capable guardian are three minimum elements for the occurrence of a crime (Cohen and Felson, 1979). Since a motivated offender is given, proximity and exposure to the motivated offender are conceptualised as a proxy of offending behaviour (Felson and Cohen, 1980). This section of the chapter presents the conceptual problems of applying LRAT as a theoretical framework to cybercrime analysis.

#### 2.3.2.1 The Distinction between Proximity and Exposure to Motivated Offender

Proximity to motivated offenders is defined as "the physical distance between areas where potential targets of crime reside and areas where relatively large populations of potential offenders are found". Whereas, exposure is defined as "the physical visibility and accessibility of persons or objects to potential offenders" (Cohen et al., 1981, p. 507). So, while proximity refers to the physical distance between targets' neighbourhood and places where potential offenders are mostly found (Meier and Miethe, 1993), exposure denotes individuals' actions that increase their visibility and accessibility to motivated offenders. Cohen and Felson (1979) propose that *physical* or *geographical* closeness to the motivated offender population increases the risk of being a victim due to the possible interaction between offenders and potential targets. The places where potential offenders concentrate are called *"hotspots of crime"* (Sherman et al., 1989, p. 37). A number of studies (Koper, 1995; Sherman and Weisburd, 1995; Braga and Bond, 2008; Malleson and Andresen, 2015; Ariel and Partridge, 2017; Quick et al., 2018) investigating the presence and the effects of hotspots of crime on the likelihood of being a victim of a crime suggest that these places increase the odds of victimisation.

The transposition of the proximity concept into cyberspace is problematic as the distance in cyberspace in constant (Yar, 2005). In other words, cyber proximity means that

every Internet user resides at the same virtual distance to the motivated offender. Vakhitova et al. (2015) argue that the operationalisation of these two concepts, proximity and exposure to the motivated offender, in cybercrime studies is a difficult task as these two key elements overlap. In order to overcome this difficulty, some scholars (Bossler and Holt, 2009; Holt and Bossler, 2013) preferred to operationalise these two elements as one concept, some other scholars (Leukfeldt, 2014; Leukfeldt, 2015; Leukfeldt and Yar, 2016) did not use these elements in their operationalisation. They operationalised attributes of a suitable target (value, inertia, visibility and accessibility) to examine the relationship between online activities and facing different forms of cybercrime.

#### 2.3.2.2 Target Suitability and Target Attractiveness

The second concept of the LRAT that create difficulties in cybercrime studies is a suitable target. Cohen and Felson (1979) argue that when a suitable target meets the potential offender at the same time and place crime occurs. The concept of target suitability has two dimensions: *routine activities* that make individuals or objects suitable targets and *attributes of individuals or objects* that make them attractive targets (Felson and Cohen, 1980; Cohen et al., 1981). The first dimension perceives individuals' daily routine activities as a risk factor for being a suitable target. Cohen and Felson (1979) propose that individuals' daily activities may cause them to be easy prey for the offenders. For instance, they argue that going out frequently at night leaves houses unguarded and create opportunities for burglars. Visibility and accessibility are two dimensions of the target suitability (Bennett, 1991). Targets that are more visible or accessible to potential offenders are more likely to be subject to a crime (Cohen et al., 1981). Tilley et al. (2015) argue that decreasing the target suitability of individuals or items can decrease crime rates.

The second dimension of a suitable target, namely target attractiveness, refers to the desirability of an object as a subject of a crime (Cohen and Felson, 1979). Value, inertia, visibility and accessibility, which are acronyms as VIVA, are the four elements that make an object or individual attractive (Cohen and Felson, 1979). Felson and Clarke (1998, p. 20) dub the products that have these attributes as "hot products" of crime. Information is the hot product of the virtual environment (Wall, 2007; Newman and Clarke, 2003). This information can be personal details, credit card numbers or bank account credentials. Demographic characteristics such as age, gender and income are also conceptualised as the proxy of the target attractiveness in traditional crime[8] studies (Miethe et al., 1987; Sherman et al., 1989; Moriarty and Williams, 1996; Fisher et al., 2010; Tilley et al., 2015).

Cohen et al. (1981, p. 508) define target attractiveness as "the material or symbolic desirability of persons or property targets to the potential offender". In economic cybercrime context, what makes a target attractive in cyberspace is vague as offenders generally have little or no information about their targets' economic well-being (Vakhitova et al., 2015). Newman and Clarke (2003) argue the primary target of online offenders is information. It seems reasonable to propose that online offenders motivated with financial ends are in search of personal information that can be used to acquire financial gains from targeted individuals (Reyns, 2013). In this aspect, it may be proposed that insignificant personal identifying information such as email addresses may be significant in determining a targets' attractiveness in cyberspace.

[8] This thesis will use the term "traditional crime" to refer crimes that take place outside the cyberspace. In other words, this term will denote offline crimes.

#### 2.3.2.3 Spacio-temporality of the Events

The congruence of a potential target and motivated offender at a particular place and time is LRAT's basic premise (Yar, 2005; Holt and Bossler, 2016). This proposition stresses the significance of the temporal and spatial order of criminal acts (Ngo and Paternoster, 2011; van Wilsem, 2013b). Yar (2005) is one of the first scholars to criticise the transferability of LRAT constructs to cyberspace. Yar (2005) proposes that contrary to real-world counterparts, virtual spatialities are unstable and volatile since they are the outcome of networked technologies (i.e. servers, nodes, fibre optic cables). So, virtual space is not similar to the geographical space that we are accustomed to. Furthermore, he asserts that the average lifespan of websites is very limited. Thus, cyberspace is not composed of fixed locations. This disappearance of cyber spatialities is contrary to the very stable existence of geographical locations of the real world spatialities.

Yar's (2005) second argument concerns the lack of synchronised flow of events at cyberspace. He argues that cyberspace is spatio-temporally disorganised due to the lack of anticipation when the suitable target would be present online. This disorganised nature of cyberspace hinders the applicability of LRAT to cybercrime since the basic premise of the theory, which highlights the importance of the patterns arouses from individuals' routine activities, is not met. Lack of this behavioural pattern may hinder the target and offender interaction in virtual space. Though Internet users (potential targets) and motivated offenders may meet at particular places, namely websites like shopping or online banking websites, they may not be present at a particular website at the same time.

In response to Yar's (2005) critiques in regards to spatially disorganised nature of cyberspace, Maimon et al. (2015) argue that even though Yar's (2005) argument about the transient existence of some websites partly reflects the lifespan of some websites, it is not valid

for those that belong to prominent online merchants, social networking websites or universities and government. In the same vein, Reyns et al. (2011) propose the Cyberlifestyle Approach which is based on a "system problem approach" of Eck and Clarke (2003, p. 35). Eck and Clarke (2003) argue that some sort of crimes like computer virus infection may happen through systems without necessitating face-to-face contact between offender and victim. Offenders utilising the same network with potential targets still can reach them regardless of the geographical dispersion. Mail bombing attack[9] is an example of system problems in real-world (Eck, 2003). Explosive containing packages may still cause harm event though offender and victim do not necessarily interact face-to-face. Reyns et al. (2011) assert that cyberspace constitutes a networked system, and this virtual space can act as a proxy of real-world physical spatialities.

Reyns at al. (2011) also address Yar's (2005) critique of the temporally disorganised nature of cyberspace. They conceptualise the time of engagement between offender and target as a continuum rather than an instant event. They argue that the actions of the perpetrators and target will eventually overlap. For instance, fraudsters send phishing emails, but the email user may open them sometime later. The time interval between the action of sending phishing email and opening an attached link constitutes the time of congruence. Hence, this attribute of the cyberspace which delineates it from the real-world form a new understanding of temporal congruence between motivated offenders and suitable targets (Choi et al., 2016; Riek et al., 2016).

Overall, this section of the chapter documented problems related to transposing some concepts of LRAT to cybercrime analysis. This thesis aims to address the aforementioned shortcomings of applying LRAT to cybercrime. Firstly, operationalisation difficulties between

[9] Mail bombing attack is the action of sending an explosive including package to a target via postal services.

differentiating proximity and exposure to motivated offender elements lead scholars either ignore one element in their analysis or treat them as one single concept. This thesis argues that the main point to be underscored in these concepts is the distinction between the visibility and accessibility of targets. While proximity refers to the mere presence of Internet users on any website, exposure refers to sharing identifying personal information such as credit card numbers or email addresses. This distinction highlights the fact that a target should not only be visible, but it also must be accessible at the same time to increase the risk of exposure to motivated offenders. This aspect of exposure, I would argue, is the most apparent distinction between exposure and proximity to the motivated offender as potential targets should take some actions to make them accessible. For instance, whereas using chat rooms may be an indicator of proximity to the motivated offender, sharing pictures can be an indicator of exposure to the motivated offender.

In economic cybercrime context, this distinction may be measured with operationalising online activities that require personal information disclosure as exposure to the motivated offender. For example, online shopping and online banking will be proxy measures of exposure to motivated offender since Internet users reveal their personal and financial information while accessing these online services. Additionally, online activities that do not require personal or financial information may be considered as proxy measures of proximity to the motivated offender. Browsing for information, reading emails or video streaming will be operationalised as proximity to the motivated offender in this thesis.

What makes an Internet user an attractive target will be another controversial issue this thesis aims to address. Previous research operationalised target attractiveness with demographic characteristics such as income or gender. However, analysis of these attributes may not provide any meaningful interpretations since online perpetrators mostly do not have

any information about Internet users' demographics. Thus, this thesis aims to explore the factors that render Internet users as attractive targets.

The previous section dealt with issues regarding the applicability of LRAT to cybercrime. This section and the following section introduce two theoretical approaches that will be utilised as a conceptual framework while examining Internet users' decision-making processes when they face an online threat and post-victimisation effects of cybercrime victimisation.

## 2.4 Protection Motivation Theory

Protection Motivation Theory (PMT) is a behavioural response theory, which aims to account for individuals' protective reactions to fear appeals (Warkentin et al., 2016; Thompson et al., 2017). PMT was originally proposed to account for the impact of fear appeal communications on behavioural change. Rogers (1975) suggested that individuals conduct a series of cognitive processes to assess the extent of the threat or harm introduced with fear appeal communications. These cognitive processes are run to evaluate a) severity of the threat b) likelihood of experiencing the threat c) efficacy of proposed response to the threat (Rogers, 1975). He argues that these three corresponding cognitive appraisal processes are conducted to mediate the acceptability of recommended solution to fear appeals. Protection motivation is the outcome of these processes. This initial model conceived fear appeals as the initiator of cognitive processes ending with protection motivation decision (Maddux and Rogers, 1983). Later, a revised version of PMT, which enriched the sources of protection motivation, was proposed. (Rogers, 1983). The revised version of PMT included rewards, response cost and self-efficacy into the model (Maddux and Rogers, 1983).

The second model grouped cognitive appraisals processes conducted to evaluate fear-arousing instances or messages into two categories: threat appraisal and coping appraisal

(Rogers, 1983). Individuals assess the severity of consequences and the likelihood of facing these consequences through threat appraisals (Rogers, 1983). Threat appraisal is a combination of two elements: perceived severity and perceived vulnerability. While perceived severity refers to the extent of expected magnitude of threat (Mattson, 2002; Phuanukoonnon et al., 2006; Ritland and Rodriguez, 2014), perceived vulnerability denotes likelihood of facing undesired consequences (Rutledge, 1987; Watt, 2001; Liang and Xue, 2010). It is proposed that the higher perceived severity and perceived vulnerability, the more likely an individual to implement adaptive behaviour (Lwin et al., 2012).

After the initial threat appraisal, a coping appraisal is made to determine individuals' capability to deter the threat and assess the effectiveness of the chosen response. Self-efficacy and response efficacy are the elements of coping appraisals (Rogers, 1975). Self-efficacy may be defined as the individual's skilfulness to impede a threat or his/her perception related to his/her ability to thwart a threat (Ifinedo, 2012; Tsai et al., 2016). Self-efficacy is a significant concept as it denotes an individual's capability to understand the extent of the online threat and determine the most effective safeguarding measure. For instance, an Internet user with high computer self-efficacy may detect a phishing attempt while reading the email and delete it without following the proposed solution for the fabricated problem. Response efficacy is the belief that proposed countermeasures will work to eliminate the impact of the threat (Beck and Lund, 1981; Floyd et al., 2000). If the individual considers the countermeasure as incapable of thwarting the threat, he/she will not implement any adaptive response. Due to that factor Internet security firms strive to enhance Internet users' perceived response efficacy with regards to the effectiveness of security software in preventing cybercrime victimisation.

Rogers (1983) later included rewards or benefits into the protection motivation theory to account for individuals' decision of risk-taking behaviours. He argues that rewards or

benefits may promote individuals' decision of continuing risk behaviour despite the perceived threat. As it was discussed in the previous chapter, deviant online activities were associated with the increased risk of facing cybercrime victimisation. The perceived reward is central to the intention of engaging with deviant online activities as rewards increase the propensity to take risks. For instance, some Internet users download pirated software (Moquin and Wakefield, 2016) or access free streaming websites (Aguiar, 2017) despite the danger of facing malware infection due to rewards of getting some benefits for free. This thesis will examine the impact of rewards on the likelihood of experiencing economic cybercrime victimisation through the lenses of victims.

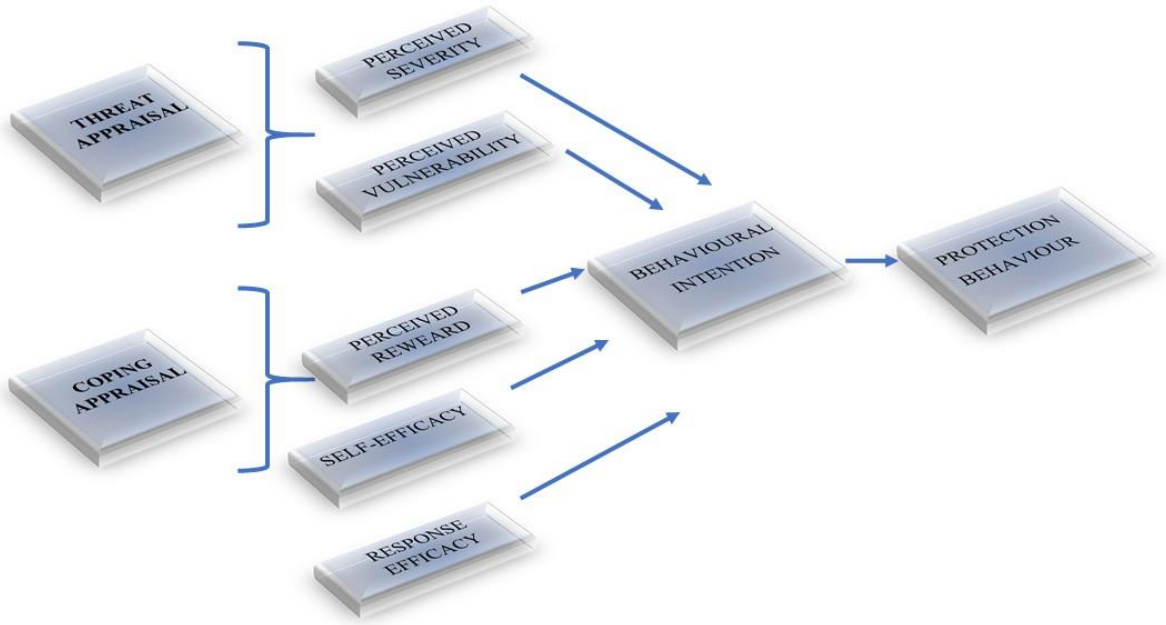



Figure 2.2: PMT Conceptual Framework (Adapted from Rogers (1983))

Rogers (1975; 1983) argue that there is a linear relationship between perceived severity, perceived vulnerability, and protection intention. When one element of interaction is low, the protection motivation will also be low. Past research about Internet users' security adaptation intention yielded conflicting results pertaining to the impact of perceived severity and perceived vulnerability on protection intentions.

Jansen and van Schaik (2016) examined how perceived severity and perceived vulnerability had an impact on Dutch online banking users' protection motivation. They have found that while perceived severity affected online banking users' intention to adopt a security measure, the perceived vulnerability did not have any impact on protection motivation. Tsai et al. (2016) researched the predictors of online safety intentions. They have found that perceived severity was positively correlated with security intentions. Kim and Kim (2016) investigated whether Internet users' perceptions related to the likelihood of facing online identity theft victimisation had an impact on their protection motivation. The results of the research indicated that whereas participants who felt themselves vulnerable to identity theft victimisation agreed to use identity theft protection services, those who were aware of severe consequences of experiencing victimisation did not consider identity theft protection services as useful. On the other hand, Youn (2005) researched the effect of threat perceptions on college students' willingness to share personal information online. He found that both perceived severity and vulnerability to threat alleviated intention of disclosing personal information.

The results aforementioned empirical research suggested that perceived severity and perceived vulnerability have a varying impact on individuals' protection motivation depending on the circumstances that individuals face a threat. Though the perceived severity of the consequences appeared to strengthen the protection intention generally, perceived vulnerability may not sometimes lead individuals to apply security measures. This lack of motivation might

be the consequence of the interaction between threat appraisal and coping appraisal. The coping appraisal process appears to act like a bridge between the perceived risk that is the outcome of the threat appraisal and the decision of implementing a protective behaviour. Individuals' perceptions with regards to the effectiveness of the safeguarding measure or individuals' self-efficacy in implementing the required precautions to the imminent threat determine the decision of protection intention. For instance, the results of Dodel and Mesch (2017) suggest self-efficacy as the most notable predictor of anti-virus software usage. They argue that those who have a greater belief in their ability to protect their computers were more likely to use anti-virus software. In another study, Milne et al. (2009) investigated how self-efficacy impacted online consumers' security behaviours. They found that high self-efficacious Internet users engaged in protective behaviours like installing anti-virus software, using strong passwords and clearing the browser cache. Response efficacy also emerges as a significant factor in implementing a security measure. Empirical research results suggest that should Internet users are persuaded that the response is effective in thwarting a threat they are more likely to use strong passwords (Zhang and McDowell, 2009) and back up their data (Crossler, 2010).

Rewards or perceived benefits were also found to impact Internet users' protection motivation. Online information disclosure studies grouped perceived rewards or as hedonic and utilitarian rewards (Wertenbroch et al., 2005; Miltgen and Smith, 2015). Utilitarian rewards are those that denote instrumental value such as money. Hedonic rewards are more self-fulfilling benefits like establishing online contacts or receiving likes for their posts (Chen et al., 2017). Salleh et al. (2013) delve into factors influencing college students' personal identifying information disclosure over social networking sites. They have found that while perceived benefits and perceived risk of disclosing personal information impacted students' decision of sharing personal information through social networking sites, privacy concern did not have any effect on personal information disclosure. Youn (2005) researching the impact of

threat perceptions on college students' willingness to share personal information online found that perceived benefits increased personal information disclosure. Similarly, Howe et al. (2012) who researched computer users security behaviours found that perceived benefits increased the risk-taking propensity of Internet users.

It is Jansen (2015) who utilise PMT as a theoretical framework in a cybercrime victimisation study for the first time. PMT was proposed as a suitable theoretical framework while examining the factors affecting online banking users' compliance with security instructions. The results of this study have not been published yet. Jansen and Leukfeldt (2016) used RAT and PMT in tandem to increase explanatory power of their research while examining the relationship between phishing, malware infection and online banking. However, PMT had a limited use in their studies since "its constructs are used as possible additional indicators explaining online banking fraud victimization" (Jansen and Leukfeldt, 2016, p. 81). Although these two studies provided a significant insight into utilisation of PMT as a theoretical framework in cybercrime victimisation studies, applications of PMT is these studies were limited. This thesis will be one of the first empirical cybercrime victimisation research examining Internet users' decision-making processes when they encounter an online threat through lenses of PMT in economic cybercrime victimisation context.

## 2.5 Approach and Avoidance Coping Paradigm

Lazarus and Folkman (1984, p. 141) define coping as "constantly changing cognitive and behavioural efforts to manage specific external and/or internal demands that are appraised as taxing or exceeding the resources of the person." Coping paradigm is proposed to explain the relationship between the stressors, environment and individuals (Chun et al., 2006). Lazarus and Folkman's (1984) transactional model and Roth and Cohen's (1986) approach-avoidance models are two theoretical approaches to coping (Anshel and Wells, 2000; Parris et al., 2012).

Lazarus and Folkman (1984) conceptualise approach and avoidance coping strategies as problem-oriented and emotion-oriented. While problem-oriented coping strategies covers active solutions to problems faced, emotion-oriented coping strategies entails passive actions like distancing from the problem (Herman-Stabl et al., 1995). Likewise, Roth and Cohen (1986) categorises coping strategies as approach coping and avoidance coping. Approach coping strategies encompasses confrontation strategies, whereas avoidance strategies refer to emotion-oriented strategies like avoiding the threat or ignoring the existence of the threat (Youn, 2009; Smit et al., 2014). As can be seen these two models explain individuals' reactions to stressors in the same way different terminology.

Avoidance strategies can be sub-categorised as active and passive avoidance strategies (Rachman, 1976). Active avoidance covers situations where individuals run away from the stressor or threat (Man et al., 1994). Active avoidance may refer to refraining oneself from accessing the Internet, avoiding online banking or uninstalling suspicious mobile applications. Passive avoidance denotes the behaviours of ignoring the stressful situation or threat (Afifi and Weiner, 2004). Passive avoidance is similar to emotion-oriented coping strategies proposed by (Lazarus and Folkman, 1984). The application of passive avoidance strategies like ignoring the attacks of the bullies is more prevalent in cyberbullying cases (Price and Dalgleish, 2010; Machackova et al., 2013). It should be noted that the active and passive divide in avoidance strategies has not been applied to cybercrime studies. Cybercrime studies applying coping approach tends to examine avoidance behaviours as a single concept. It is generally health studies (Schmidt et al., 2005; Lykeridou et al., 2011; Peterson et al., 2011) that tends to differentiate between active and passive avoidance strategies as a way of coping.

I would argue that the distinction between active avoidance and passive avoidance is important in cybercrime context for the following reasons. Firstly, while active avoidance

strategies, which denote quitting risky online activities, may prevent the occurrence of economic cybercrime victimisation, passive avoidance strategies indicating ignoring the threat may cause repeat victimisation since ignoring the online threat does not mean ending its existence. However, application of active avoidance strategies may have adverse impacts on Internet users' online lifestyles since it entails stopping using some online services.

Moreover, as Wall (2010a) argues Internet users may perceive online perpetrators as omnipotent super criminals who cannot be stopped due to the media representation of the cybercrime cases. This erroneous belief may lead to passive avoidance since Internet users would perceive economic cybercrime victimisation inevitable. Lastly, passive and active avoidance divide may be helpful to assess Internet users' perceptions with regards to the effectiveness of guardianship measures. Internet users who do not consider online security measures would apply passive avoidance strategies by ignoring the application of any safeguarding measures.

Though coping approaches were proposed to account for individuals' reactions to stressors in real-world situations like stress management related studies (Haley et al., 1987; Meyer et al., 2008; Torres, 2010; Holton et al., 2016) and health studies (Siegel et al., 2001; Walters and Simoni, 2002; Ko et al., 2016), this approach has also been adapted to Internet security studies (Liang and Xue, 2009, 2010; Smit et al., 2014). However, coping approach has limited application in cybercrime studies. Only a handful of cyberbullying studies (Price and Dalgleish, 2010; Šléglová and Cerna, 2011; Machmutow et al., 2012; Parris et al., 2012; Machackova et al., 2013) utilised a coping approach to understand college students survival strategies after experiencing cyberbullying.

Šléglová and Cerna (2011) utilised a coping paradigm to understand negative impacts of victimisation on adolescents. They found that cyberbullying experiences caused changes in

victims' online behaviours. The findings indicated that victims restricted their risky online behaviours such as limiting shared information online or deleting pictures from the Internet. The results of Parris et al. (2012) who researched students' coping strategies in the aftermath of experiencing cyberbullying suggested that students were more likely to adopt avoidance strategies like deleting messages. Machackova et al. (2013) examined the effectiveness of coping strategies for cyberbullying victims. Their findings indicated that cyberbullying victims adopted both active and passive avoidance strategies to cope with adverse impacts of victimisation. Seeking support, technical solutions and ignoring the bully were the most cited coping strategies. (Šléglová and Cerna, 2011).

## 2.6 Summary

This Chapter has outlined the theoretical dimensions of this doctoral thesis. The review of the literature suggests that applicability of LRAT to cybercrime is problematic and future work is required to address potential shortcomings of transposing LRAT's conceptual elements to cyber environment. This thesis aims to contribute to the growing body of cybercrime victimisation literature by providing operationalisation of all elements of the theory in cybercrime context and conducting a systematic test of applicability of LRAT to economic cybercrime victimisation. PMT, which is originally proposed to understand individuals' behavioural reactions to fear appeals, will be utilised as theoretical lens to examine Internet users' cognitive responses to online threats. Approach-Avoidance Coping Paradigm will also be used to explore adverse impacts of economic cybercrime victimisation experiences on Internet users' online lifestyles and safeguarding measures. Application of these three theories as theoretical and conceptula framework may offer some insighths into our understanding of the causes and impacts of economic cybercrime victimisation.

Moreover, several authors (Jaishankar, 2007; Ngo and Paternoster, 2011; Holt and Bossler, 2016) stress the importance of introducing new theoretical approaches to understand cybercrime victimisation. This thesis argues that past empirical studies, which generally utilised LRAT as a theoretical framework, have ignored the socio-cultural nature of cyberspace. These studies generally focus on the role of individuals' demographics and their online routine activities on the risk of being a victim of cybercrime. Meier and Miethe (1993) criticise the current victimisation theories for ignoring the effects of social context on the risk of victimisation. They argue that individuals may become a victim of a crime regardless of their lifestyles and routine activities. This assumption proposes that certain social factors such as living in a high crime rate place may have a greater impact on the likelihood of becoming a victim than individuals' lifestyles. Application of these three theoretical approaches in one single studies may this thesis to gain new insights about causation of the economic cybercrime victimisation.

# Chapter 3 Cybercrime Victimisation

## 3.1 Introduction

This chapter provides an outline of the literature pertaining to this thesis researching the causes of economic cybercrime victimisation together with psychological and behavioural adverse impacts of victimisation experiences on individuals. The aim of this chapter is to illustrate how empirical research informed research questions of this doctoral thesis. The first section of the chapter reviews the results of empirical cybercrime victimisation research employing LRAT as a theoretical framework. The second section of the chapter deals with modus operandi of online perpetrators. The results of research pertaining to phishing, malware infection and hacking will be presented in this second section. The following section reviews economic cybercrime victimisation literature. Card-not-present fraud, online banking fraud and online identity fraud will be examined in this penultimate section. The last section of this chapter displays the results of studies researching Internet users' emotional responses to negative life events and adverse consequences of these emotional reactions on Internet users' online behaviours and security intentions.

## 3.2 Correlates of Cybercrime Victimisation

Lifestyle Routine Activities Theory (LRAT) posits that while exposure and proximity to motivated offender increase the risk of victimisation, the presence of a capable guardianship may prevent the occurrence of victimisation (Cohen et al., 1981). Cybercrime victimisation studies adapting opportunity theories perspective as a theoretical framework utilised the conceptual constructs of this approach while operationalising their variables. A review of empirical studies follows conceptual constructs of LRAT.

### 3.2.1 Exposure and Proximity to Motivated Offender

LRAT posits that individuals' lifestyles and routine activities increase the risk of victimisation since these activities enhance persons' contacts with would be offenders at risky times and places (Cohen and Felson, 1979). Following this line of logic, cybercrime victimisation studies researched the impacts of online routine activities on the risk of experiencing victimisation. As noted in the second chapter, due to conceptual problems of transposing exposure and proximity constructs of theory to cyberspace environment, researchers either operationalised these two conceptual elements as one single construct or used one of them. Due to that factor results of empirical studies pertaining to these constructs will be presented together.

Empirical cybercrime victimisation research yielded inconsistent and contradictory results about the effects of normal daily activities on the risk of facing cybercrime victimisation. Buying goods or products online appeared to be a risk factor for online victimisation. Several studies thus far have linked online shopping with cybercrime victimisation (Marcum et al., 2010; Pratt et al., 2010; Reyns, 2013). Internet banking emerged as another risk factor. The results of past empirical research suggested that Internet banking users are more likely to be victimised than those who do not use these services (Hutchings and Hayes, 2008; Reyns, 2013, 2015). Engaging with online social activities have also been associated with an increased risk of victimisation. The results of Marcum et al. (2010) revealed that those who use chat rooms at least one hour a week were likely to receive sexually explicit material. Likewise, van Wilsem (2013b) illustrated that using social media increase the odds of online harassment victimisation.

However, some other scholars (Ngo and Paternoster, 2011; Williams, 2015) have found that legitimate routine online behaviours do not affect the likelihood of being a victim of

cybercrime. Instead, empirical results suggest that risky online behaviours like downloading free games or opening unknown email attachments were associated with increased risk of online identity theft victimisation (Ngo and Paternoster, 2011; Reyns, 2013). Moreover, deviant online activities such as pirating media, viewing adult content and using other people's Internet connection without authorisation emerged as risk factors of being a victim of malware infection (Bossler and Holt, 2009; Holt and Bossler, 2013).

As can be seen, reviewed studies focused on the impacts of Internet users' online lifestyles on the risk of victimisation due to LRAT's propositions implicitly putting the responsibility of victimisation on individuals' lifestyles or daily routine activities. Thus, extant research failed to explore the effects of other factors such as technological vulnerabilities on the risk of victimisation. This thesis seeks to address this gap through examining influences of technological vulnerabilities which are beyond Internet users' control on the risk of victimisation.

Being descriptive in nature is another shortcoming of much of the previous cybercrime victimisation research. Although these studies illustrated the association between online activities and risk of victimisation, they failed to account for the causal links between online lifestyle parameters and victimisation. This thesis aims to explore and understand why certain normal online activities like online shopping or online banking pose the risk of cybercrime victimisation.

### 3.2.2 Target Suitability and Target Attractiveness

A review of the cybercrime victimisation studies illustrated that there are conceptual differences between target suitability and target attractiveness, which are documented in the previous chapter (the second chapter). Whereas target suitability refers to being vulnerable or open to perpetrators' malicious actions (Finkelhor and Asdigian, 1996), target attractiveness

denotes the state of being more desirable due to their specific attributes like economic value when compared to other potential targets (Miethe and Meier, 1994). Despite these conceptual distinctions, much of the cybercrime studies operationalised these concepts interchangeably (Vakhitova et al., 2015). Previous cybercrime research focused on two aspects of the target suitability/target attractiveness: individuals' demographic characteristics and online behaviours.

LRAT posits that individuals' demographics may increase their target attractiveness (Cohen and Felson, 1979; Cohen et al., 1981). Income, age and gender were the most researched demographics.

Income, as a target attractiveness factor, received considerable attention in cybercrime literature. The research findings of the relationship between income and victimisation are mixed. Whereas some studies illustrate that income is positively correlated with exposure to online scams and online identity theft victimisation (Garg and Nilizadeh, 2013; Reyns, 2013), some others (Holtfreter et al., 2005; van Wilsem, 2011; Dai et al., 2014; Policastro and Payne, 2014) yield no relation between income and different forms of online victimisation, namely credit card and bank fraud, fraud targeting and telemarking fraud. Rather than being a direct impact on the likelihood of being a target of cybercrime, income may have a moderating effect on the chance of being targeted (Reyns, 2013). It might be presumed that Internet users with high-income levels would engage with online financial activities like doing more online shopping or using online banking more frequently then low-income Internet users. This frequency of online financial service usage might be a factor impacting target suitability (Reyns, 2013). On the other hand, individuals with low-income levels might be more eager to engage with risky online activities like free downloading or responding scam emails offering an easy way of getting rich (Garg and Nilizadeh, 2013).

Age is another factor that hypothesised to be related to target suitability. The results of some empirical studies demonstrated that young people are more likely to be a victim of cybercrime, (Pratt et al., 2010; Ngo and Paternoster, 2011; van Wilsem, 2011, 2013a; Dai et al., 2014; Leukfeldt and Yar, 2016); however, Reyns (2013) found that older people are at the increased risk of online identity theft. Some other research (Holtfreter et al., 2008; Reyns et al., 2011; Holt and Bossler, 2013; Policastro and Payne, 2014) yielded absence of a significant relationship between age, target attractiveness and cybercrime victimisation.

It is argued that young individuals' active online lifestyles, propensity to take the risk, being impulsive and engaging with deviant online activities as the possible explanations for the results indicating young Internet users' as at increased risk of cybercrime victimisation (Ngo and Paternoster, 2011; van Wilsem, 2011). Although Reyns' (2013) study did not clarify why older Internet users were more likely to experience identity theft victimisation, Internet self-efficacy may be a factor that facilitates cybercrime victimisation among older Internet users. Some other research (Holtfreter et al., 2008; Reyns et al., 2011; Holt and Bossler, 2013; Policastro and Payne, 2014) yielded absence of a significant relationship between age, target attractiveness and cybercrime victimisation.

The impact of gender differences on the risk of experiencing economic cybercrime victimisation also received considerable attention. Literature again yields mixed empirical evidence about the effect of gender on being a suitable target. The results of some studies illustrate that males are more likely to be the target of online fraud or online scams (Holtfreter et al., 2008; Garg and Nilizadeh, 2013; Policastro and Payne, 2014). For instance, Reyns (2013) suggest that males are at increased risk of experiencing online identity theft victimisation; he proposed males' downloading behaviour as a possible explanation of this result. However, this proposition was based on any empirical analysis. Some other studies show that females are

more likely to be a victim of malware infection and online sexual offences (Bossler and Holt, 2009; Marcum et al., 2010; Holt and Bossler, 2013). Nonetheless, (Ngo and Paternoster, 2011) found no gender effect on the seven different forms of online victimisation. For example, the results of van Wilsem (2011) demonstrate that there is no statistically significant effect of gender on the risk of being a victim of online crime.

Besides individuals' demographic characteristics, the impact of online activities on the risk of being a suitable target was also researched. Yet, only a few scholars (Marcum et al., 2010; Ngo and Paternoster, 2011) have researched the relation between online behaviour and target suitability. Ngo and Paternoster (2011) studied the correlates of the different forms of cyber victimisation, namely computer virus infection, experiencing phishing, encountering online harassment, receiving unwanted adult material, being solicited for sex and encountering online defamation. Online communication with strangers, sharing personal information online, opening unknown attachments and clicking on the links in the emails hypothesised to be a risk factor for increased target suitability. Only clicking on links was correlated with only one form of the victimisation, computer virus infection. The results of this study suggest that the absence of the relationship between online behaviours and increased target suitability.

Another study conducted by Marcum et al. (2010) researched the impact of computer-mediated communication on the chance of being a victim of sexual crime among college students. They reported that college students who provided their personal information to strangers online were more likely to face sexual solicitation than those who did not provide personal information online. Hence Marcum et al. (2010) argue that online activities that elevate target suitability lead to increased risk of victimisation. This result contradicts Ngo and Paternoster (2011) who found no relation between sharing personal information online and experiencing different forms of online sexual victimisation.

As can be seen the results of past empirical research on factors facilitating target suitability displays inconsistency. These discrepancies may be the effect of type of cybercrime victimisation as every crime has its specific conditions to occur (Clarke, 1995). The vagueness of suitable targets in cyberspace may be an explanation of the lack of relationship between Internet users' demographic characteristics and target attractiveness. As previously referred to, anonymity is the most common attribute of online lifestyle. Most online activities do not require disclosure of demographic characteristics, which makes it harder for online perpetrators to spot suitable targets. This thesis endeavours to discern the factors rendering Internet users a target of an online attack.

### 2.2.3 Absence of a Capable Guardian

Lifestyle Routine Activities Theory posits that the presence of a capable guardian is a significant factor in crime prevention (Cohen and Felson, 1979). Guardianship can be defined as the ability of a thing or a person to prevent the occurrence of the crime (Cohen et al., 1981). Capable guardianship is categorised initially into two groups: physical guardianship measures and social guardianship measures (Miethe and Meier, 1990). Physical guardianship measures are those that prevent unauthorised entrance into a place or provide protection. Alarms, street lights, fences, protective tools (a pepper spray or a gun) could be examples of the physical guardianship measures in the real world (Robinson and Robinson, 1997). On the other hand, social guardianship refers to the presence of an individual to increase safety. Family members, friends or teachers can be examples of social guardianship (Spano and Nagy, 2005).

Guardianship measures in cybercrime studies are generally divided into two distinct categories as physical and personal guardianship measures (Ngo and Paternoster, 2011; Holt and Bossler, 2013; van Wilsem, 2013b). Whereas physical guardianship measures refer to protective software like anti-virus software or firewalls, personal guardianship measures

denote Internet users' skills to defend themselves from online threats. However, some other scholars (Bossler and Holt, 2009; Reyns et al., 2011; Paek and Nalla, 2015) added social guardianship denoting the presence of another individual while accessing the Internet. Moreover, Williams (2015) proposes a different typology of guardianship in cyberspace. He categorises guardianship measures as passive physical guardianship (anti-virus software or firewalls), active personal guardianship (changing security settings or passwords) and personal avoidance guardianship (doing less Internet banking).

Past empirical research again yields mixed results about the effect of the guardianship on the chance of being a victim of a cybercrime. Since different forms of cybercrime require different guardianship measures, the review below of the empirical studies researching the effect of guardianship on the chance of being a victim of cybercrime is based on the classification of cybercrimes.

#### 2.3.3.1 Computer Integrity Crimes

Computer integrity crimes are those that involve a crime against networked computer systems. Hacking is the most vivid example of computer integrity crimes (Wall, 2007). As these crimes encompass intrusion of computer systems, security software and firewalls are the most effective safeguarding measures devised to prevent the occurrence of victimisation (Symantec, 2018). However, the results of past empirical research suggest that the effectiveness of security software at cybercrime prevention is questionable. The results of some studies (Bossler and Holt, 2009; Ngo and Paternoster, 2011; Holt and Bossler, 2013) suggested anti-virus software and firewalls as a low impact solution thwart malware infection. The results of these studies indicated that Internet users who used security software were more likely to experience malware infection. Moreover, the study conducted by van Wilsem (2013b) yields no relationship between the risk of hacking victimisation and anti-virus software usage. These

results are contrary to expectations as the presence of security software should reduce malware infection risk.

#### 2.3.3.2 Computer Content Crimes

Computer content crimes are related to the content of the computer such as the distribution of pornography and hate crime (Wall and Williams, 2007). Offensive communications like cyberbullying and cyberstalking are also considered as computer content crimes (Srivastava, 2012; Tsakalidis and Vergidis, 2017). The results of the study conducted by (Marcum, 2011) show that personal guardianship measures such as the presence of a teacher while using the Internet decrease the odds of receiving online harassment. Marcum et al. (2010) found that using anti-virus programs does not decrease the risk of being a victim of cyberbullying. Similarly, Reyns et al. (2011) argue that digital guardianship methods such as profile tracker increase the risk of being a computer content victim. These results suggest the relationship between the type of safeguarding measure and type of online threat may determine the effectiveness of safeguarding measures. As cyberbullying is an interpersonal offence digital guardianship measures would not be effective in crime prevention. However, the presence of a third party (parent or teacher) emerged to increase the risk of victimisation since the presence of another person may hinder engaging with deviant online behaviours.

#### 2.3.3.3 Computer Assisted Crimes

Computer-assisted crimes are online crimes that can be committed in the real-world, but networked technologies facilitated the commission of the offences (Wall, 2007). Fraud, identity theft and cyber deception are examples of computer-assisted crimes. Past empirical research yielded mixed results with regard to the relationship between guardianship measures and risk of experiencing computer-assisted crimes. Policastro and Payne (2014) found that there is no relation between guardianship measures and telemarketing fraud. Similarly,

Hutchings and Hayes (2008) point out that using email filters does not decrease the chance of being a victim of phishing. They also found that those who used firewalls were more likely to be a victim of phishing. On the other hand, Williams (2015) examined the online identity theft victimisation in European countries at the country and individual level. His findings disclosed that Internet users who applied passive physical guardianship measures like installing anti-virus software were less likely to experience online identity theft victimisation.

One of the critiques directed to LRAT was ambiguity related to the relative importance of conceptual elements for the occurrence of victimisation (Miethe et al., 1987). It is argued that guardianship is the most significant concept for the occurrence of cybercrime victimisation due to its role in protecting individuals from online threats (Grabosky, 2001; Bossler and Holt, 2009). The results of past empirical cybercrime victimisation research set the importance of personal and digital guardianship, however, these victimisation studies neither examined the factors that influence the effectiveness of the Internet users' personal guardianship measures nor Internet users' protection motivation. Examining the factors that affect Internet users' decision-making systems when they experience online threats may provide insight into our understanding of why some guardianship measures fail to protect online users.

This section of the chapter has reviewed the cybercrime victimisation literature pertaining to correlates of cybercrime victimisation. This section limited reviewed studies to those applying opportunity theories of victimisation as a theoretical framework. This next section of the chapter examines cybercrime studies researching modus operandi of online perpetrators.

## 3.3 Precursors of Economic Cybercrime Victimisation

Phishing, malware infection and hacking are considered to be the most common methods to acquire Internet users' personal identifying information as well as financial information (Wall, 2013d; Williams, 2015), which would be utilised to attain financial gain.

### 3.3.1 Phishing

Phishing has become a demanding challenge for Internet users for over a decade as fraudsters increasingly target individuals with socially engineered tactics to gain information from them (Wall, 2008b). Perpetrators utilise unsolicited emails and bogus websites to gain personal or financial information to be used for subsequent fraud attempts (Almomani et al., 2013). Figure 3.1 illustrates the classification of phishing attempts.

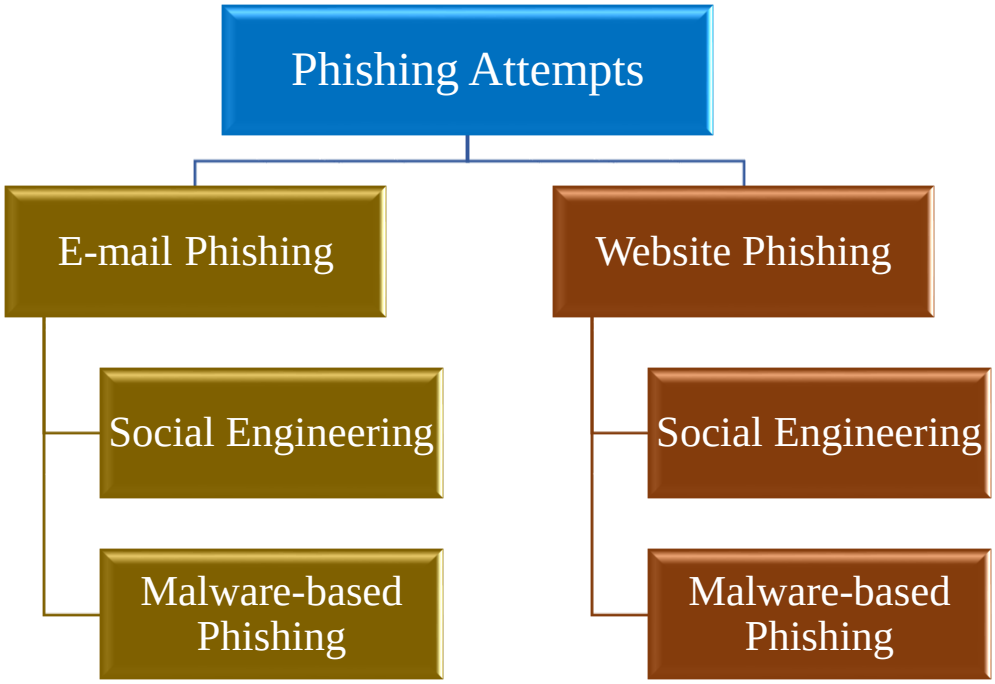



Figure 3.1: *Classification of Phishing Attempts*

#### 3.3.1.1 Email Phishing

According to the recent Symantec Internet Security Threat Report, emails are the primary channel of phishing attacks (Symantec, 2017). Phishing attempts are valuable assets for the perpetrators as these kinds of attacks allow them to reach a large number of individuals who are geographically distant (Wall, 2007). A confidence trickster can also utilise many tools such as names and logos of big brands to disguise their identity and increase the believability of the messages conveyed in the emails. Moreover, diminished costs and risks are the other advantages of utilising email phishing attempts (Tuli and Juneja, 2016). Although many phishing emails are sent to all targets that are present in the email database, still some phishing emails target specific individuals or companies with a distinct aim (Menon and Guan Siew, 2012; Levi et al., 2015; FireEye, 2018). This targeted form of phishing is defined as spear phishing, which includes a part of personal information of the Internet users or companies to trick them into providing their personal or financial information (Caldwell, 2013). Spear phishing attempts are considered to be more sophisticated and challenging as they utilise social engineering methods like utilising personal identifying information, fear appeals or urgency cues to confuse individuals (Wall, 2013b; Halevi et al., 2015). The recent cybersecurity report published by Symantec illustrates that a majority of infection vectors are spear phishing (71% of all vendor infections) (Symantec, 2018).

Technical means such as malware containing links as well as social engineering are two common methods utilised to trick Internet users into yielding personal information (Hutchings and Hayes, 2008; Davinson and Sillence, 2010). Pharming is a malware-based technique used to direct the Internet traffic between the target computer, a legitimate website and a bogus website (Kraemer-Mbula et al., 2013; Reurink, 2016). The infected browsers direct clients to bogus websites such as online banking web pages to get sensitive data. The infection may occur

in two scenarios. Sending malware embedded emails is one method. When the user opens malware containing mail drive-by-download occurs automatically (Karlof et al., 2007; Stamm et al., 2007). Utilising emails containing links bearing malware is another way of infecting browsers (Brody et al., 2007). However, clients are required to click on the link to activate the malware. These methods are purely technological when compared to social engineering methods that require tricking Internet users into providing personal information (Wall, 2013d).

Social engineering, which aims to exploit Internet users' weaknesses, plays an essential role in phishing cases (Bullée et al., 2015; Krombholz et al., 2015). Fraudsters increasingly target Internet users through emails including highly sophisticated and challenging social engineering tactics to solicit financial or personal information (Butavicius et al., 2016; Clark, 2017). Social engineering is initially conceptualised as employing socially tailored tricks to gain sensitive data such as passwords or username to access computer systems (Weinberg, 1966; Abraham and Chengalur-Smith, 2010). However, the scope of social engineering has extended to cover personal and financial information of Internet users (Newman and Clarke, 2013). The aim of social engineering in a phishing context is to manipulate Internet users into divulging personal or financial information (Nirmal et al., 2010; Lakshmi and Vijaya, 2012; Mishra et al., 2012). To that end, fraudsters exploit Internet users' social and psychological vulnerabilities. The extant phishing literature focused on these vulnerabilities, which are classified as external and individual vulnerabilities.

## External Vulnerabilities

Cialdini (2009) proposed six influence techniques in relation to external vulnerabilities, namely social proof, consistency, liking, scarcity, authority and reciprocity. Apart from cybercrime and Internet security studies, effectiveness of influence techniques has been researched in various areas such as marketing (Roughead et al., 1998; Eisend, 2004; Cugelman et al., 2011), public health (Buller et al., 2000; Mansfield et al., 2006; van Achterberg et al., 2010), family relationship (Kümpel Nørgaard et al., 2007; Nørgaard and Brunsø, 2011; Sundie et al., 2012; Haselhoff et al., 2014). The results of these studies indicate that each of these influence tools has varying impacts depending on personal, social and psychological conditions.

Research related to testing empirical evidence of the impact of these methods in cybersecurity appears to indicate that the effectiveness of these factors is highly context dependent. While the results of Wright et al. (2014) indicated that four influence methods, reciprocity, scarcity, liking and social proof increased the odds of responding phishing emails, those of Silic and Back (2016) suggested that liking is the most powerful tool to gather information from employees through social network sites. Research conducted by Williams et al. (2017) demonstrates that it is the combined effect of different influence techniques and personal or social circumstances that increase the susceptibility of Internet users to phishing attacks. Oliveira et al. (2017) worked on the impact of influence techniques across demographic characteristics of email users. They found that different age groups display various vulnerabilities to influence tools. Whereas reciprocation, which refers to feeling obliged to reply a communication, was found to be more effective in divulging older Internet users into revealing personal information, scarcity, denoting limited availability of something valuable, emerged to increase the likelihood of responding to phishing email for young Internet users.

Authority emerged to increase susceptibility to victimisation for all age groups. Apart from Cialdini's (2009) influence tools, fear appeals, urgency cues and time pressure were also found to impact email users' decisions when confronted with phishing attempts.

Fear appeals seem to be one of the most effective deception methods to coerce individuals to comply with given messages (Chen, 2017; Jansen and van Schaik, 2018). Witte (1992, p. 392) defines fear appeals as "persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends" (Witte 1992, p. 329). Fraudsters include fear-arousing statements together with bogus or fabricated scenarios to increase Internet users' perceived susceptibility to the presented threat. The results of the empirical studies indicate that account closure, account update, unauthorised access to the account, unusual account activities, a recent transaction from PayPal account are the most frequently used fear appeals (Vishwanath et al., 2011; Moore and Clayton, 2012; Harrison et al., 2016).

Urgency cues also appeared to be potent tools to coerce Internet users to make spurious decisions. The rationale behind the application of urgency cues is to divert Internet users' attention from phishing detection cues like security indicators while forcing Internet users to make hasty decisions (Wang et al., 2012). Research conducted by Vishwanath et al. (2011) support this thesis of diverted attention. They have found that disproportionate attention to urgency cues like *the update, access, protect, cancel, confirm* (Park and Taylor, 2015) decreased the amount of attention to other cues while leading Internet users to respond to a phishing email.

Time pressure conveyed in phishing emails was another factor found to impair Internet users' decisions. It is proposed that time pressure messages like *immediately, urgent, within one hour* increase the propensity to take risks (Young et al., 2012; Hu et al., 2015). Studies

conducted by (Zhang et al., 2012; Luo et al., 2013) have indicated that recipients who were exposed to email messages conveying time pressure were more likely to respond to phishing emails, however, Wang et al. (2012) found that computer literate email users were more successful in thwarting phishing attempts. Similarly, Kim and Hyun Kim (2013) who studied the impact of persuasive messages in phishing emails found no significant relationship between time pressure and the likelihood of responding to a phishing email. The discrepancies between the results of these studies may stem from the operationalisation and measurement differences. Fraudsters usually include several messages into emails to get the combined effect of each element. For instance, a fear appeal warning about an account closure may be backed up with time pressure indicating an urgent response. Thus, it might be the combined effect of these messages that leads Internet users responding to phishing emails. Measuring the effect of each element may be misleading.

**Individual Vulnerabilities**

Demographic characteristics like age and gender emerged as the individual vulnerabilities that were associated with susceptibility to phishing attacks (Heartfield et al., 2016; Oliveira et al., 2017). The results of the several empirical studies (Kumaraguru et al., 2009; Sheng et al., 2010; Khonji et al., 2013) indicate that young Internet users who are aged between 18 and 25 are more likely to respond phishing emails. However, Oliveira et al. (2017) who studied age differences in susceptibility to spear phishing attacks found that older women were more susceptible to spear phishing attacks. The results of the study also displayed that while young Internet users were more likely to respond phishing emails offering benefits like a winning prize, older Internet users were more likely to respond emails where reciprocation was suggested. These results may suggest that the hooks presented in emails have various impacts for different age groups due to variances in their expectations, and the way they

perceive online communication. Older Internet users may consider it rude to ignore emails, which leads them to engage with phishing emails.

The results of the past empirical research suggested that female Internet users were more susceptible to phishing attacks (Sheng et al., 2010; Halevi et al., 2015; Sun et al., 2016). For instance, Sheng et al. (2010) who conducted a role play survey found that female participants were more likely to click on the links presented in the phishing emails and susceptible to divulge personal information through bogus websites. However, the result of another study carried out by Mohebzada et al. (2012) who conducted a large-scale experimental phishing study among university staff, and students yielded no significant relationship between susceptibility to phishing attempts and gender. The discrepancy between the results of these studies may be attributed to computer self-efficacy. While the former study utilised a large-scale sampling, the latter used university staff and student as a sample population. Several studies have shown that college students or staff are more knowledgeable about IT related issues than population (Guy and Lownes-Jackson, 2010; McCoy, 2010).

#### 3.3.1.2 Website Phishing

Website phishing is the second variation of phishing attempts. Online perpetrators create bogus websites to divulge Internet users to reveal their personal financial information (Smith, 2010). These websites may be summarised into three broad categories. The first category of websites are the bogus websites that mimic the genuine websites. Offenders create these types of websites to acquire personal or financial information of Internet users (Mathew et al., 2010). Internet users are directed to these websites either by a link presented in a phishing email or through search engines (Kienzle and Croall, 2009). These fake websites usually imitate financial websites like online banking or e-wallet websites. The second type of bogus websites is created for consumer fraud or shopping fraud attempts. These websites either offer

some services for higher prices or allegedly sell products for lower prices (Reisig and Holtfreter, 2013). The last type of bogus websites involves those websites created to steal personal information through malware infection. There are many websites that offer free streaming of movies, drama series or sports activities as well as free adult content. However, most of these websites bear the risk of malware infection through drive-by-downloads and pop-up windows (Bossler and Holt, 2009; Rafique et al., 2016; Goldsborough, 2017).

Despite the significant threat posed by bogus websites, most of the academic effort is directed to technical solutions such as bogus website detection. However, little is known about the relationship between engaging with those websites and the risk of becoming a victim of economic cybercrime. This thesis aims to fill this gap by researching the impact of accessing bogus websites on the likelihood of losing money online.

### 3.3.2 Malware Infection

Malware, which is the combination of malicious and software, covers a wide range of code based online threats like computer viruses, trojan horses or keyloggers (Ena, 2008). Infected files, freely distributed programs or websites are utilised to infect target electronic devices (Bossler and Holt, 2009; Ma et al., 2012). Malware infection poses a significant threat to electronic devices security, Internet users' personal information and privacy (Bettany and Halsey, 2017).

Past research about malware infection showed that routine online activities were associated with the risk of malware infection. (Reyns, 2015) found that online shopping, online social networking and online booking were more likely to be a victim of malware infection. The results of Ngo and Paternoster (2011) indicated that Internet users who clicked on the links presented in email attachments were less likely to be a victim of malware infection. This unexpected result may be attributed to the wording of the questionnaire which caused confusion

about the time ordering of the events. Participants who were less likely to click on the link might be those who were already victimised. Hence, the victimisation experience may have promoted safeguarding behaviour. Leukfeldt (2015) found an association between malware infection and online activities like downloading and online gaming. Downloading infected files may be an explanation for this sort of association. However, Bossler and Holt (2009) found no relationship between legitimate online activities like using chat rooms and email and risk of malware infection. The results of Holt and Bossler (2013) who examined the relationship between online routine activities and malware infection suggested that it is engaging with online deviant activities rather than legitimate online activities that increase the risk of malware infection. They identified viewing pornography, pirating media, unauthorised access to someone's Internet connection and pirating media as the correlates of malware infection.

Malware is mostly utilised as a tool to commit more serious crimes like hacking, website phishing or identity theft (Sood and Enbody, 2011; Grégio et al., 2014). The relationship between malware infection and other forms of cybercrime (i.e. hacking, phishing or identity theft) have been researched. However, little is known how malware infection facilitates economic cybercrime victimisation. This thesis explores the relationship between malware infection and economic cybercrime victimisation.

### 3.3.3 Hacking

Newman and Clarke (2013) argue that the eventual goal of hackers is to acquire information. They categorise targeted information as "intellectual property, intelligence, information systems and services of various kinds (i.e. banking, purchasing)" (Newman and Clarke, 2013, p. 18).

Hackers carry out hacking attempts to acquire information either for their own goals or the third parties. Several studies have found that hacked information is sold through online markets. Holt (2013) examined ten publicly accessible Russian web forums utilised to exchange hacked information or hacking tools. Another empirical study conducted by Hutchings and Holt (2015) also researched online black markets. Their research findings yielded that hackers not only sell stolen data, but they also help other hackers to improve their skills through tutorials.

Hacking is generally associated with the macro level threats such as data breaches of big companies or governmental bodies (Greene, 2015; Elhai et al., 2017). However, the results of the past empirical research indicate the presence of a relationship between hacking and cyber victimisation at the individual level. van Wilsem (2013b) studied online correlates of hacking victimisation and the relationship between experiencing hacking and online harassment victimisation. The results of the study found no association between online communicative activities like participating in online forums or using social media and the risk of experiencing hacking victimisation. However, Reyns (2015) who researched online lifestyle correlates of hacking victimisation found that engaging with online social activities were a risk factor hacking victimisation. The results of the study indicate that sharing personal information online, accessing the Internet for online social networking and online booking emerged to increase the risk of hacking victimisation. Similarly, Leukfeldt and Yar (2016) identified engaging with online social activities like participating in online forums and social networking websites as the risk factor for hacking victimisation. Engaging with deviant online activities like pirating media, hacking and accessing adult content were also found to be risk factors for hacking victimisation (Bossler and Holt, 2009; Holt and Copes, 2010). For instance, Bossler and Holt (2009) found that those who engaged with hacking run the risk of malware victimisation from other hackers.

Hacking victimisation is also found to be associated with other forms of cyber victimisation such as identity theft (Reyns and Henson, 2016), online harassment (van Wilsem, 2013b), malware infection (Bossler and Holt, 2009; Chu et al., 2010). For instance, Reyns and Henson (2016) who studied identity theft victimisation in Canada found that experiencing hacking increased the risk of identity theft victimisation. Correspondingly, van Wilsem (2013b) identified a significant overlap between hacking and online harassment victimisation. However, the relationship between hacking and economic cybercrime has not been researched yet. This thesis will address the gap in the literature by examining the association between experiencing hacking victimisation and the likelihood of facing economic cybercrime victimisation.

## 3.4 Economic Cybercrime Victimisation

Economic cybercrime is an umbrella term that encompasses various financially motivated online offences (Levi et al., 2015). Previous cybercrime victimisation studies researched different types of economic cybercrime in separate studies. This section of the chapter reviews the three most common forms of economic cybercrime victimisation.

### 3.4.1 Card-not-present Fraud

Card-not-present Fraud is the unauthorised use of banking cards' information while the physical card is not present (Montague, 2010). Precautions applied to prevent skimming and to scan the physical card as well as increased volume of online transactions have motivated online offenders to devise new strategies to acquire Internet users' payment card information UK (Wall, 2010b; Reyns and Henson, 2016). The extant research on the payment methods mainly focus on the factors affecting customers' payment method choice (i.e. Ching and Hayashi, 2010; See-To et al., 2014; Arango et al., 2015) and technical solutions to reduce the risk of

financial loss through online attacks (i.e. Sendo et al., 2005; Ahmad et al., 2016; Vishal and Johari, 2018). Only a handful of studies have researched the correlates of card-not-present fraud. Those empirical studies generally examined the relationship between low-self control, which leads to engaging with risky online activities and credit card fraud victimisation.

Past research related to credit card fraud yielded inconsistent results with regards to the relationship between low-self control and CNP fraud victimisation. Bossler and Holt (2010) who explored the impact of self-control on the various forms of cybercrime victimisation found no relationship between low-self control and credit card information theft. However, Holtfreter et al. (2010) found that Internet users with low-self control were more likely to be a victim of credit card fraud due to engaging with risky online activities which increased their exposure to perpetrators. Holtfreter et al. (2008) researched a different aspect of card-not-present fraud victimisation. They researched the impact of online credit card fraud victimisation on the online behavioural adaptation. The research results indicate that financially impulsive respondents were less likely to limit their online actions, which in turn increased the risk of victimisation. A recent study researching the behavioural impact of credit card fraud victimisation showed that credit card fraud victims were less likely to use online payment methods (Kahn and Liñares-Zegarra, 2016).

### 3.4.2 Online Banking Fraud

As in the case of card-not-present fraud, online banking fraud is a neglected research subject in criminology. Most studies in the literature have generally focused on the technical remedies to prevent online banking account takeovers and deter attacks targeting banking systems (i.e. Wei et al., 2013; Carminati et al., 2015; Abdallah et al., 2016). The factors affecting Internet users' online banking acceptance are other popular research subjects in the literature (i.e. Pikkarainen et al., 2004; Yap et al., 2010; Chandio et al., 2017). Few scholars

have conducted research on the causes of online banking fraud. Jansen and Leukfeldt (2015) explored the causes of online banking fraud in Netherland through qualitative analysis of six hundred victimisation cases reported by a Dutch bank. The results of this study pointed out phishing and malware infection as the main causes of being an online banking fraud victim. Jansen and Leukfeldt (2016) examined victim facilitation in online banking fraud victimisation through Routine Activities Theory and Protection Motivation Theory lenses. Malware infection and phishing emerged as the precursors of the online banking fraud victimisation. Negligence and low-self efficacy were reported as the facilitating factors of victimisation. Though these two studies contributed to the literature by yielding malware infection and phishing as the antecedents of online banking fraud, they failed to examine the causal links between Internet users' online behaviours and becoming a victim. Moreover, Reyns (2013) and Reyns and Henson (2016) established the relationship between identity theft and online banking usage. Reyns and Henson (2016) found that online banking usage increased the risk of identity theft by 13%. However, their research failed to account for why and how online banking increased the odds of identity theft victimisation. This thesis addresses these shortcomings of past research by examining the victimisation processes of economic cybercrime victims.

### 3.4.3 Online Identity Fraud

It might be suggested that identity theft is one of the most popular crimes that attracted public attention and concern in recent years (Copes et al., 2010; Holt and Turner, 2012; Reyns and Henson, 2016). Despite growing interest in identity theft and identity fraud victimisation, there is a dearth of empirical research on the behavioural factors leading to victimisation (Holt and Bossler, 2014; Paek and Nalla, 2015; Reyns and Henson, 2016). Scholars researching cybercrime or economic cybercrime are mostly interested in the trends, the economic impact

and cost of identity theft at the national and international level. Only handful research studied online lifestyle correlates of identity fraud victimisation. Holt and Turner (2012) examined the correlates of online identity theft among college students, staff and faculty of a university in the US. The results of the study indicated that risky online activities increased the odds of facing online identity theft and male Internet users were more likely to engage with risky online activities. However, they failed to identify which online activities were risky and which of these risky online activities boosted the risk of victimisation. Engaging with online gambling also emerged to be a 'deviant' online activity that increased the risk of identity theft. It appears that perpetrators utilise gambling sites both to steal personal identifying information and money laundering (Levi, 2009; McMullan and Rege, 2010; Banks, 2012).

Reyns (2013) explored the association between online routine activities and identity theft victimisation through British Crime Survey (BCS) 2008/2009 by utilising Routine Activities Theory (RAT) as a theoretical framework. He operationalised online identity theft with questions measuring credit card fraud and banking fraud. Accessing the Internet for online communicating, shopping, online banking and downloading appeared to be risk factors for online identity theft. Despite making an invaluable contribution by being one of the first empirical studies researching online correlates of online identity theft, there is a methodological pitfall of this study. As the author also highlighted in the limitation section of the paper, the measurement of online identity theft was problematic as BCS 2008/2009 did not distinguish online and offline elements of credit card fraud and banking fraud. Hence, it was impractical to measure the online aspect of identity theft victimisation. Failure in displaying conceptual differences between identity theft and identity fraud was another limitation of this study. This study operationalised identity fraud variables (credit card fraud and banking fraud) as the proxy of identity theft victimisation. However, Wall (2013d) differentiates identity fraud from

identity theft in that identity fraud is the application of identity theft, which means that every identity theft incident does not necessarily lead to financial loss.

Williams (2015) studied online identity theft at country and individual level through RAT perspective. The most significant contribution of this study was to show the relationship between selling goods online and risk of online identity theft. Illustrating the importance of places that Internet users access the Internet was also notable. The results of the study indicated that those using public computers like the university and library computers were at increased risk of victimisation. Lack of association between legitimate online activities and online identity theft was another significant finding, which contradicted previous studies (Pratt et al., 2010; Reyns, 2013).

Paek and Nalla (2015) investigated the online behavioural correlates of online identity theft in Korea. They operationalised legitimate online usage with the online activities such as using the Internet for online banking, shopping, chatting, instant messaging, gaming and peer-to-peer activities whereas they operationalised deviant online activities as illegal software downloading, using another person's resident registration number and posting negative comments about someone. They obtained two dependent variables, legitimate and deviant online behaviour. The results of the study found a strong association between legitimate online activities and online identity theft victimisation and a weak relationship between deviant online behaviour and victimisation. Their study contributed the cybercrime literature by highlighting the importance of online behavioural correlates of identity theft. However, they failed to measure the impact of individual online behaviours on the risk of victimisation as they combined all online activities to obtain a single variable. Furthermore, they considered peer-to-peer activities as a legitimate online activity. However, peer-to-peer programs are utilised to share copyrighted materials without paying any fee, an action which indicates digital

copyright infringement (Rowstron and Druschel, 2001; Gull and Flowers, 2016). Thus, this online activity should have been considered a deviant online activity.

Another empirical study conducted by Reyns and Henson (2016) explored the online determinants of online identity theft victimisation in Canada through the lenses of Routine Activities Theory. This study utilised the Canadian General Social Survey to conduct quantitative analysis. The results of their study indicated that using the Internet for online banking and online shopping increased the odds of identity theft victimisation. Hacking and phishing also emerged as the risk factors for online identity theft victimisation. Contrary to most of the cybercrime studies the results of this study can be generalised to the Canadian population as they utilised a national survey that sampled adults.

This section of the chapter reviewed the results of empirical cybercrime victimisation research examining the causes of being a victim of economic cybercrime. This next section of the chapter presents the results of empirical studies investigating the emotional impacts of victimisation experiences and the influence of emotional reactions on Internet users' online behaviours and safeguarding measures.

## 3.5 Emotional and Behavioural Responses to Victimisation Experiences

Negative life experiences and criminal victimisation may have adverse effects on individuals' psychological well-being (Yin, 1980). Adverse life events can produce stress, shock, panic, anger, anxiety and fear of crime (Gale and Coupe, 2005). This part of the last section defines fear of crime, which is considered to be the strongest emotional reaction to negative life events (Liska et al., 1988; Heath and Gilbert, 1996), juxtapose it to other emotional responses (concern, perceived risk and anxiety) and then reviews the empirical fear of crime research.

### 3.5.1 Fear of Crime

While economic cybercrime impacts individuals, financial institutions and governments financially, it may also have adverse impacts on individuals' psychology, social relations and online lifestyles (Stafford et al., 2007; Reyns, 2013; Paek and Nalla, 2015).

Garofalo (1981, p. 841) defines fear of crime as *"emotional reaction characterized by a sense of danger and anxiety about physical harm".* As can be seen, this definition restricts the fear of crime to negative emotions produced by physical harm. Garofalo (1981) put forwards the intention of differentiating between the emotional reactions produced by the worry of property loss and fear of potential physical harm as a rationale of this limitation. He argues that while the threat of property loss initiates a cognitive process, that of physical harm sparks an intrinsic emotive reaction. This explanation suggests that Garofalo (1981) make a distinction between worry and fear as well as cognitive and emotional aspects of fear of crime. Although Garofalo (1981) accepts that loss of property may also create a sense of fear, he argues that this fear is the reflection of the fear of physical harm. For instance, the possibility of encountering a physical attacked in case of coming across with the burglar.

Initially, Ferraro and Grange (1987, p. 72) defined fear of crime as "negative emotional reactions to crime or the symbols associated with crime". Later, Ferraro (1995, p. 23) defined it as "an emotional response of dread or anxiety to crime or symbols that a person associates with crime" Another definition provided by Henson and Reyns (2015, p. 92) conceives fear of crime as "an emotional response to a danger or threat of an actual or potential criminal incident." Based on these definitions it can be said that fear of crime is a negative emotional reaction to present or anticipated danger or threat.

#### 3.5.1.1 Fear of Crime versus Concern

The difference between concern and fear of crime is one of the issues in fear of crime debate. It is Furstenberg (1971) who firstly maintained that fear of crime is not the only concept to define emotional reactions to crime events (Smith, 1984; Clark, 2003). Furstenberg (1971) argues that fear of crime and concern about crime are used interchangeably and this usage creates conceptual confusion. He argues that concern about crime is not related to harm directed to an individual; rather it is "resentment of social change and resistance to further alterations in the status quo" . In other words, concern about crime is related to the seriousness of crime in general. Furstenberg (1971) further argues that fear of crime is individuals' perceptions about the crime in their neighbourhood. He suggests that fear of crime is greatly influenced by crime rates in the neighbourhood. It can be argued that Furstenberg (1971) equates fear of crime with a perceived risk of victimisation (Sundeen and Mathieu, 1976). Lotz (1979) supported Furstenberg's (1971) distinction between concern and fear of crime. However, his study suggested that conservative attitudes impact the level of concern, while Furstenberg (1979) proposed that concern is affected by the resentment to social changes. Later, Ferraro and Grange (1987) posit that concern, which is the opinion about the seriousness of the crime, is conceptually different from fear of crime, however, fear of crime is also conceptually different from the perceived risk of victimisation. Skogan (1999) argues that concern about crime is individuals' assessment of the seriousness of the crime for society. Concern about crime fuelled by crime statistics, media representation of crime and rumours about crime events as well as social changes (Garofalo, 1981; Skogan and Maxfield, 1981; Cavender, 2004).

#### 3.5.1.2 Fear of Crime versus Perceived Risk of Victimisation

Although initial fear of crime studies conceptualised fear of crime as a single phenomenon, it is argued that fear of crime and perceived risk of victimisation are conceptually

different after the 1980s (LaGrange and Ferraro, 1989; Warr, 1993; Ferraro, 1995; Rountree and Land, 1996). Whereas fear of crime refers to a set of emotional reactions, the perceived risk of victimisation encompasses the cognitive assessment of the likelihood of experiencing victimisation (Rengifo and Bolton, 2012). It should be noted that fear of crime and perceived risk of victimisation are not conceptualised as separate constructs rather two interrelated concepts (Ferraro and Grange, 1987; LaGrange and Ferraro, 1989; Ferraro, 1995). Recent empirical research appears to support this proposition of interconnectedness (Kanan and Pruitt, 2002; Wyant, 2008; Cook and Fox, 2011). It should also be noted that there is a tendency in fear of crime literature to measure these two constructs as a single phenomenon. Rader (2004) argues that measuring fear of crime and perceived risk of victimisation is practically impossible due to the interrelation between these two concepts. Examining these two concepts as a whole may yield more reliable results (Rader, 2004; Rader et al., 2007; May et al., 2010). Rader (2004, p. 691) names combined the use of these concepts as "the threat of victimisation".

#### 3.5.1.3 Fear of Crime versus Anxiety

The relationship and distinction between fear of crime and anxiety is another facet of fear of crime debate in the literature. Later Ferraro (1995) altered the definition of fear of crime by including the terms, anxiety and dread. Ferraro (1995, p. 23) defines it as "an emotional response of dread or anxiety to crime or symbols that a person associates with crime". However, he did not give any reference for the reason of inclusion of anxiety and dread into the definition. Hollway and Jefferson (1997) perceive anxiety as the innate universal nature of human being. They argue that anxiety is not shaped by social forces; rather it shapes the way individuals experience the risk of victimisation. Anxiety is the unconscious estimation of things perceived as a threat to self. They argue that fear of crime is the expression of anxiety caused by uncertainties in every aspect of life event. Binder (1999) suggests that anxiety is the

anticipation of potential harm where the source of this feeling is unclear. He also makes a distinction between fear and anxiety. He argues that while fear denotes emotional reactions to immediate danger, anxiety refers to negative emotions caused by past or future events. He further argues that most of the empirical research measure anxiety rather than fear of crime. Binder (1999) suggests that fear is the emotional manifestation for something known or present anxiety is a reaction to an anticipated danger.

All in all, it can be maintained that fear of crime ranges from individual-level emotional manifestations to the likelihood of experiencing victimisation to macro level perceptions of the extent of the crime in society (Ferraro and Grange, 1987; Rountree and Land, 1996). The extent and the intensity of the range of emotions may display variations based on the contextual factors (Bannister and Fyfe, 2001).

As noted above Rader (2004) suggests researching different dimensions of fear of crime holistically to prevent measurement errors and ambiguity. Following this line of logic, this thesis examines the fear of economic cybercrime and perceived risk of economic cybercrime victimisation holistically. Review of empirical studies pertaining to fear of cybercrime and perceived risk of cybercrime will be presented together.

### 3.5.2 Fear of Cybercrime

Despite a considerable number of studies researching the fear of traditional crimes, there is a lack of empirical research on fear of cybercrime (Henson et al., 2013; Yu, 2014). Only a handful studies examined the extent and impacts of fear of cybercrime. Though a great deal of growing body of fear of crime studies have researched fear of online interpersonal victimisation such as cyber harassment or cyberbullying (i.e Henson, 2011; Yu, 2014; Pereira and Matos, 2016; Pereira et al., 2016; Keith, 2018), fear of cybercrime in general (Maddison and Jeske, 2014; Brunton-Smith, 2017; Virtanen, 2017) and fear of online identity theft

(Roberts et al., 2013; Hille et al., 2015; Cornelius, 2016) have also been researched. However, the fear of economic cybercrime has not been researched yet. This thesis aims to address this gap in the literature. Determinants of fear of crime are generally summarised into three groups: personal traits, social determinants and psychological factors (Yin, 1980; Skogan, 1986; Box et al., 1988). The review of the empirical research will be based on this categorisation of determinants of fear of crime.

#### 3.5.2.1 Personal Traits

Demographic characteristics gender, age and race, are considered to be determinants of fear of crime. Fear of traditional crime studies consistently suggested gender differences as a predictor of fear of crime (Warr, 2000; Franklin and Franklin, 2009; May et al., 2010). The extant research on fear of crime indicated that females are more fearful than males (Schafer et al., 2006; Jennings et al., 2007; May et al., 2010; Gutt and Randa, 2016). Three key approaches suggested explaining the prevalence of fear of crime among women is identified. Social learning approach suggests that messages indicating role plays and gendered norms are internalised by individuals (Cobbina et al., 2008; van Eijk, 2017). Fear of crime is the manifestation of learned gender expectations since patriarchal societies impose being fearless as a male role play (Madriz, 1997). Sex assault approach conceives fear of being a victim of a sex assault as an underlying reason for the general fear of crime. It is argued that females are fearful of ending every crime with a sex assault (Warr, 1993; Ferraro, 1996). Thus, the perception of the likelihood of a sex assault increases the fear of crime among female (Fisher and Sloan, 2003). Vulnerability perspective strives to account for the prevalence of fear of crime among females with a sense of lack of protection due to physical and social vulnerability (Stanko, 1995; Pain, 2001). It is suggested that women who do not consider themselves strong

enough to thwart a potential threat are more likely to be fearful of crime (Rader and Haynes, 2011).

Fear of cybercrime studies yielded conflicting results pertaining to the gender difference in fear of cybercrime. Fear of online interpersonal cybercrime studies proposes that females are more fearful of experiencing cyber harassment or cyberbullying than males (Henson et al., 2013; Pereira et al., 2016; Virtanen, 2017). However, the results of studies researching online identity theft and malware infection suggest no gender difference in fear of cybercrime (Roberts et al., 2013; Yu, 2014). The results pertaining to the prevalence of fear of online interpersonal crime (cyber harassment and cyberbullying) suggest that fear of cybercrime may be conceptually different from fear of traditional crimes. Implications of these results will be discussed together with that of this thesis in Discussion Chapter.

Age is another demographic characteristic considered to have an impact on the fear of crime. Fear of traditional crime studies associated high levels of fear of crime with older people (Ortega and Myles, 1987; Covington and Taylor, 1991; Moore and Shepherd, 2006; Boateng, 2016). Skogan and Maxfield (1981) argue that vulnerability which has two dimensions as physical and social, impacts fear of crime among older people. It is suggested that old person perceptions related to their physical inability to thwart a physical attack alleviate the fear of crime in general (Box et al., 1988). With regards to fear of cybercrime, the results of cybercrime studies indicated no age difference in fear of cybercrime (Henson et al., 2013; Roberts et al., 2013; Yu, 2014). These results that contradict with those of fear of traditional fear of crime indicate the existence of some factors that moderate the relationship between fear of cybercrime and age.

#### 3.5.2.2 Social Determinants

Previous victimisation experience (direct victimisation experience) and interactions about crime like media news or other individuals' victimisation experiences (indirect victimisation experience) were proposed to be social determinants of fear of traditional crime (Yin, 1980; Silverman and Kennedy, 1985; Skogan, 1986). The results of the previous fear of traditional crime studies suggested that both previous victimisation experience (Smith and Hill, 1991; Russo and Roccato, 2010; Sironi and Bonazzi, 2016) and interactions about crime (Garofalo, 1981; Swaray, 2007; Tseloni and Zarafonitou, 2008; Grubb and Bouffard, 2015)increased the fear of crime. Fear of cybercrime studies yielded contradictory results. It appears that both direct and indirect victimisation experiences increased the fear of online interpersonal victimisation (Alshalan, 2006; Henson et al., 2013; Yu, 2014). However, the results of Yu (2014) suggest the presence of a statistically significant relationship between previous victimisation experience and computer virus infection, whereas no significant relationship was found between fear of cybercrime and digital piracy and online scams.

#### 3.5.2.3 Psychological Factors

Perceived risk of victimisation and perceived seriousness of victimisation are proposed to be psychological determinants of fear of traditional crime (Yin, 1980; Vitelli and Endler, 1993). As it was noted earlier, perceived risk is identified as a separate concept from fear of crime (Ferraro and Grange, 1987; Ferraro, 1995). Empirical research indicated that there is a reciprocal relationship between fear of crime, perceived risk of victimisation and perceived seriousness of victimisation. The relationship between these constructs will be dealt with in detail in the following section where the impact of victimisation will be discussed.

### 3.5.3 Consequences of Fear of Cybercrime

Skogan (1999) asserts that individuals display their fear of crime by changing their living patterns. It is (Furstenberg, 1972) who initially proposed that behavioural responses can be categorised into two distinct classes: avoidance and mobilization (Riger et al., 1982; Lab, 1990). Avoidance strategies are those applied to decrease the risk of victimisation (Furstenberg, 1972). Avoiding going out at night or doing less shopping is the tactics employed to manifest fear as a behaviour. Spatial avoidance which is defined as staying away from the areas labelled as dangerous is considered to be one of the most common forms of avoidance behaviour (Warr, 1993). Mobilization techniques are safeguarding measures applied to protect properties and individuals (Rosenbaum, 1988) Alarms, locks or guns are the devices that can be utilised to maintain mobilization. (Taylor, 1996). Cybercrime studies categorised behavioural responses into two groups: changes in security intention and online lifestyles.

#### 3.5.3.1 Security intention

Previous Internet security studies suggested that negative online experiences impact Internet users' security intentions. Claar and Johnson (2012) investigated home computer users' behavioural adaptations to use computer security software. They have found that participants who had prior security problems felt more vulnerable and adopted security precautions to prevent future incidents. Similarly, the results of Tsai et al. (2016) and Chen et al. (2016) indicate that those who had faced online threats were more likely to adapt to security precautions. Mwagwabi et al. (2014) researching the effect of user perception of passwords and security threats on compliance with password guidelines point out that those who were exposed to hacking attempt were more likely to comply with password and security guidelines. Thompson et al. (2017) examined the determinants of the home computer and mobile device

security behaviour. Their findings demonstrate that previous experience related to security breaches enhanced security intentions of Internet users.

#### 3.5.3.2 Behavioural change

Studies researching the impact of fear of crime on Internet users shopping behaviour indicated that fear of crime and perceived risk of victimisation decrease Internet users online shopping intention (Forsythe et al., 2006; Kukar-Kinney and Close, 2010; Chang and Wu, 2012; Dai et al., 2014). The relationship between perceived risk and online behavioural adaptation was also researched. Reisig et al. (2009) researched the impact of perceived risk of credit card theft victimisation on Internet users' online behaviours through a telephone survey conducted with 573 participants in Florida. The research yields that Internet users with high levels of perceived risk were more likely to decrease their online shopping and spent less time online. Similarly, D'Alessandro et al. (2012) researching the impact of perceived risk on expensive and high-risk products like gemstones found that online shopping intention shown a decrease as a result of the perceived risk of being defrauded. Henson et al. (2013) examined the relationship between fear of online crime, perceived risk of online victimisation among college students. The results of the study revealed a positive relationship between fear of online crime and perceived risk of online victimisation.

As can be seen, previous security intention studies mainly measured impacts of negative online experiences such as virus infection or phishing attempt on Internet users' security intentions. However, the impacts of economic cybercrime victimisation on security intention has not been researched yet. Moreover, behavioural adaptation studies were generally concerned about Internet users' shopping intention. The scope of previous research was limited. Hence, little is known how victimisation experiences influenced Internet users' decision with engaging other normal and deviant online activities. This thesis addresses these

limitations of previous studies by examining the effects of economic cybercrime victimisation on Internet users' security intentions and online lifestyle through the lenses of approach-avoidance coping paradigm as a conceptual framework. This application provides a valuable methodological strength while researching this issue.

## 3.6 Summary

This chapter has provided an outline of cybercrime victimisation literature. As the review indicated despite a growing body of cybercrime victimisation research, there is a dearth of theoretically informed economic cybercrime victimisation studies which examine the phenomenon holistically. While a small body of research is interested in correlates of target suitability/target attractiveness, a considerable portion of cybercrime studies dealt with discerning the relationship between Internet users' demographic characteristics, online lifestyles and risk of experiencing cybercrime victimisation. Only a handful of studies investigated the emotional impacts of victimisation experiences on Internet users' behavioural responses and security intentions.

The main limitation of cybercrime studies employing LRAT as a theoretical framework limited their scope to examining the influence of Internet users' lifestyles and demographic characteristics on the risk of cybercrime victimisation. It appears that this approach prevented scholars from exploring impacts of macro variables such as technological vulnerabilities or data breaches of companies/agencies holding personal information of the Internet users. This thesis aims to contribute to the literature by providing a more detailed account of the causes of economic cybercrime victimisation. To that end, new theoretical and conceptual lenses (PMT and Approach-Avoidance) are applied to better understand both causes and adverse impacts of economic cybercrime victimisation. The next section will present the mixed-methods research design adapted to research economic cybercrime victimisation.

# Chapter 4 Methodology

## 4.1 Introduction

This chapter presents the research design and the research methodology as well as the underpinning methodological and epistemological considerations while choosing a mixed methods approach to research economic cybercrime victimisation. The chapter begins by providing the rationale for implementing a mixed methods research paradigm to examine economic cybercrime victimisation. It then goes on to describe the quantitative research design and analytical procedures utilised to address the research questions. The chapter concludes with a reflexive account of the qualitative research process.

## 4.2 The Rationale for Utilising a Mixed Methods Research Paradigm

Using multiple approaches to understand the social world is not a new issue and it can be traced back to Ancient Greek philosophers' ideas of viewing reality (Johnson et al., 2007). However, it was the introduction of the concept of triangulation that made social scientists debate the complimentary use of quantitative and qualitative research methods. Campbell and Fiske (1959) and Denzin (1978) may be considered as the founding theorists of triangulation in social sciences (Carter et al., 2014; Joslin and Müller, 2016), though, Denzin's (1978) conceptualisation of triangulation gave rise to methodological concerns about using multiple research methods in a single research study. These concerns among scholars initiated the debates around the paradigm-method fit, which centres around the question of the compatibility of the philosophical stances and the research paradigms (Hanson et al., 2005).

Rossman and Wilson (1985) aiming to synthesise paradigm debates distinguish three approaches to this issue of paradigm-method fit: purist, situationalist and pragmatist. While

purists (i.e.Smith, 1983; Collins, 1984) opposed the compatibility of the qualitative and quantitative research paradigms due to their inherent epistemological and ontological differences, situationalist scholars (i.e.Rosenblum and Louis, 1981; Kidder and Fine, 1987) partly supported the incorporation of two research paradigms in one single study. Though they believed that certain methods offer a more suitable research design in some circumstances (Rossman and Wilson, 1985; Hanson et al., 2005). Contrary to these views, pragmatists argue that mixed methods research design, with the aim of gaining in-depth understanding through corroborating strengths of the two research paradigms, is applicable to any research question regardless of the circumstances (Johnson and Turner, 2003; Johnson and Onwuegbuzie, 2004). Having a pragmatist worldview, this reseach aiming to *understand* economic cybercrime victimisation rejects the idea of incompatibility of the research paradigms and lends support to incorporating quantitative and qualitative research methods to conduct a rigorous research (Johnson and Onwuegbuzie, 2004).

A comprehensive literature review of relevant published papers and books about mixed methods has shown that it is difficult to find a commonly accepted definition of mixed methods. Whereas some definitions stress mixing of qualitative and quantitative data (Ivankova et al., 2006) others emphasise the benefits of integrating analysis procedures and drawing inferences (Teddlie and Tashakkori, 2006; Mertens and Tarsilla, 2015). Nonetheless, Johnson et al. (2007, p. 123) provide a holistic definition of mixed methods design: *"Mixed methods research is the type of research in which a researcher or team of researchers combines elements of qualitative and quantitative research approaches (e.g., use of qualitative and quantitative viewpoints, data collection, analysis, inference techniques) for the broad purposes of breadth and depth of understanding and corroboration."* The significance of this definition for this thesis is its emphasis on in-depth understanding and corroboration since the main rationale for employing a mixed methods approach was to make complimentary use of quantitative and qualitative

research methods to understand economic cybercrime victimisation holistically.

Research aims and research questions are considered to be the primary factors in designing research (Ivankova et al., 2006; Creswell and Plano Clark, 2007). The main advantage of a mixed method research design is its ability to address various types of research questions that cannot be addressed with a single research method (Onwuegbuzie and Leech, 2006; Tashakkori and Creswell, 2007). My first research aim was to test the applicability of Lifestyle Routine Activities Theory to economic cybercrime victimisation, which can best be addressed with a quantitative research design due to statistical rigour of quantitative analysis to test a hypothesis (Johnson and Onwuegbuzie, 2004; Greene, 2008). My second research aim was to understand underlying mechanisms that facilitate victimisation, while the last research aim was to understand how the victimisation experiences impact Internet users. Qualitative research methods are suitable to reach these two aims. A mixed methods research design emerged to be the most suitable research paradigm to address these questions. Triangulation, complementarity, development, initiation and expansion are the five conceptual elements to be considered prior to design a mixed methods research (Greene et al., 1989). These conceptual elements that informed the decision of applying a mixed methods paradigm will now be evaluated with a reflexive account of the research process.

Triangulating quantitative results with qualitative semi-structured interviews is a significant benefit of the mixed methods research design. Greene et al. (1989) argue that enhancing validity is the main rationale for triangulation since incorporating strengths of two or more research paradigm may offset intrinsic limitations of each research method, which in turn overcomes the biases each method poses. In addition, Hammersley and Atkinson (2007, p. 184) contends that "what is involved in triangulation is not the combination of different kinds of data per se, but rather an attempt to relate different sorts of data in such a way as to counteract

various possible threats to the validity of our analysis." Interviews can be the best tool to triangulate the results of quantitative analysis (Flick, 2008). Although statistical analyses of the Crime Survey for England and Wales (CSEW) 2014/2015 produced generalizable findings, due to the pitfalls of statistical analysis procedures, causal connections between variables might justifiably be open to discussion. To make up for this disadvantage, I benefitted from semi-structured interviews that were designed to both explore new aspects of victimisation and to triangulate results of the quantitative analyses conducted at the first phase of the research.

Complementarity is another advantage of utilising a mixed methods research methodology. Whereas triangulation refers to combining strengths of research methods to justify research findings, complementarity denotes enriching research findings through examining different facets of the phenomenon under consideration (Rocco et al., 2003; Johnson and Onwuegbuzie, 2004; Petter and Gallivan, 2004). Onwuegbuzie and Johnson (2006, p. 51) argue that mixing two research paradigms does not only mean triangulating or corroborating two approaches, but it also means putting "complementary strengths" of these two approaches. Semi-structured interviews with victims of economic cybercrime were conducted with the aim of examining the phenomenon through lenses of victims, and with the aim of furthering understanding of economic cybercrime victimisation. Complimentary use of both methods was intended to help form a more sophisticated picture of economic cybercrime victimisation, encapsulating both the experiences of victims and trends reflected in statistical analyses (Clark and Creswell, 2014). Additionally, complementary use of two or more research methods also enables clarification of the findings yielded from another method (Rossman and Wilson, 1985; Onwuegbuzie and Collins, 2007). For instance, statistical analysis results demonstrated that online shopping increased the risk of victimisation. However, it was not clear why online shopping poses a threat. Semi-structured interviews with victims unearthed the causal mechanisms that made online shopping a risk factor.

The third rationale to apply a mixed methods research approach was development. In a mixed methods paradigm, one research method may serve as a basis to develop another research design (Caracelli and Greene, 1993). This requires sequential use of two or more research paradigms to develop a sampling strategy or research aims (Teddlie and Yu, 2007). The vulnerable population was discerned through statistical analysis of CSEW 2014/15, and these results were utilised to form sampling criteria for semi-structured interviews. Moreover, quantitative analysis results informed the development of the interview guide. Quantitative analyses results informed semi-structured interviews by identifying new relevant interview questions (Creswell, 2009) or by elaborating them (Creswell et al., 2003).

The results of a research method may sometimes indicate the need for exploring an aspect of the phenomenon, which was not foreseen prior to the research process (Onwuegbuzie and Teddlie, 2003). A mixed methods research design aids the researcher "to gain new insights and to reframe the original understanding of the problem." (Petter and Gallivan, 2004, p. 6). For instance, the results of quantitative analysis pertaining to the impacts of electronic device usage on the risk of victimisation, let me think about the effect of other technological elements of cyberspace such as Wi-Fi usage. This idea initiated examining technological vulnerability aspect of economic cybercrime victimisation.

Expansion is the last advantage of applying a mixed methods research design to be considered. The rationale for applying multiple research paradigm is to investigate various components of the phenomenon to expand the scope of the study (Greene et al., 1989; Greene, 2008). For instance, while quantitative research design tested the applicability of LRAT to economic cybercrime, qualitative semi-structured interviews were used to expand findings of quantitative analyses by providing in-depth perspectives of victims. Moreover, semi-structured interviews were carried out with the aim of understanding unexpected results of statistical

analyses conducted in the first phase (Rossman and Wilson, 1985; Morse, 1991). The quantitative phase of the research indicated that online government website usage increased the risk of victimisation. The causes of this unanticipated result were explored through semi-structured interviews.

## 4.3 Research Design and Analytic Strategy

Several authors attempted to create a typology of mixed methods research design. For example, Johnson and Onwuegbuzie (2004) describe research designs as a continuum, where quantitative and qualitative research methods are at each pole, and mixed methods designs are in the middle of them. Figure 4.1 illustrates this continuum of the research designs (Johnson et al., 2007). Tashakkori and Teddlie (2003) identified forty types of mixed methods research design in the literature. Implementation timing of research methods, the priority of methods and mixing procedures of methods emerged to be three common criteria of grouping these forms of mixed methods designs (Clark and Creswell, 2014). This doctoral research applied a sequential quantitatively driven mixed methods research design to address the research questions.

This thesis, which applies an objectivist victimological stance, aimed to discern the causes of economic cybercrime victimisation and its psychological and behavioural impacts on Internet users' online lifestyles. Quantitative data (CSEW 2014/2015) was utilised to examine the effect of Internet users' online behaviours on the risk of experiencing economic cybercrime victimisation. The breadth of online activities measured in CSEW 2014/2015 and the quantitative analysis results informed the data collection and data analysis of the qualitative phase of the research. Qualitative data utilised in a number of ways such as addressing the weaknesses of CSEW 2014/2015 dataset, expanding and explaining quantitative analysis result. This sequential analytic approach initially informed the formation of interview guide.

The questions included in semi-structured interview guide constructed in a way to both triangulate the quantitative findings and explore the issues that were not measured in quantitative dataset. For instance, interview questions aimed to measure and understand the impact of Internet users' engagement with online deviancy on the risk of victimisation or whether mobile application usage had an impact on the likelihood of experiencing economic cybercrime victimisation. These types of questions aimed to find out the causal relationship between Internet users' online activities and the risk of becoming a victim were less open-ended. The content analysis method was utilised to examine the patterns.

However, some more open-ended questions aiming to understand participants views' and perceptions related to their victim identity and emotional and behavioural reactions to the economic loss experienced were also included in the interview guide. For example, interview questions *"Some people who experienced economic cybercrime may not define themselves as a victim. How do you feel about that?"* or *"Did your victimisation experience have any effect on you apart from losing money?"* aimed to explore victims' perceptions of victim identity and harm received other than financial loss. A discourse analytic approach might have provided valuable insights into our understanding of cyber victim identity through examining the construction of victim identity in social and cultural context (Dunn, 2008; Keller, 2012). Anderson et al. (2001) successfully integrated content analysis and discourse analysis methods while researching rape victims' perceptions regarding victim-blaming. Yet, a discourse analytic approach could not be applied in this doctoral research due to lack of information-rich answers to the interview questions exploring participants' perceptions of victim identity. This could be viewed as the natural outcome of the research process informed by objectivist victimological stance, and the research objectives focused on discerning the causal relationships between Internet users' online lifestyles and the risk of facing economic cybercrime victimisation. Future studies informed by more objectivist victimological research

aims may explore the formation of cybercrime victim identity through the application of discourse analysis method. Figure 4.2 illustrates the phases of this doctoral research.

Figure 4.1
*Mixed Methods Quantuum*

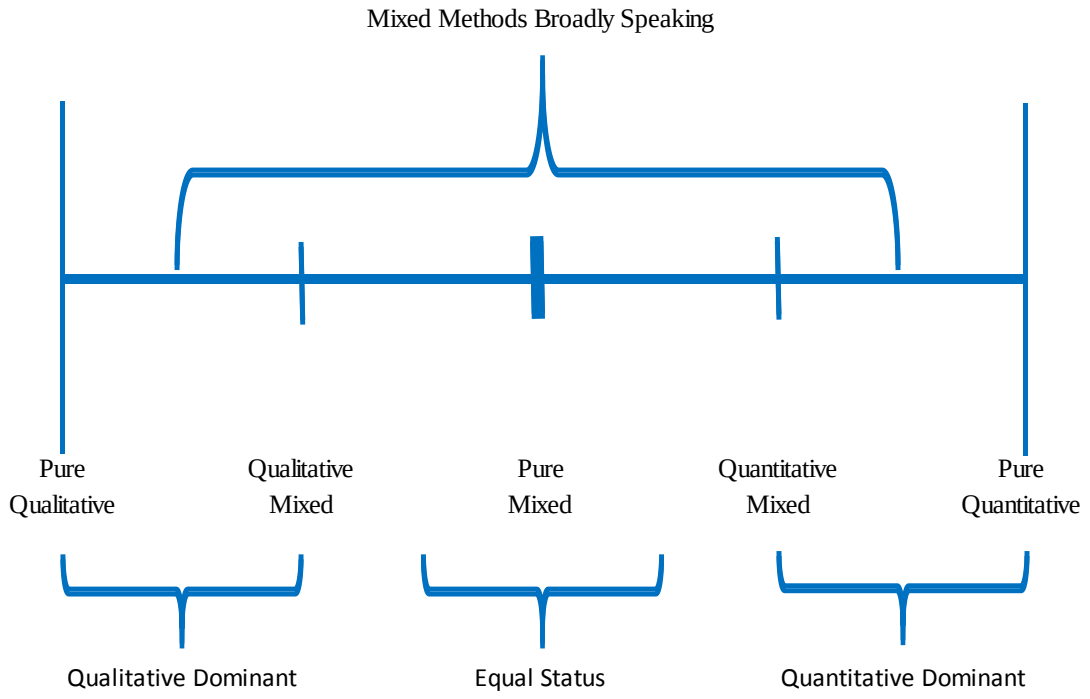
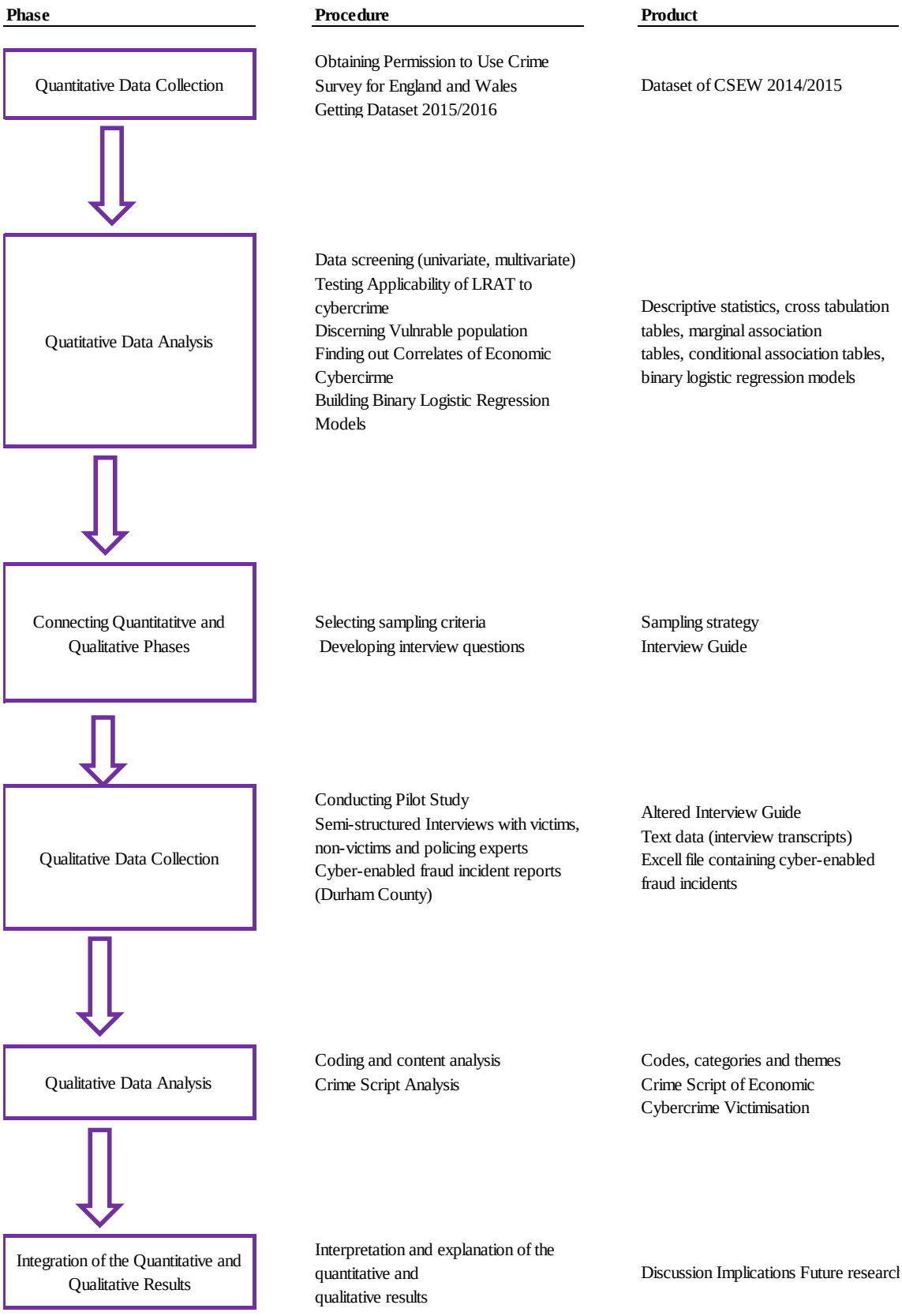



Figure adapted from Johnson et al., (2007).

Figure 4.2
*Visual Model of Research Design*




Adapted from Ivankova et al. (2006) and Creswell and Plano (2007)

## 4.4 Design of Quantitative Phase of Research

This research applied a secondary data analysis method, which is *"an empirical exercise carried out on data that has already been gathered or compiled in some way",* (Dale et al., 1988, p. p.3) as a quantitative phase of mixed methods research design. The dataset of CSEW 2014/2015 was used to test the applicability of LRAT to cybercrime as well as to discern online lifestyle correlates of economic cybercrime victimisation. The Crime Survey England and Wales, formerly known as the British Crime Survey, is a self-reported crime survey and it has been conducted since 1981 (Office for National Statistics, 2015). It has been conducted annually since 2001 (Jansson, 2007). Firstly, the underpinning rationale of using a secondary dataset will be discussed, and then challenges and rewards of using the dataset of CSEW 2014/2015 will be evaluated.

Accessing high-quality, accurate data may be the most important aspect of secondary data usage (Goodwin, 2012). The design and data collection of the primary data requires both expertise and effort (Patzer, 1995; Stommel and Wills, 2004). Secondary data such as Crime Survey for England and Wales enables research to reach the highest quality of data, which is beyond the ability and capability of a single person to collect (Cantor and Lynch, 2000; Smith, 2008). In addition, the application of sequential mixed methods research design may be time-consuming since it requires the collection of both quantitative and qualitative data (Driscoll et al., 2007; Mark, 2015). Using secondary datasets can alleviate this drawback of mixed methods design (Johnson and Turner, 2003; Caruth, 2013). Not only data collection is time-consuming but also variable coding is a lengthy process (Vartanian, 2010). The opportunity of downloading Crime Survey for England and Wales in a various format including SPPS helps to reduce the time spent on data preparation and coding processes.

Lack of key variables may be considered as the most significant shortcoming of secondary data usage (Bryman, 2008). Large scale crime surveys are usually conducted by governmental agencies or private companies for the purpose of understanding the current state of crime and its implications for policymakers. Although such surveys are very comprehensive, they may still lack some variables that address the research question. Complimentary use of a qualitative research method can up this pitfall of using secondary data (Ivankova, 2014; Biddix, 2018). The aspects that could not be addressed through secondary data may be explored via qualitative data. After assessing the significance of secondary data usage, the challenges and rewards of using CSEW 2014/2105 will now be evaluated.

The issue of accessing reliable secondary data about cybercrime is a well-established college to cybercrime studies (Shenton, 2004; Yuan et al., 2014; Levi, 2016, 2017; Levi et al., 2017). Crime Survey for England and Wales is considered to be one of the valuable sources for criminologists since it seeks information related to various types of crimes (Ghosh and Swaminatha, 2001; Crow and Semmens, 2008; Connelly, 2016).

Notwithstanding, a number of challenges and rewards were encountered due to CSEW 2014/2015 usage. Ill-presentation of cyber involvement in financial loss and fraud (Module 13) was the biggest challenge faced. For instance, respondents owing a credit card were asked if they experienced loss of money due to misuse of credit card and bank account information. However, it was hard to identify the cases bearing cyber element at one point (Yuan et al., 2014). It was not clear whether the victimisation was the outcome of a cold call or accessing a fraudulent website. To overcome this challenge some variables were re-coded or merged through SPSS syntax editor. The details of this process will be explained in the following section.

The ambiguity caused by the wording of the questions was another challenge encountered (Patzer, 1995; Tashakkori and Teddlie, 2008; Connelly, 2016). The wording of the questions related to online security measures failed to capture the chronology of the occurrence of victimisation experience and application of security software, which hampered the assessment of the effectiveness guardianship measures in preventing economic cybercrime victimisation. The cross-sectional nature of the dataset was a challenge to identifying the relationship between Internet users' online actions and repeat economic cybercrime victimisation. Longitudinal survey design may be helpful in tracing back the respondents' online lifestyles.

Representativeness of CSEW is another issue. The CSEW 2014/2015 interviewed 35,000 adults aged over 16 (Office for National Statistics, 2016b). A minimum of 650 respondents was chosen from each Police Force Area (PFA). This large sample size is an advantage of CSEW. Nonetheless, CSEW applies the multistage cluster sampling procedure to recruit participants. This procedure uses the postcode address file (PAF) of people residing in England and Wales (Maxfield and Babbie, 2015). Being a survey of households, CSEW excludes those living in many different types of institutions, hostels, homeless, residential homes, apartments (Bergman, 2008; Scurlock-Evans and Mahoney, 2016). This sampling strategy impedes capturing the real extent of economic cybercrime victimisation in the UK. Interviews with elderly participants aged over 60, disclosed that those living in shelter houses were more vulnerable to economic cybercrime victimisation due to unavailability of help from younger ones. Similarly, student participants emerged to be more likely to engage with risky online activities like peer-to-peer sharing, which in turn increased the risk of loss of money through virus infection.

Despite the above-mentioned challenges of utilising dataset of CSEW 2014/2105, some rewards were also received. An impartial picture of economic cybercrime and increased validity and reliability are the benefits of using CSEW 2014/2105 dataset. CSEW provides an unbiased picture of economic cybercrime victimisation when compared to other private security survey providers (Guba, 1981; Mellon, 1990) . Due to the concerns over experiencing adverse financial and reputational effects when the facts made public, private companies may be reluctant to provide real figures or fail to present the whole nature of economic cybercrime (Patzer, 1995; Malterud, 2001; Teddlie and Tashakkori, 2010). In addition, a high response rate is considered to be one of the main requirements of validity and reliability of interpretations based on the survey dataset (Whittemore et al., 2001; Denzin and Lincoln, 2017). Though slightly lower than usual CSEW response rates ranging from 72% to 75%, CSEW 2014/2015 had a relatively high response rate with 70% , when compared to the average response rate of 52% for surveys (Finlay, 1998; Walsh, 2003; Raven, 2006; Hammersley and Atkinson, 2007).

### 4.4.1 Sample Size

Though the CSEW 2014/2015 had a sample size of 35,000 composed of adults aged over 16 (Office for National Statistics, 2016b), dataset filtered to have more robust data. Since the survey has a follow-up structure, all questions were not asked of all respondents, which means that different modules have different sample sizes. In order to have a sample that responded Internet-related questions, the dataset was filtered according to the question asking whether participants accessed the Internet over that last twelve months. A data set of 5665 sample size was obtained after filtering procedure.

### 4.4.2 Operationalisation

The Crime Survey for England and Wales 2014/2015 measures financial loss through various questions. Both the Online Security Module (12th module) and the Financial Loss and Fraud Module (13th module) include financial victimisation questions. Whereas the Online Security Module includes the questions that measure pure online financial crimes, Financial Loss and Fraud Module contain the questions that measure hybrid financial crimes, which can be defined as financial crimes that can be the result of both online and offline causes (Flick, 1992; Wall, 2015). As discussed earlier, economic cybercrime is an umbrella term that covers many types of online financial crimes (Levi, 2016, 2017) . Outcome variables that were used in the analyses were created through recoding present variables. The following section will explain the procedure of obtaining outcome variables such as online banking fraud, card-not-present fraud and economic cybercrime. Firstly, the definition of terms is provided before explaining procedures applied to obtain outcome variables.

### 4.4.3 Definitions of Outcome Variables

**Online Banking Fraud:** Online banking fraud refers to the loss of money from online banking account through unauthorised access to online banking information.

**Loss of Money through Virus Infection:** Loss of money through virus infection denotes the way that offender(s) gained access to either bank card information or online banking account.

**Loss of Money through Phishing (Responding Communication):** Loss of money through virus infection again refers to the way offenders accessed either bank card information or online banking account.

**Online Identity Fraud:** Online identity fraud is the gain of money through compromised personal information such as bank card numbers or online banking account details.

**Card-not-present Fraud:** Card-not-present Fraud occurs when bank cards are used in the absence of a physical plastic card. It is also named as remote purchase fraud.

**Economic Cybercrime:** Economic cybercrime encompasses all forms of online financial crimes.

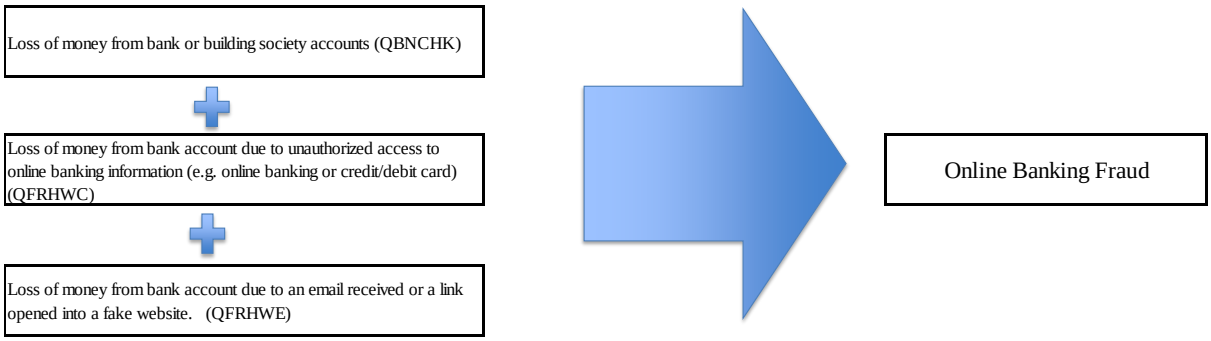
**Statistical Procedures to Obtain the Outcome Variable:**

As stated above, being a follow-up survey, all questions were not asked all respondents, which means that some variables had different missing values. This feature of the survey made using merge or combine variables impossible as utilising in-built commands required the same amount of cases to operate. Should in-built commands be used, the results would be erroneous. To prevent this issue new commands were written through SPSS syntax editor. The syntax coding procedure for obtaining online banking fraud will be explained below as an example. Other syntax codes used to create variables can be found in Appendix Seven.

**Online Banking Fraud (onln_bnk_frd):** Online banking fraud variable was obtained through a combination of three variables that measured different situations in which respondents faced online banking fraud (qbnchk, qfrhwc and qfrhwe). Whereas variable **Qbnchk** refers to the loss of money from a bank or building account while using the Internet, variable **qfrhwc** denotes loss of money due to unauthorised access to online banking information (hacking), and variable **qfrhwe** refers to the loss of money from a bank account due to opening an email link opened into the fake website (phishing). Figure 4.3 illustrates the process of obtaining an online banking fraud variable.

Figure 4.3

*The Statistical Procedure to Obtain Online Banking Variable*




As Table 4.1 illustrates variables had different missing values, which indicate that all questions were not asked, same participants. To overcome this issue firstly variables were recoded into different variables (recode_qfrwhc, recode_qfrhwe and recode_qbnchck). While value 0 referred to the non-victim category, value 1 denoted to victim category. Missing values were re-coded as a separate category and a value, 5, was assigned for this category.

Table 4.1
*Descriptive Statistics for Online Banking Victimisation*

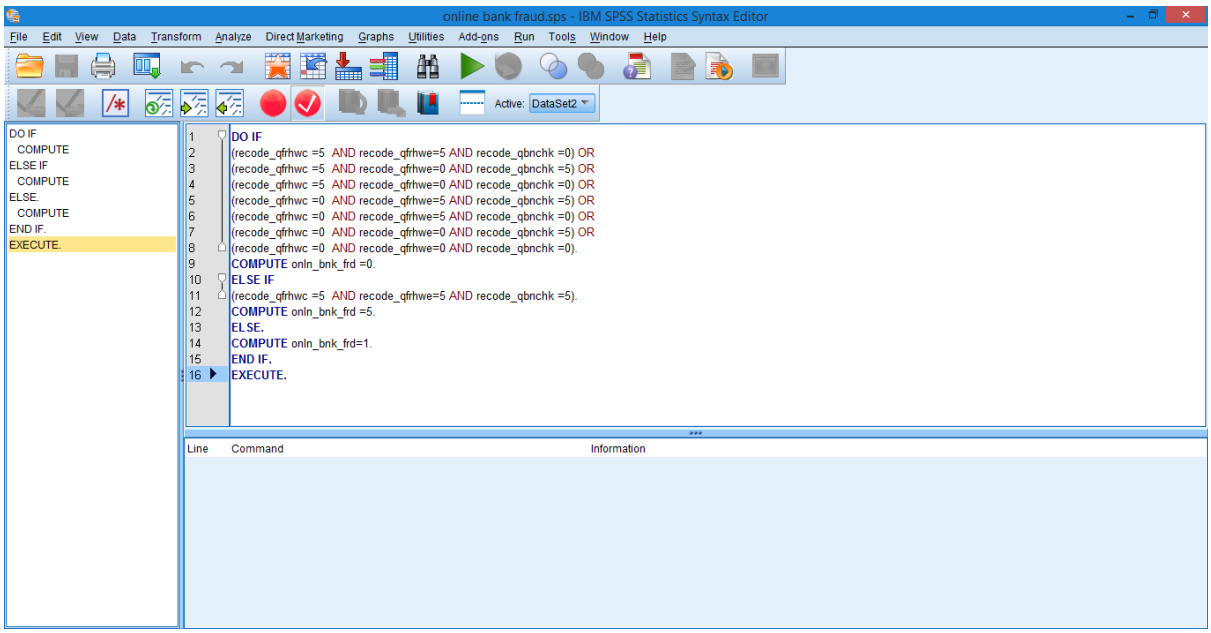
| Variables | Yes | No | Total | Missing |
|---|---|---|---|---|
| Loss of Money from bank or building society account while using the Internet | 42 | 26 | 68 | 21386 |
| Loss of Money from bank or building society account due to unaouthorised access to online banking information | 274 | 1010 | 1284 | 20170 |
| Loss of Money from bank or building society account due to an email received or a link opened in a fake website | 54 | 1230 | 1284 | 20170 |

After recoding variables, a syntax code was written to assign cases which denote victimisation, non-victimisation and missing (not being asked that question) to their new corresponding categories. Figure 4.4 illustrates the screenshot of the syntax editor. After the execution of the command variable denoting online banking fraud (onln_bnk_frd) was

obtained. Lastly, the missing value category was re-coded as missing. The same procedure was applied to obtain other variables.

Figure 4.4

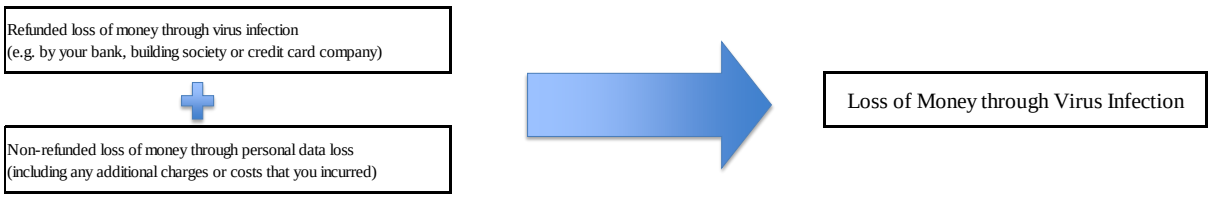
*Syntax Editor Screenshot*




**Loss of money through virus infection (lossevirimp):** This variable was obtained through a combination of two variables, (evirimpa and evirimpb), which measured whether respondents lost money due to virus infection. While variable **evirimpa** refers to the non-refunded loss of money through virus infection, variable **evirimb** denotes refunded loss of money through virus infection. Figure 4.5 illustrates this process of coding.

Figure 4.5

*Statistical Procedure to Obtain Loss of Money Through Virus Infection Variable*



**Online Identity Fraud (lossedatimp):** This variable was obtained through a combination of two variables, (edatimpa and edatimpb), which measured whether respondents lost money due to unauthorised access to personal information. Whereas variable **edatimpa** refers to the non-refunded loss of money through personal data loss, variable **edatimpb** refers to the refunded loss of money through personal data loss. Figure 4.6 demonstrates the process of obtaining this variable.

Figure 4.6

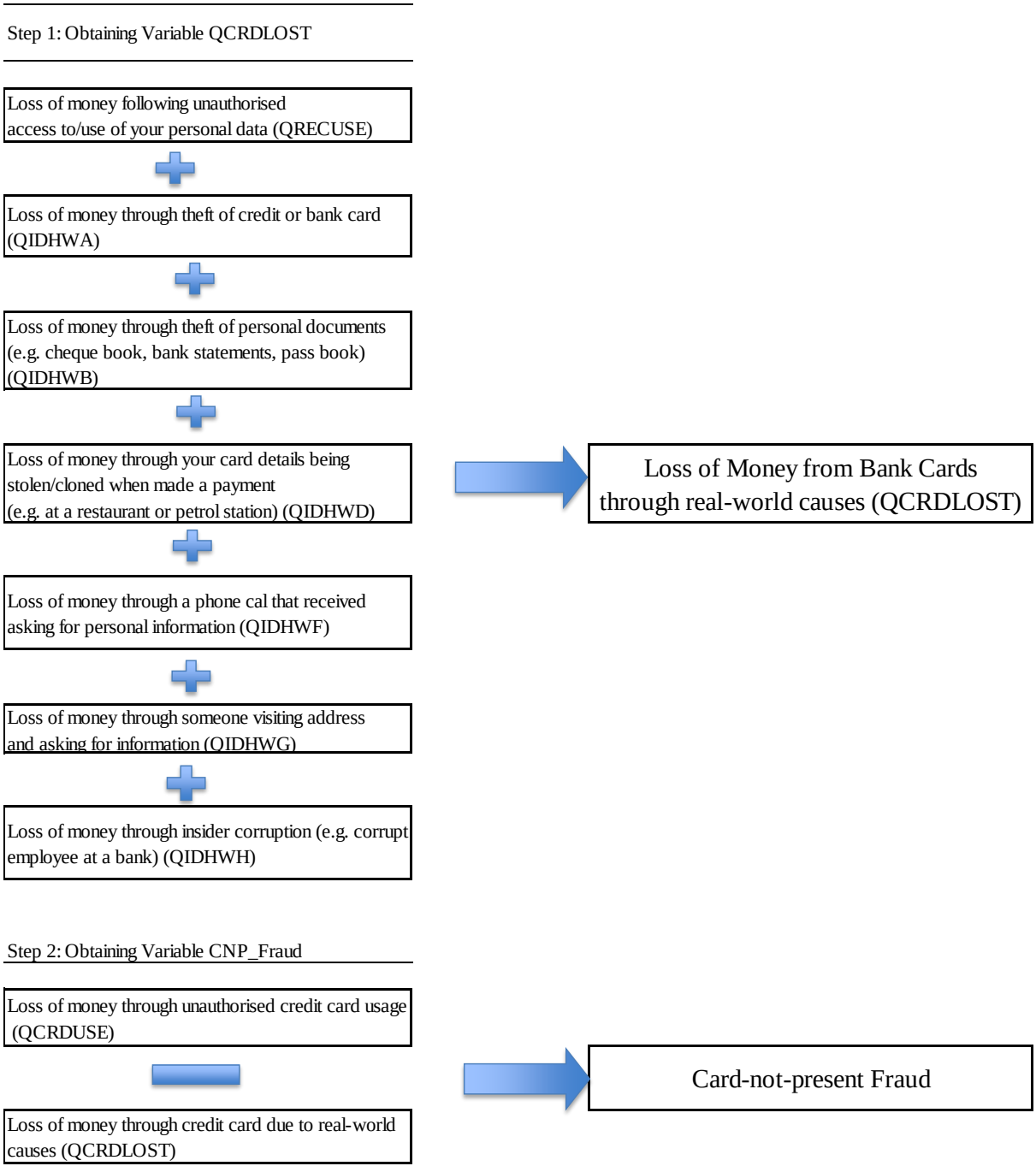
*Statistical Procedure to Obtain Online Identity Fraud Variable*


**Card-not-present Fraud (cnp_fraud):** CSEW 2014/2015 did not measure card-not-present fraud directly; however, this variable can be obtained through subtracting cases that represent financial loss due to real-world causes from credit card fraud cases. Firstly, variables measuring the loss of money due to real-world causes, namely qrecure, qidhwa, qidhwb, qidhwd, qidhwf, qidhwg and qidhwh, were combined. In that way, variable quidw was obtained. After that, cases of quidw were subtracted from the credit card fraud variable (qcrduse) to obtain card-not-present fraud cases (cnp_fraud). Figure 4.7 demonstrates the process of obtaining the card-not-present fraud variable.

**Economic Cybercrime (econ_cyber):** This variable was obtained through a combination of five forms of economic cybercrime, namely online banking fraud, loss of money through virus infection, loss of money through phishing (responding to communication), online identity fraud and card-not-present fraud.

Figure 4.7

*Statistical Procedure to Obtain the Card-not-present Fraud Variable*




### 4.4.4 Operationalisation of Response Variables

LRAT proposes that crime is the combination of three elements: motivated offender, suitable target and absence of capable guardian (Hindelang et al., 1978; Cohen and Felson,

1979). Since the motivated offender is a given fact, two elements, namely exposure and proximity to the motivated offender, were conceptualised as the function of a motivated offender. Independent variables were grouped according to this LRAT victimisation model. This section will explain the operationalisation of response variables used in the analyses.

**Exposure to the motivated offender:** In traditional crime studies, outdoor activities, especially night-time activities such as going to a bar (retail outlet selling alcohol), was hypothesised to increase risk of victimisation (Miethe et al., 1987; Mustaine and Tewksbury, 1998). Frequency of these activities was operationalised as a predictor of exposure to motivated offender (Mustaine and Tewksbury, 2000a; Tewksbury and Mustaine, 2001).

Cybercrime studies applied RAT and LRAT as theoretical perspectives hypothesised that individuals' online life-style facilitate victimisation by increasing Internet users' exposure to motivated offenders (Choi, 2008; Holt and Bossler, 2013; van Wilsem, 2013b). Online activities such as online shopping or time spent online was operationalised as the exposure element of theory. The results of past empirical research suggest that time spent online (Pratt et al., 2010; Reyns et al., 2011; van Wilsem, 2011, 2013b), online shopping (Pratt et al., 2010; van Wilsem, 2011, 2013b), using social networking sites (van Wilsem, 2013b), using online banking (Hutchings and Hayes, 2008; Reyns, 2013; Reyns et al., 2015; Williams, 2015), e-mailing or using chat rooms/instant messaging (Marcum et al., 2010; Marcum, 2011; Reyns, 2013; van Wilsem, 2013a, 2013b; Williams, 2015) was associated cyber victimisation.

This thesis argues that online activities such as using social networking sites or using email, chat rooms/instant messages should be operationalised as the proxy of proximity to a motivated offender element of the theory since Internet users are not necessarily required to disclose their personal information while accessing these online activities. Following this line of logic, online activities requiring personal information reveal were operationalised as the

exposure element of the theory. Online activities, using the Internet for online banking or managing finances and shopping online, were operationalised as a proxy of exposure to the motivated offender. Using online government websites was also operationalised as exposure element as Internet users provide both financial and non-financial identifying information to these websites. Frequency of Internet usage was another factor that hypothesised to increase the risk of victimisation. Table 4.2 displays operationalisation of exposure to the motivated offender in cyberspace.

Table 4.2
*Exposure to Motivated Offender*

| |
|---|
| Online banking or managing finances (e.g. paying credit cards) |
| Buying goods or services (internet shopping, inc. music / film downloads) |
| Online government services (e.g. tax returns, DVLA, council tax, benefits) |
| Frequency of Internet Usage |

**Proximity to Motivated Offender**: Neighbourhood characteristics such as living in an area mainly occupied by potential offenders were operationalised as proximity to motivated offender (Miethe and Meier, 1990; Rountree et al., 1994; Fisher et al., 2010). Reyns et al. (2011), who studied cyberstalking among college students, operationalised chat room usage as proximity to motivated offender since Internet users and potential online offenders converge at the same time and place. In this research, online activities such as using the Internet for social networking, email, instant messaging and chat rooms, browsing for news or information and playing online games was operationalised as proximity element of theory. Table 4.3 illustrates the operationalisation of the proximity element of the theory.

Table 4.3
*Proximity to Motivated Offender*

| |
|---|
| Social networking (e.g. Facebook, Twitter) or blogging |
| E-mail, instant messaging, chat rooms |
| Browsing for news or information (e.g. BBC, Wikipedia) |
| Playing online games/doing quizzes/competitions |

**Absences of Capable Guardianship:** LRAT postulates that a capable guardian may prevent the occurrence of victimisation (Cohen et al., 1981). Cybercrime literature divided guardianship measures into two categories (Ngo and Paternoster, 2011; Vakhitova et al., 2015). Whereas digital or physical guardianship denotes security measures provided by anti-virus programmes or firewall; personal guardianship refers to security measures applied by Internet users. This thesis categorised guardianship measures according to their aimed usage. For instance, while some security measures aim to protect the integrity of computers from online threats, other security measures aim to protect online accounts security. This categorisation of guardianship measures would enable us to examine the *'capability'* of guardianship measures in providing a certain type of guardianship. For instance, whereas digital guardianship measures can be useful to prevent virus infection, they may not be effective in protecting the financial information of Internet users. This sort of categorisation will enable us to make a more systematic analysis. Figure 4.8 and Table 4.4 demonstrate categorisation of guardianship measures.

Figure 4.8
*Online Guardianship Measures*

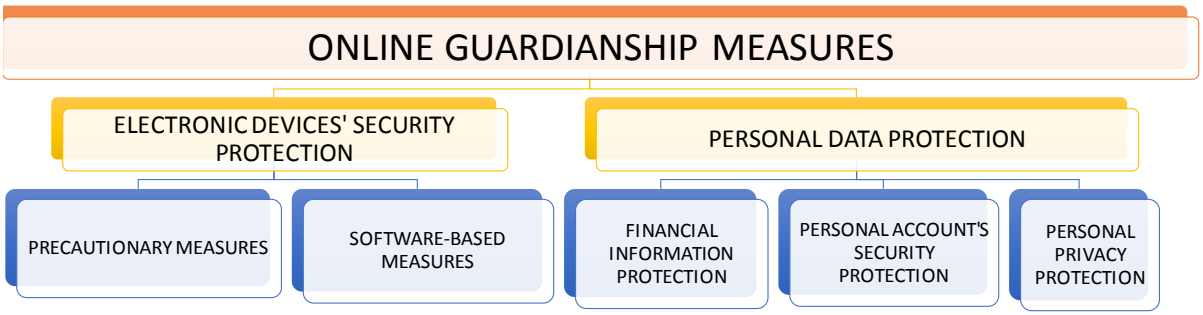



Table 4.4
*Online Guardianship*

| |
|---|
| *1. Guardianship Measures to Protect Electronic Devices' Security* |
| *1a. Precautionary Guardianship Measures to Protect Electronic Devices' Security* |
| Only downloaded known files or programs |
| Deleted suspicious emails without opening them |
| Protected your home wireless connection (wi-fi) with |
| a password or been cautious using |
| *1b. Software-based Guardianship Measures to Protect Electronic Devices' Security* |
| Downloaded software updates and patches whenever prompted |
| Installed anti-virus or other security software, such as a firewall |
| Scanned computer regularly for viruses or other malicious software |
| *2. Guardianship Measures to Protect Personal Data* |
| *2a. Guardianhip Measures to Protect Financial Information* |
| Only used well-known or trusted sites |
| Checked for signs that a site is secure when |
| buying online (closed padlock sign/https website |
| *2b. Guardianship Measures to Protect Personal Account's Security* |
| Used complex passwords (contain letters, numbers and symbols) |
| Used a different password for each different online account |
| Logged out of websites when you are finished |
| Adjusted website account settings (e.g. privacy settings) |
| *2c. Guardianship Measures to Protect Personal Privacy* |
| Only added known persons as friends on social networks. |
| Been careful about putting personal details on social networking sites |
| (e.g. date of birth,place of work) / not put personal details online |

**Control Variables:** Control variables can be defined as "extraneous variables that influence the outcome to represent potential confounds whose effects must be eliminated before causal assertions regarding the explanatory variable can be made."(Mehta, 2001, p. 2727). Previous research on cybercrime utilised demographic characteristics such as age and gender as control variables (Bossler and Holt, 2009; Leukfeldt, 2015; Choi et al., 2016; Leukfeldt and Yar, 2016). Though their studies yielded inconsistent results, they provided a good insight to assess the impact of age and gender on the risk of cyber victimisation.

Education level and income have also been used as control variables in cybercrime studies (van Wilsem, 2011; Leukfeldt, 2014; Policastro and Payne, 2014; Leukfeldt and Yar, 2016; Reyns et al., 2016; Wolfe et al., 2016). Leukfeldt and Yar (2016) found that education those with higher education and paid job run a higher risk of experiencing malware infection. Similarly, studies conducted by (Pratt et al., 2010; Paek and Nalla, 2015) found a positive relationship between education level and online identity theft victimisation. In addition, Reyns (2013) found that Internet users with higher income were more likely to be the target of online identity theft. Education level and annual household income were included in logistic regression analysis as a control variable. CSEW 2014/2015 used a 14 scale measure to divide the annual household income level of respondents, however; Savage et al. (2013) categorised British Population into seven groups, namely elite, established middle class, technical middle class, new affluent workers, traditional working class, emergent service workers and precariat, based on their annual household income. Their annual household income categorisation was used in this research to examine victimisation tendency between these categories. Table 4.5 displays control variables utilised in binary logistic regression analysis.

Table 4.5
*Demographic Characteristics*

| | |
|---|---|
| Age | |
| | 16-29 |
| | 30-59 |
| | 60+ |
| Gender | |
| | Male |
| | Female |
| Education | |
| | A levels or above |
| | Below A-level |
| | No qualifications |
| Income | |
| | Under £10,000 |
| | £10,000-£19,999 |
| | £20,000-£29,999 |
| | £30,000-£39,999 |
| | £40,000-£49,999 |
| | £50,000-£69,999 |
| | Over £70,000 |

### 4.4.5 Contextual Vulnerabilities Elements

**Type of the Device Used to Access the Internet:** To the best of our knowledge, up to now, no research has examined the role of devices used to access the Internet in becoming a victim of economic cybercrime. It is hypothesised that electronic devices such as mobile phones, tablets create vulnerabilities for their users as these devices usually bear security breaches (Symantec, 2016). Desktop computer and laptop used at home/work/college was conceptualised as low-risk devices as these devices are usually protected with anti-virus

programmes, there is limited access from strangers to these computers, and usually, secure Internet connections are used to access the Internet. Laptops used away from home/work/college, mobile phone and handheld computers were conceptualised as high-risk devices since Internet users who use laptops used away from home/work/college to access the Internet generally are more likely to use insecure Internet connections such as free public Wi-Fi. Mobile phone and handheld computers were also hypothesised to increase the risk of victimisation as they have some security issues such as mobile applications and accessing the Internet via insecure public Wi-Fi (Table 4.6).

Table 4.6
*Electronic Device Used to Access the Internet*

| |
|---|
| Low Risk Devices |
| Desktop computer (at home or work or school/college) |
| Laptop (at home or work or school/college) |
| High Risk Devices |
| Laptop (away from home and work or school/college) |
| Mobile phone or smartphone |
| Handheld computer (e.g. iPad, tablet, palmtop) |

## 4.5 Analytic Strategy of Quantitative Phase of the Research

Quantitative analyses were conducted to address two research questions: testing applicability of LRAT to economic cybercrime victimisation and discerning online lifestyle correlates of economic cybercrime victimisation. Statistical analyses ranging from univariate to multivariate analysis were performed to address this goal. This stepwise approach was implemented to conduct in-depth analyses while looking at various aspects of the phenomenon under examination and make more reliable inferences (Singh, 2007; Field, 2009).

Univariate analyses were performed to get basic information about variables to be used in more complex analysis. Whereas bivariate analyses were conducted to test the presence of relationship between online activities, online guardianship measures and experiencing economic cybercrime victimisation; multivariate analyses were conducted to test the applicability of LRAT to economic cybercrime victimisation through constructing binary logistic regression models and three-way contingency tables. To that end, three hypotheses were formed. The first two hypotheses, which assumes the presence of associations between Internet users' online lifestyles and facing cybercrime, were tested through bivariate analyses, the third hypothesis was tested through multivariate binary logistic regression analysis.

### 4.5.1 Univariate Analysis:

Univariate analysis, the method of describing the data with frequency distribution and graphs (Morris, 2006; Ruben and Babbie, 2009; Ho, 2013), was performed at the first phase of quantitative analysis with the aim of both introducing the variables utilised in bivariate and multivariate analyses and displaying frequency distribution of economic cybercrime victimisation in the UK. Percentages, as well as frequencies, were reported. Graphs related to these descriptive statistics were also provided. Univariate analysis through descriptive statistics is a convenient way of describing data; however, they are not very informative in terms of making inference (Tacq and Tacq, 1997; Denis, 2015). To overcome this limitation, bivariate and multivariate analysis were conducted in the second and third phase of quantitative analysis.

### 4.5.2 Bivariate Analysis:

Bivariate Analysis is a sort of statistical procedure where the association between two variables are examined without considering the effect of the third variable on the relationship (Weinstein, 2010; Gordon, 2012). Bivariate analysis is also a powerful tool in testing hypotheses (Walker and Maddan, 2008; Fitzgerald and Fitzgerald, 2013). Cross-tabulation or

contingency tables were utilised to both examine the association between variables and to test the applicability of LRAT to economic cybercrime. Some previous cybercrime studies (Hutchings and Hayes, 2008; Bossler and Holt, 2009; Pratt et al., 2010; Reyns, 2013) used Pearson's correlation test to examine the association between two categorical variables, however; while Pearson's correlation test is more suitable to test the relationship between two continuous variables, Pearson's Chi-square test is more suitable to test the relationship between two categorical variables (Blaikie, 2003; Field, 2009; Rosenthal and Rosenthal, 2011). Since all the variables used in this research were categorical variables, Pearson's Chi-square test and Phi test were used to examine the presence, strength and direction of the relationships between variables.

Pearson's Chi-square or chi-square goodness-of-fit-test is a test of independence conducted to evaluate whether the difference between observed and expected values is significant (Russo, 2004). This test was utilised to determine the presence of the association between online activities, guardianship measures and experiencing economic cybercrime victimisation. To that end, firstly, the Null hypotheses ($H_0$), which asserted the absence of association between variables and the alternative hypotheses ($H_a$) stating the presence of the correlation were formed. Secondly, contingency tables were formed, and the statistical tests (Chi-square and Phi) were performed through SPSS Quantitative Analysis software. A default significance level of 0.05 ($\alpha$=0.05) was set as the threshold for testing the hypothesis through chi-square test since this significance level is more suitable for testing hypotheses (Churchill and Doerge, 1994; Payton et al., 2003). Phi coefficient ($\theta$) was used to measure the strength of measurement in Chi-square based analysis (Dytham, 2011; Jackson, 2013). Whereas values from 0.00 to 0.10, referred to a weak association, values ranging from 0.11 to 0.30 denoted moderate association between binary variables and values greater than 0.30 referred to strong association (Healey, 2014). Based on these analyses inferences were made about the presence

of the relationship between online activities, online guardianship measures, demographic characteristics of the Internet users and experiencing economic cybercrime victimisation.

### 4.5.3 Multivariate Analysis:

Bivariate analysis is an efficient method to examine the relationship between two variables whereas multivariate analysis is a more sophisticated tool to explore the relationship between two or more variables while holding other variables constant (Weinstein, 2010; Gordon, 2012). In other words, multivariate analysis enables researchers to control the effects of other variables while examining the relationship between two phenomena (Agresti, 1996). After deciding to conduct multivariate analysis, the choice of the appropriate test became of utmost importance. As response variables in this analysis were dichotomous categorical variables, namely categorical variables with two categories, binary logistic regression and log-linear analysis were two possible statistical methods that could be used to research the applicability of LRAT to cybercrime.

The log-linear analysis is a variation of cross-tabulation analysis which may be considered as the generalisation of the Chi-square test (Spicer, 2005; Treiman, 2014). The log-linear analysis is more suitable to examine the relationship between categorical variables without making a distinction between outcome and response variables (Simkiss et al., 2015). Binary logistic regression is a sort of regression where the outcome variable is dichotomous, though, the response variables may have more than two categories (Osborne, 2014; Strickland, 2017).

This reserach applied binary logistic regression analysis method as this application promises some advantages over running log-linear analysis: Firstly, while log-linear modelling requires a two-step analysis process, logistic regression modelling yields results at one step (Engel and Keen, 1994). Secondly and more importantly, binary logistic regression analysis

yields more interpretable results since binary logistic regression analysis provide information about the magnitude and direction of the relationship between outcome and response variables. The log-linear analysis does not provide any information about the magnitude and nature of association (Tansey et al., 1996). In other words, binary logistic regression analysis yields result in that measure how one unit change in response variable causes changes in outcome variable (Verma, 2012). Since finding out the impact of online activities on the risk of experiencing cybercrime is one of the aims of this doctoral research, binary logistic regression analysis emerged as the most appropriate analysis method to address the research questions.

#### 4.5.3.1 Analytic Procedure:

Some assumptions should be checked prior to conducting binary logistic regression analysis (Agresti, 1996; Weinstein, 2010). The absence of multicollinearity denoting a high level of correlations between response variables (Pituch and Stevens, 2016) is the first assumption of binary logistic regression (Field, 2009). It is vital to check the presence of multicollinearity since in the case of multicollinearity; the response variables appear to have no significant impact on the outcome variable, which may be contrary to the real situation (Ho, 2013). Variance Inflation Factor (VIF) is one way of diagnosing the presence of multicollinearity between response variables (Gordon, 2012). VIF scores lower 10 can be considered as lack of multicollinearity (Field, 2009; Gordon, 2012; Ho, 2013). The presence of multicollinearity between response variables was checked through SPSS analysis software. VIF analysis results ranged from 1.001 to 1.281, which indicated that there was no multicollinearity between response variables.

After seeing that the data satisfied conditions for binary logistic regression analysis, the components of theory, exposure and proximity to the motivated offender, target suitability and absence of capable guardianship, were tested separately and then all components were put

together to test LRAT theory as a victimisation model. The relationship between the outcome and the response variables can be measured with Odds ratio. “The OR represents the odds that an outcome will occur given a particular exposure, compared to the odds of the outcome occurring in the absence of that exposure.” (Scotia, 2010, p. 227). Whereas Odds ratio values greater than 1 indicated an increased risk of victimisation, those less than 1 indicated a decreased risk of victimisation. Obtained Odds ratio (Exp (B)) values of test results were used to draw inferences about test results.

Examining the relationship between demographic characteristics of Internet users and the risk of experiencing economic cybercrime was another goal of this research since this analysis results would inform qualitative sampling strategy. Three-way contingency tables are considered to be suitable for the analysis where the researcher aims to observe the distribution of the relationship between two variables over the categories of a third variable (Malhotra and Birks, 2012). Another benefit of applying a three-way contingency analysis is the opportunity to eliminate the confounding effect of a third variable (Agresti, 1996). Thus, three-way contingency tables appeared to be an appropriate test to examine the risk of experiencing economic cybercrime through categories of age, gender, education level and annual household income. To that end, firstly marginal association tables were built for each demographic characteristic. Marginal association tables are 2*2 tables that display the relationship between two variables without considering the effect of third variable (Agresti, 1996). These tables were used as a reference to compare the results of three-way conditional association tables.

A test of homogeneous association must be conducted to check the presence of a three-way interaction between variables before conducting a three-way analysis since if there is a three-way association between three variables lower level (two-way) associations cannot be interpreted unambiguously (Azen and Walker, 2011). Breslow-Day test of homogeneous

association and Cochran's test were conducted to see whether the relationship between three variables can be examined with three-way conditional association tables. After conducting these two tests, Mantel-Haenszel tests were performed to interpret the degree of association between using the Internet for online financial activities, risk of experiencing economic cybercrime victimisation and different strata of demographic characteristics of Internet users.

This section of the chapter aimed to give an overview of the mixed methods approach, the rationale behind utilising this research paradigm, research design applied to address research questions and analytic procedures conducted to run statistical tests. The next section of the chapter will provide a reflexive account of the qualitative phase of the research.

## 4.6 Reflexive Account of the Qualitative Phase of Research

This section of the chapter will provide a reflexive account of the qualitative phase of this research. This reflexive account will be given from methodological and personal angles. Given that dissecting these two aspects of reflexivity is impractical (Finlay, 1998), a methodological reflexive account concerning assuring reliability and validity of this thesis as well as personal reflexivity is dealing with my personal experiences as a non-British male PhD student from a policing background will be interwoven.

It is widely accepted that a researcher's background together with his/her personality and epistemological stance influence the research process, initiating from formulating the research questions to interpreting the research findings (Malterud, 2001; Colbourne and Sque, 2004). Reflexivity emerges as a key instrument in distinguishing the impact of the researcher on each phase of the research. Finlay (2002, p. 532) argues that "reflexive analysis in research encompasses continual evaluation of subjective responses, intersubjective dynamics, and the research process itself." Though it appears to be unattainable to find out a commonly agreed definition of the term reflexivity (Lynch, 2005; Archer, 2007), it may be defined as a "process

of reflecting critically on the self as researcher" (Denzin and Lincoln, 2017, p. 246), the "human as instrument" (Guba, 1981, p. 75). Methodological (epistemological) and personal reflexivity are two variants of reflexivity to be dealt with at this part of the chapter.

Transparency, substantiated through a methodological reflexive account of the research process, is considered to be essential in ensuring reliability and validity of the research (Karnieli-Miller et al., 2009). Given that absolute objectivity is unattainable, an inevitable consequence of human nature (Mellon, 1990), it is best to document the rationale of the research and role of the researcher in the research process (Flick, 2008). In this sense, reflexivity is perceived as a methodological tool in quest of maintaining reliability and validity of the research (Finlay, 1998; Whittemore et al., 2001; Walsh, 2003; Raven, 2006).

Personal reflexivity, a way of disclosing the social self of the researcher impacted by factors like age, gender and ethnicity, is another aspect of being reflexive (Usher, 2002). "Personal reflexivity involves reflecting upon the ways in which our own values, experiences, interests, beliefs, political commitments, wider aims in life and social identities have shaped the research." (Willig, 2013, p. 10). Recognizing and attempting to minimise the power balance between the researcher and informants in criminological research is another value of being reflexive throughout the research process (Grant, 2014; Lumsden and Winter, 2014).

### 4.6.1 Reliability and Validity

Though originated from the positivist epistemology, the concepts of reliability and validity received considerable attention from both qualitative and mixed methods paradigms (Patton, 1990; Strauss and Corbin, 1990). Needless to say, due to inherent epistemological stances of quantitative, qualitative and mixed methods research paradigms, these two concepts correspond to different meanings and applications in each paradigm (Kirk et al., 1986; Baumgarten, 2010). From a positivist research perspective, while the terms reliability refers to

the extent to which a measurement yields consistent and replicable outcomes; validity denotes the notion of correspondence between the measure and the indicator, a term which underscores the capability and success of indicator in obtaining the intended measurement (Carmines and Zeller, 1979; Curtis et al., 2013; LoBiondo-Wood and Haber, 2014).

Qualitative research paradigm, where subjectivity and intrinsic researcher bias prevail, perceives validity as a tool for gaining insights into informants' experiences, reflections and understanding (Maxwell, 1992). The researcher with his all inescapable influence on the research process is the measure per se (Patton, 2002). Designing and implementing appropriate research schemes (Brewer and Crano, 2000; Creswell and Miller, 2000; Golafshani, 2003), developing strategies to prevent researcher bias (Maxwell, 2012) and reactivity (Hammersley and Atkinson, 1995) are proposed to be the ways to secure validity in qualitative research. The concept of reliability is generally perceived as inapplicable to qualitative research paradigm (Stenbacka, 2001) since replicability is not an easy task due to subjectivity and unique nature of qualitative studies (Beck, 1993; Merriam, 1998). Lincoln and Guba (1985) suggest the concept of trustworthiness as the reminiscent of reliability and validity for the qualitative research paradigm. Truth value, applicability, consistency and neutrality are the proposed criteria to ensure trustworthiness in a qualitative study (Guba, 1981). These criteria are proposed as "naturalistic counterparts" of reliability and validity (Guba, 1981, p. 76). Later, Lincoln and Guba (1985) replaced these terms with their new corresponding concepts: credibility, transferability, dependability and confirmability respectively. Credibility and transferability are at the heart of this proposed model of trustworthiness (Shenton, 2004; Connelly, 2016). The former refers to internal validity, and the latter denotes external validity. Whereas dependability replaces reliability, confirmability is the analogy of objectivity (Lincoln and Guba, 1985).

With regards to the mixed methods research paradigm, which is proposed to overcome the weaknesses and promote strengths of the two former research paradigms (Teddlie and Tashakkori, 2006), suggests *inference quality* as the counterparts of reliability and validity (Abbas and Charles, 2003). This approach, an integrative framework, seeking reconciliation between views over reliability and validity between two leading research paradigms contends that design quality and interpretive rigour are the paramount concepts in ensuring rigour in mixed methods research (Tashakkori and Teddlie, 2003, 2008). Design quality refers to selection and application of the appropriate research design that is capable of addressing the research questions and goals, whereas interpretive rigour is about the assessment of accuracy and consistency of the interpretation originated from the data (Teddlie and Tashakkori, 2010; Levi et al., 2017). I implemented the steps suggested by Ritchie et al. (2013, p. 286) to conduct rigorous research aiming to understand economic cybercrime victimisation.

As this thesis applied a sequential explanatory mixed methods research design, I initiated the research process by conducting a quantitative analysis of CSEW 2014/2105. Upon writing the first draft of qualitative results, I devised a sampling design informed by quantitative analysis results to prevent researcher bias (Collins et al., 2006). Criteria of participants' demographics were set to obtain "symbolically representative" of the British population. After recruiting participants and getting ethics approval, I conducted semi-structured interviews in a way to allow respondents to express their victimisation experiences without researcher manipulation (Dörnyei, 2007). Iterative data analysis is generally accepted as an essential method to prevent researcher bias (Creswell et al., 2003). To that end, I implemented a systematic and iterative process of content analysis to obtain robust inference from the data. In addition, interpretations were supported with evidence from both quantitative analysis results and direct citations from interviews.

### 4.6.2 Sampling

Robinson (2014)'s four-point approach was adopted to conduct sampling for the semi-structured interviews. Defining the sample universe, deciding a sample size, selecting a sampling strategy and sample sourcing are the steps of this approach.

#### 4.6.2.1 Defining the Sample Universe

Delineation of a sample universe is the first step of sampling (Robinson, 2014). An extensive review of the literature illustrated that most of the previous cybercrime studies (i.e. Choi, 2008; Holtfreter et al., 2008; Bossler and Holt, 2009; Marcum et al., 2010; Choi, 2011; Ngo and Paternoster, 2011; Reyns et al., 2011; Henson et al., 2013; Holt and Bossler, 2013; Reyns et al., 2015) set college students as a sample universe. Although such sampling strategy may be beneficial in accessing information-rich cases as most of the respondents were knowledgeable about online threats, it may fail to illustrate all facets of the problem due to under-representativeness of the target population. For instance, both the aforementioned studies and CSEW 2014/2015 did not research the cyber victimisation among the elderly population (those over sixty years) living in sheltered houses. This elderly population may have certain properties such as being lonely or lack of computer knowledge, which separate them from the other demographic groups. To address these sampling issues of the previous cybercrime studies, this research set adult UK population who have access to the Internet as sampling universe. Precise sampling criteria defining the characteristics of the target population and eligibility of participation in this research were also defined (Nash and Scott, 2008; Salmons, 2017).

#### 4.6.2.2 Sample Size

The sample size is considered to be one of the essential issues to be contemplated to obtain desired research outcomes (Marshall et al., 2013; Ryan, 2013). Although quantitative studies heavily rely on large number sample sizes due to some statistical concerns and the desire of generalizability; qualitative studies, where in-depth understanding of the research phenomenon is more stressed, apply relatively small sample sizes (Onwuegbuzie and Daniel, 2003; Rosenthal and Rosenthal, 2011; Emmel, 2013). It is evident that qualitative researchers do not attach too much importance to sample size (Onwuegbuzie and Leech, 2007), nonetheless, the sample size is still an important concern for the validity of research findings as well as gaining an in-depth understanding of the research topic (Thomson, 2010). While small sample size bears the risk of inadequate resource to gain insight, needless large sample size put the risk of repetition in data (Padgett, 2016). Data saturation proposed by grounded theory may provide a solution to these sample size consideration (Bowen, 2008). Adding new participants to research to the point where repetitiveness emerges in data is at heart of this data saturation method (Sandelowski, 1995; Dworkin, 2012). However, determining the saturation point is not an easy task for novice researchers given the ambiguity of sample size guidelines (Marshall et al., 2013). Following sampling size recommendation of the scholars is another way of determining sample size. Literature suggests that a sample size ranging from twenty to thirty is enough for an interview-based study (Morse, 2000; Creswell and Plano Clark, 2007). A study researching the sample size of the PhD studies is adopting a qualitative approach has found that the mean sample size of the PhD studies was thirty-one (Mason, 2010).

In addition, considering value of tracking trajectory of participants' lives for criminological studies (Farrington, 1991, 2006), conducting a longitudinal research would enable us to follow online lifestyles and security behaviours of the participants, which could

provide more information about the impact of online lifestyle on the risk of experiencing economic cybercrime victimisation . However, conducting a longitudinal research was beyond the capability of this thesis taking the lack of resources and time into account. Utilising a control group would make up this drawback and provide an opportunity to compare online behaviours of victims and non-victims. (David and Sutton, 2011; Lewis, 2013). Based on these considerations sample size around thirty seemed appropriate for this doctoral research.

#### 4.6.2.3 Devising a Sampling Strategy

It is argued that the choice of sampling strategy is mainly driven by the purpose and the rationale of the research (Patton, 1990) as well as the desired extent of generalisability of the findings (Rees, 2011; Sekaran and Bougie, 2016). The sampling strategy is generally viewed as one of the focal distinctions between quantitative and qualitatively informed studies (Devers and Frankel, 2000). While quantitative sampling is generally driven by probability sampling, qualitative sampling heavily relies on non-probability or purposeful schemes (Carvalho and White, 1997; Bamberger, 2000; Gerrish and Lacey, 2010; O'Dwyer and Bernauer, 2013). Accessing information-rich cases is of paramount importance for a purposeful qualitative inquiry (Teddlie and Yu, 2007) as "studying information-rich cases yields insights and in-depth understanding rather than empirical generalizations." (Patton, 2002, p. 230).

Neergaard and Ulhøi (2007) identifies twenty variations of qualitative sampling strategies adopted by qualified researchers. I applied complimentary use of purposive sampling maximum variation, quota and snowball sampling methods. This informed decision was made "to achieve comparability across different types of cases on a dimension of interest." (Teddlie and Yu, 2007, p. 80).

Maximum variation sampling aiming to capture variations in perspectives through recruiting participants having various backgrounds (Pitney and Parker, 2009; Mujere, 2016) is

considered to be an effective sampling method for the interview based studies (Seidman, 2013b). Economic cybercrime encompasses various types of online financial crimes such as loss of money through phishing or hacking (Seda, 2014). To examine the nature of various sorts of economic cybercrime, no specific type of economic cybercrime victimisation was set as sampling criteria. Losing money from bank cards, online banking accounts and e-wallets such as PayPal as a consequence of online activities within last two years and having access to the Internet were set as sampling criteria for the victim participants group. The sampling criteria for the control group were using the Internet for financial purposes like online shopping and not having a financial loss due to Internet usage. While the sampling criterion for experts was working in IT departments of governmental organisation, it was serving in the cybercrime unit for police officers.

The rationale of choosing quota sampling is to examine the impact of the contextual conditions such as having an active online lifestyle, computer literacy or being alone in sheltered house impacts the risk of victimisation. To that end, age and gender were set as inclusion criteria for both victim and non-victim participant groups since implementing attributes that the researcher wants to examine as inclusion criteria is a way of quota sampling application (Polgar and Thomas, 2011; Schneider and Whitehead, 2013). Triangulating the results displayed in Chapter Five and those of previous cybercrime studies (i.e. Bossler and Holt, 2009; Leukfeldt, 2015; Choi et al., 2016; Leukfeldt and Yar, 2016) suggesting age and gender differences in the risk of experiencing cyber victimisation was another goal of this informed choice. Equal age and gender balance were established to explore age and gender differences in economic cybercrime victimisation. Table 4.7 displays the inclusion criteria of sampling for this thesis.

#### 4.6.2.4 Sample Sourcing

**Recruitment Strategy and Gaining Access to Participants**

Convenience sampling was adopted to recruit participants. Convenience sampling considered to be most common qualitative method (Schneider and Whitehead, 2013) since it provides an opportunity to access individuals who are available or easy to recruit (Kothari, 2004; Bachman and Schutt, 2016). Though this method saves time and effort in recruiting participants, a possibility of lacking external validity that ensures generalisability of the findings to the target population is the greatest challenge of this application (Blankenship, 2010; Maxwell, 2012). Missing the voice and perspective of individuals' living in different locations appears to be the main source of the external validity concern (Wells, 1999; Olsen et al., 2013). The borderless nature of the Internet enabled me to overcome this drawback. With the unprecedented proliferation of the availability of the Internet, most of the individuals have access to the Internet regardless of their geographical locations. This means "a shift from physical to discursive boundaries" (Given, 2008, p. 456). Taking this borderless nature of cybercrime into account, I recruited participants regardless of their geographical locations. I recruited most of my participants mainly from the North-East of the UK due to the ease of accessing participants.

Table 4.7
*Sampling Criteria*

| |
|---|
| **First Group (Victims of Economic Cybercrime)** |
| Age |
| Under 30 years |
| Between 30 and 60 years |
| Over 60 years |
| Gender |
| Male |
| Female |
| Being a Victim of Economic Cybercrime within last 24 months |
| Accessing the Internet |
| **Control Group** |
| Age |
| Under 30 years |
| Between 30 and 60 years |
| Over 60 years |
| Gender |
| Male |
| Female |
| Accessing the Internet |
| No Economic Cybercrime Victimisation Experience within last 24 months |
| **Experts Group** |
| Police Officers |
| Governmental Web Experts |
| Private Sector |

Representativeness of the general population in convenience sampling is another issue that raises the question of the external validity (Williams et al., 2018). As mentioned in the previous sections of this chapter, most cybercrime studies used college students as a sample universe due to the ease of access. This research addressed this challenge of representativeness of the adult UK population through setting age and gender as inclusion criteria, which aimed to achieve a balanced distribution with regards to age and gender of the participants. Disseminating fliers, advertising on social media, community outreach and snowball sampling were the strategies adopted.

Utilising fliers as a mean of recruiting participants is a popular way of advertising the research, though their effectiveness in recruitment is open to question (Close et al., 2013; Rait et al., 2015). After preparing fliers that advertise my research (Appendix Six), permission was sought from the local branches of companies such as Tesco, Homebase, Wilko, Sainsbury and Lidl to refer my research to their employers and display the fliers of the research in their facilities allocated to their staff (Appendix Three). Fliers were also handed out to passers-by on the street. Though some people got interested in the research, I faced difficulties in recruiting participants as there was a reluctance to share personal information and victimisation experiences with a stranger. This kind of recruitment difficulty is more prevalent in health care (i.e. Chandra and Paul III, 2003; Badger and Werrett, 2005; Howard et al., 2009; Donovan et al., 2016) and criminology studies (Liamputtong, 2007; Logan et al., 2008; Buchanan et al., 2009), where lack of trust and misconceptions about the research prevails. In addition, being an international student, my accent alarmed some people about the risk of facing a fraud attempt. Some of the people that I approached open heartedly asked whether my research was a fraud attempt itself. However, this kind of challenge is not unique to my research. For instance, O'Leary (2014) researching victim communities at two different locations in the UK after two notorious high profile crime, had faced similar challenges while trying to gain access

to these communities. He acknowledges suspicion about being a media member and lack of trust as two barriers that impeded successful access to informants for his research.

Posting messages on social media was another recruitment method that I implemented. The ability to reach a large number of potential participants and cost-effectiveness make research advertisement through social media a preferred recruitment method (Fenner et al., 2012; Ramo and Prochaska, 2012). A study conducted by Johnson et al. (2014) suggested the use of social media in recruiting hard-to-reach population with rare diseases as a fruitful tool. Though, Yuan et al. (2014) researching effectiveness of social media in recruiting participants with human immunodeficiency virus-positive found weak a relationship between social media posts and survey clicks. I posted advertisements on social media platforms such as Facebook, Twitter and Callfofparticipants.com to make the research public; however, this method also failed to raise a significant volume of interest for the research.

Though I knew that getting access to participants would be a demanding job, this failure was an upsetting experience for me. Relating this failure to my ethnic background and lack of communication skills were the main sources of the distress. Having fifteen-year law enforcement experience, I always considered myself as an able communicator. After this experience, I realised that it was power imbalance inherent to the relationship between law enforcement officers and the public that facilitated communication on behalf of me (Togher et al., 1997; Biradavolu et al., 2009). Yet, this time the power balance was in favour of individuals whom I approached to recruit. This meant that I needed to develop skills for establishing rapport in various social contexts, where different power balances present.

I also considered engaging with a recruitment company as a solution to this challenge. However, I gave up this idea very quickly as it was accepting defeat. I thought I would not be a real researcher without overcoming the barrier of establishing rapport with the target

population. At this point in the research, besides getting advice from my supervisors about confronting recruitment challenges, I referred back to the qualitative research literature to identify potential barriers that hinder a successful recruitment process. To my surprise, I came across a lot of papers discussing researcher distress. Lack of explanation about the benefits of the research for the community (Myles et al., 2018), distrust to foreigners arose from fear of crime provoking scam attempts or previous victimisation experience (Reynolds, 2003; Ravenscroft, 2004; Stafford et al., 2007) and research fatigue caused by unprecedented volume of research seeking participants (Galea and Tracy, 2007; Clark, 2008) emerged to be potential barriers to recruitment. Community outreach (White and Verduyn, 2006; Metcalfe and Sexton, 2014; Tun et al., 2015) and snowball sampling (Penrod et al., 2003; Sadler et al., 2010) emerged to be the most suitable recruitment strategies.

At this point in the research, I tried to recruit participants through personal referrals of friends as well as members of the Age UK, members of Durham County International Women Group. I attended several Age UK's "Beat the Scam" meetings held in various locations of Northeast. After the presentation of Age UK's representative, I had the opportunity to explain the goals of the research and its potential benefits for the community. Interview procedure was also briefly explained to overcome the curiosity pertaining to data collection procedures. Care was taken to avoid giving too much information about the research. Wengraf (2001) dubs this kind of challenge as slang information, which may cause bias or diversion in respondents' future accounts. Some of these meetings took place at sheltered houses. This provided an opportunity to access individuals with various backgrounds while exploring the impact of age and loneliness on the risk of experiencing victimisation. Most of the victim participants aged over sixty years were recruited through these meetings. I also attended some events organised by the Durham County International Women Group. I recruited some of my female victim participants through this channel. Establishing rapport with International women group

members boosted the visibility of my research as they shared my fliers within their social networks and made referrals for snowball sampling.

Before beginning recruitment procedure, I envisaged that recruiting male participants would be easier than recruiting female participants as approaching to same sex would be easier in social circumstances. However, to my surprise, it was females who more readily accepted participation. This gender difference in willingness to participate cybercrime research may be explained with females' curiosity about discovering the factors facilitated their victimisation since my interviews would be an opportunity to contemplate about the occurrence of the victimisation. Anxiety over disclosing online lifestyle may be a facilitator of male unwillingness to participate research as the literature suggests that males are more inclined to engage with deviant online lifestyle (Li, 2006; Sengupta and Chaudhuri, 2011; O'Dea and Campbell, 2012). This hinted underscoring privacy and confidentiality issues while describing the study to the target population.

Snowball sampling is found to be an effective sampling strategy for the studies dealing with sensitive issues (Biernacki and Waldorf, 1981; Milne et al., 2004; Reyns, 2013). Economic cybercrime victimisation experience might be considered as a sensitive topic to an extent since victims mostly blame themselves and feel ashamed for losing money due to their own mistakes (Levi and Pithouse, 1992; Mason and Benson, 1996). Accessing economic cybercrime victims aged over sixty was a challenge as a flier distribution strategy indicated that it was difficult to establish rapport with older individuals. Thus, I decided to apply snowball sampling since the ease of recruiting hard-to-reach participants with similar eligibility criteria is one of the advantages of snowball sampling (Sadler et al., 2010; Goodman, 2011).

After getting in touch with some elderly participants, I asked them if it was possible to refer my research to their friends with similar experiences. As Internet usage, especially for

financial purpose, among individuals over sixty years was rare when compared to younger generations (Rege, 2009; Pratt et al., 2010), spotting older people without application of snowball sampling strategy would be very daunting and a time-consuming process. Another value of snowball sampling for recruiting hard-to-reach population is establishing a trust link between the participants and the researchers (Shaghaghi et al., 2011; Dusek et al., 2015). Distrust stemmed from both fear of crime linked to previous victimisation experiences, and media representation of scam attempts was documented during the literature review. Participants' referrals were of great help in overcoming this significant recruitment barrier. After recruiting participants and conducting the Interviews, I recruited some of my participants through referrals of interviewees.

**Participants**

I recruited thirty-two victims of economic cybercrime, twelve non-victims as a control group and ten police officers and experts dealing with economic cybercrime. Detailed demographic information of the participants is demonstrated in Table 4.8.

*Table 4.8*
*Summary of the Interviews Conducted*

| Victims of Economic Cybercrime | | |
|---|---|---|
| Age | Gender | |
| | Male | Female |
| Under 30 years | 5 | 5 |
| Between 30 and 60 years | 6 | 6 |
| Over 60 years | 5 | 5 |
| Total number of participants | 16 | 16 |
| **Control Group** | | |
| | Gender | |
| | Male | Female |
| Under 30 years | 2 | 2 |
| Between 30 and 60 years | 2 | 2 |
| Over 60 years | 2 | 2 |
| Total number of participants | 6 | 6 |
| **Policing** | | |
| | Gender | |
| | Male | Female |
| Police Officers | 5 | 1 |
| Governmental Web Experts | 3 | |
| Private Sector | 1 | |
| Total number of participants | 9 | 1 |

### 4.6.3 Ethical Issues and Obtaining Ethics Approval

Durham University School of Applied Social Sciences Ethics Committee gave approval for the research in October 2016 (Appendix One). Participants were enabled to read the participant information sheet (Appendix Two) before the interviews. Key points such as anonymising their identity and recording interviews as well as the opportunity of quitting interview or not responding any unwanted questions were explained verbally before asking participants to sign consent form (Guest et al., 2012). Participant information sheets and consent forms were sent electronically to participants who were interviewed via Skype. Participants interviewed online were asked to send a confirmation email rather than signing a consent form as printing, singing and scanning confirmation form would occupy participants' time. Overall the ethics procedures also conformed to those set out by the British Sociological Association (B.S.A.) (see https://www.britsoc.co.uk/ethics.)

### 4.6.4 Interview Guide

The development procedure of the interview guide was mainly informed by the results of quantitative analysis. The content of the interview was arranged to both triangulate quantitative analysis results and to research aspects that were not covered by quantitative analysis (Appendix Five). This stage of the research was both explanatory and exploratory in nature.

### 4.6.5 Conducting Semi-Structured Interviews

Semi-structured interviews, the effectiveness of which is determined by the power relations between the researcher and the interviewee, is regarded as one of the most essential data collection methods in qualitative research paradigm due to its flexibility and power of generating in-depth knowledge through participants' accounts (Edwards and Holland, 2013;

Jones et al., 2013). It was proposed that the researcher positionality informed by age, gender, ethnicity and occupational background impacts the power relations in interview procedure (Ybarra and Mitchell, 2008; Denzin and Lincoln, 2017). I applied some measures to maintain a balanced power distribution between me and participants. To that end, interview setting, social distance and attitudes towards participants' reflections were utilised.

The opportunity of interview venue selection is generally regarded as a sign of power distribution in favour of interviewees (Grant, 2014). Interview settings are considered to be of utmost importance in conducting a fruitful knowledge production as some individuals tend to withhold information due to the influence of environment on human nature (Dyck, 1997; Frost, 2009; Doody and Noonan, 2013; Albuquerque et al., 2014). While some individuals may feel comfortable and relaxed in their home settings, some others may find the public place a secure environment (Mann and Stewart, 2000). Participants' home, workplace or public places may be chosen as the interview site.

Selection of one of these sites introduces challenges as well as rewards. Convenience, comfort, safety and travel costs are the considerations to be evaluated before making informed decisions about interview site selection (Raworth et al., 2012). To offer the most convenient interview setting, as a sign of respect to participants' needs and preferences, I encouraged participants to select the location of the interview before scheduling a meeting (Randall, 2011). Interviews with participants who were under sixty years old were mainly conducted in public places such as cafés and bars based on participants' choices, though, social places as sites of the interviews bear increased challenge of safeguarding privacy and confidentiality (Edwards and Holland, 2013). Interviews were mostly scheduled to at quiet times and materials such as interview guide, and voice recorder was not disclosed to overcome those challenges. I memorised the questions in the interview guide and uploaded them into my smartphone, to

refer should I need them, prior to the meetings. Interviews with participants who were over sixty years old took place either at their home or at the common rooms of the sheltered houses. Interviews with police officers and experts dealing with economic cybercrime took place at their offices.

I aimed to create a welcoming and relaxing atmosphere for the interviews. Before beginning interview procedures, I gave a brief description of the research including the aims of the research. I explained the precautions aimed at safeguarding privacy and anonymity of the interviewee (Welsh and Lavoie, 2012). Some of these precautions were deleting voice files after transcription, anonymising participants' name and destroying transcription after the submission of the thesis (McCudden, 2015; van Heumen, 2015). After making sure that participants understood the content of the participant information sheet and having the consent form signed, I began with general questions such as demographic information and frequency of Internet usage. Interviews were conducted in a flexible manner. I asked open-ended questions to the participant and used prompts if I perceived that responded had difficulties in understanding what I mean. In addition, some questions that appeared to be irrelevant to participants' victimisation experiences were not asked. For instance, if a participant lost money due to responding a fraudulent communication (phishing), I did not ask questions related to malware infection. Sensitive questions such as deviant online behaviour or participants' social, economic and psychological conditions were asked to the end of the interviews as most participants appeared to be a little bit nervous at the beginning of the interviews. Establishing mutual confidence and trust was another reason for leaving sensitive questions to the end of interviews.

Interviews with participants under sixty years old lasted about forty minutes whereas those with elderly people lasted slightly shorter as most elderly people did not use mobile

devices or public Wi-Fi to access the Internet, they gave short responses to my questions related to these technological aspects of victimisation. Interviews were audio recorded as it would be helpful to listen to conversations again to get a sense of meaning attached by interviewee (Fasick, 1977). Another benefit of audio recording is the opportunity to prove that interviews were conducted with real people. Though, I faced a challenge of using an audio recorder. I asked some questions related to deviant usage of the Internet. Middle age and older participants mostly denied engaging with such online usage. Nonetheless, some of my participants admitted to engaging with deviant online usage after finishing audio recording. This indicated the existence of distrust in spite of efforts to ensure it.

It is proposed that the use of terms or phrases may have implications for the power balance between the researcher and the respondent (Kvale, 2006; Hoffmann, 2007; Daley, 2010). I asked my participants whether they perceived themselves as a victim or not. Rather than using the term *'victimisation'*, I reiterated the phrase, *negative experience*, to denote my cautious manner for participants' feelings. Kvale (2006, p. 489) propose this kind of attitude as a sign of objectivity. "If social scientists want to become objective, they should seek the rare, extreme situations where their objects have maximum possibilities for protesting against what the researchers say about the situations where the objects are allowed to raise questions in their own terms rather than the researchers' term." Daley (2010) who researched lesbian and queer women community working in psychiatric and mental health services confronted participants' reactions for using the term lesbian instead of queer, a situation which widened the social distance between the researcher and the participants. Hoffmann (2007) experienced similar challenges when conducting a study at a coal mine. The use of the phrase, chairperson rather than chairman, created ideological discomfort for one of her interviewees. She explains this comfort as the sign of desire gaining power in the interview. "In this way, he did not merely express his preference but asserted a condition I had to satisfy to gain his participation. …he

determined the words I used, affecting the tone of the interview and its questions." (Hoffmann, 2007, p. 335).

Disclosing my background to participants seemed to be a crucial decision as it might have some practical implications for knowledge production. I had worked as a gendarmerie officer for fifteen years prior to commencing my postgraduate studies (MSc Criminology and PhD) at Durham University. As stated above, I desired to create an intimate and relaxed atmosphere for an interview; however, I feared that disclosing my professional background might hinder intimacy and broaden social distance between me and participants as some participants might find talking to a police officer formal or rather annoying. Due to these considerations, I preferred stating my doctoral student status while talking about me. Though, I explained my identity to police officers both to create a sense of intimacy and prevent possible future misunderstandings such as institutional concerns around the vetting issues.

My positionality as a researcher may be considered as a partial insider since I could be regarded as an insider due to my professional background and active online lifestyle. Nonetheless, I could also be considered as an outsider because of my ethnicity and age, which certainly highlighted some cultural differences between me and participants. Fiona Measham who experienced similar positionality issues as she was a clubber prior to research career, explains this status as "for clubland researchers who are also clubbers, 'taking sides' means confronting and exploring the conflicting emotions that arise from combining identities, and interacting with 'research subject' on both a personal and professional level" (Moore and Shepherd, 2006).

What I also have discovered was that my identity as a researcher was not stable throughout the research vis a vis participant's perception of myself (Lazarsfeld, 1958; Saunders and Zucker, 1999). Depending on the participants' age and our social relationship my

positionality fluctuated. For instance, I sometimes was an ‘expert’ while interviewing with older participants living in a sheltered accommodation but a son for my friend’s family. Sometimes I positioned as an insider while interviewing postgraduate students and a complete outsider during the interviews with female participants. Having law enforcement experience helped me to adapt to this flux of identities. With regards to interviews with police officers, my positionality fluctuated as well. I felt insider at times police officers talked about challenges they faced; however, quite an outsider when they were explaining the structure of policing combatting economic cybercrime.

I made use of this variety of identities during knowledge production. Having various identities during the knowledge production phase of the research enabled me to look at the economic cybercrime victimisation from different angles and gain rich information due to a sense of trust and intimacy created. On the one hand, being an insider helped me to ask more detailed questions about interviewees’ sincere perceptions about economic cybercrime and possible reasons’ of becoming a victim. I observed that participants reflected more at times when the social distance was very close. Though, they appeared to withhold themselves about private issues like deviant online usage. On the other hand, being an outsider facilitated gaining in-depth knowledge about online deviancy as the participants appeared to speak more freely to a foreigner whom they will never see. With this aspect, my ethnic background, which apparently hindered recruitment process, aided me during interviews.

### 4.6.6 Pilot Study

Discerning the potential design errors and identifying the key challenges prior to research is at the heart of conducting a fruitful study (Blessing and Chakrabarti, 2009; Daniel and Sam, 2011; Locke et al., 2014). It is, therefore, of utmost importance to conduct a small-scale pilot study before the main project (Hall and Hall, 2008; Maxwell, 2012). Many criminology studies (Farrall and Gadd, 2004; Finch and Munro, 2005; Boyle et al., 2007; Horn et al., 2015; Moore et al., 2016) conducted pilot studies prior to the main research not only to test research design (David and Sutton, 2011) but also to find out the potential pitfalls of research procedures (van Teijlingen and Hundley, 2002). Seven semi-structured interviews were conducted with victims of economic cybercrime. Age of participants was the main criteria for recruiting participants for the pilot study. Two participants were under thirty years old, two interviewees were between thirty and sixty years old, and one respondent was over sixty years old. I recruited an equal number of participants for each gender for two age categories under sixty years old. Implementing pilot study provided several benefits in terms of research design testing, interview guide alteration and assumptions testing.

The foremost benefit of conducting a pilot study for this thesis was pinpointing the need for alterations to the interview guide. Though not unique to this thesis, the need to divide questions into more comprehensive sub-sections, defining key terms, clarifying statements and adding new questions emerged as issues to be handled. Some other studies (i.e. Shimmen, 2011; Sterner and Sheng, 2013; Garton, 2014) conducting semi-structured interview base studies distinguished similar challenges. After conducting and transcribing pilot study audio recordings, interviews were analysed to assess whether questions were clear enough to be understood. I perceived that some of the questions needed to be divided into sub-questions as they dealt with more than one topic at the same time. Moreover, I changed the wording of some

questions as participants appeared to need an explanation of some terms such as phishing. New questions were also added to the interview guide to clearly understand the causes of victimisation. For instance, to distinguish between hacking and malware infection, a question asking whether participants observed unusual slowness in their devices used to access the Internet before experiencing victimisation. Besides, after reading pilot study transcriptions for several times, I realised that there might be a relationship between individuals' real word problems or social conditions and experiencing economic cybercrime victimisation. New questions asking participants' social, economic and psychological conditions before experiencing victimisation were also included in the interview guide.

With regards to testing the ability of the research design to address the research questions and the hypotheses proposed, primary analysis of the pilot study interviews suggested the interview guide's significant capability to address these issues. What is more, primary analysis of pilot study data indicated a possibility of integrating Protection Motivation Theory (Rogers, 1975) and Coping Adoption Approach Paradigm (Lazarus, 1980) into one single model, which is dubbed as 'The Cyber Victimisation Coping Model ' by this thesis (Figure 4.9). Viability of this proposed model was tested during the main study.

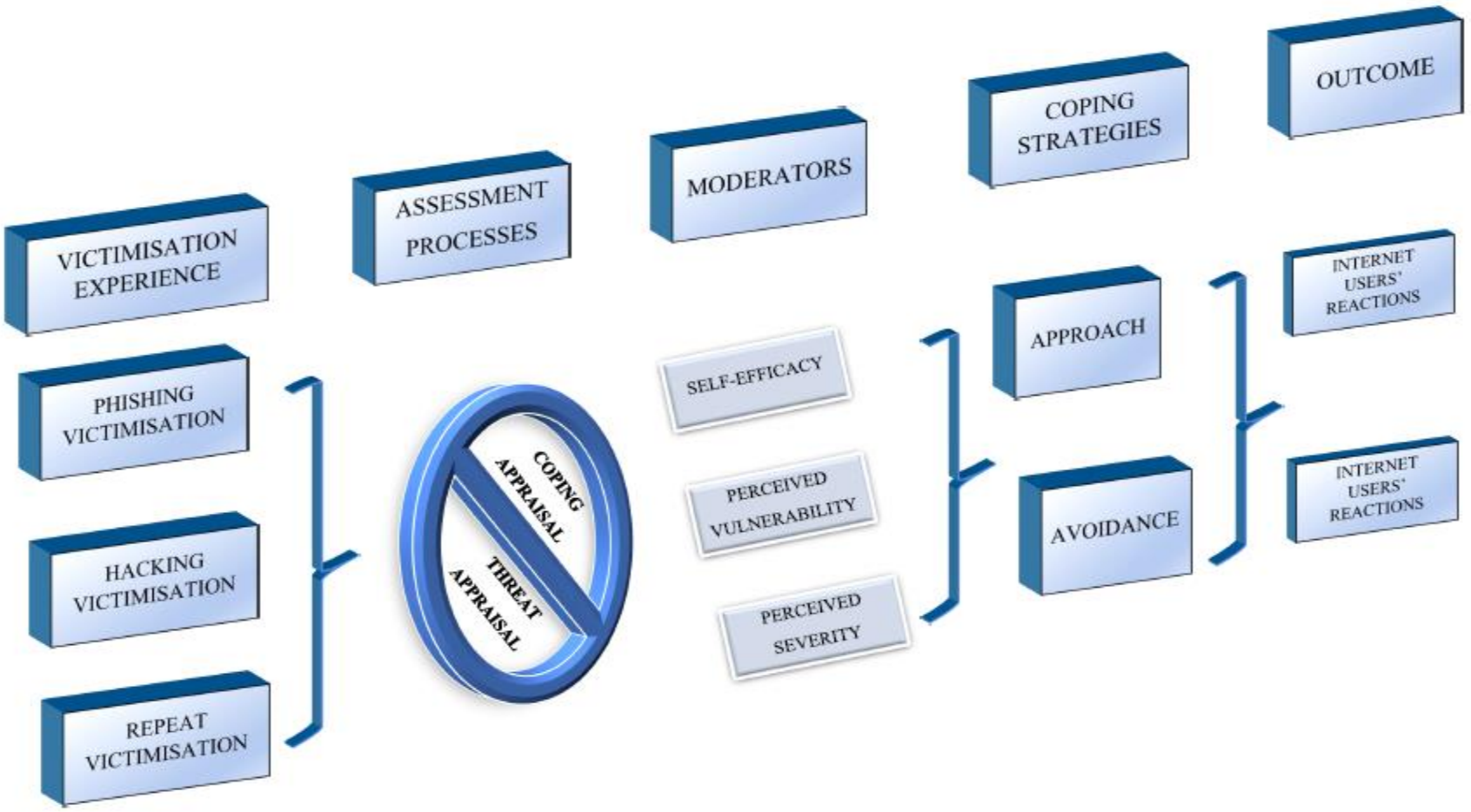



Figure 4.9: *The Cyber Victimisation Coping Model*

Another outcome of the pilot study was the choice of place for conducting interviews. I conducted my interviews at cafés where there was loud music mixing with the noise of the other customers. While transcribing pilot study interviews, I find out that the quality of recordings was very poor, which made it difficult to transcribe. Based on this experience, I tried to conduct the interviews at quiet times of cafés. Note taking was another strategy I used to overcome poor recordings

## 4.7 Analytic Procedure: Content Analysis

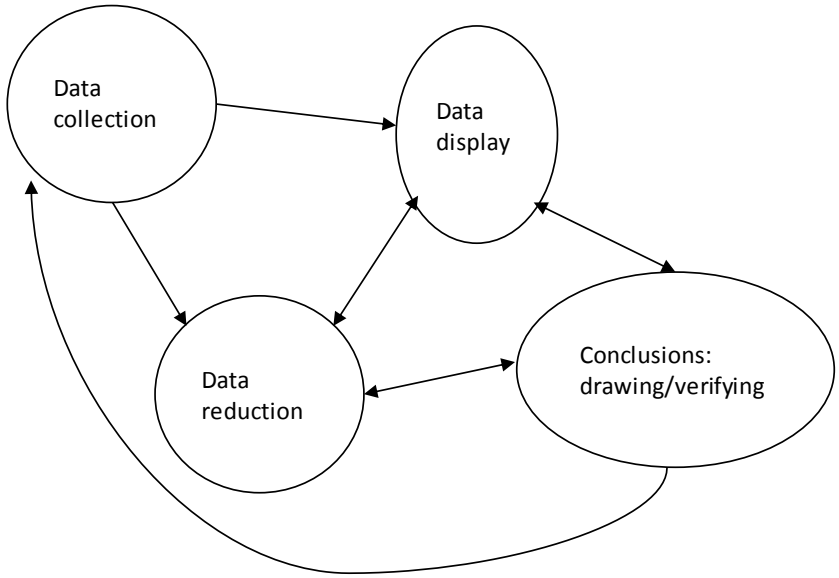
This thesis utilised content analysis method to provide a systematically analysed, replicable and valid account of economic cybercrime victimisation and discern the adverse effects of victimisation experiences through victims' lenses. Content analysis method can be quantitatively or qualitatively driven. Quantitative content analysis is "a method of analysing the contents of documents that uses quantitative measures of the frequency of appearance of particular elements in the text." (Jupp, 2006, p. 40). Whereas qualitative content analysis is "a research method for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns" (Hsieh and Shannon, 2005, p. 1278). The quantitative content analysis method was utilised to triangulate the quantitative analysis of CSEW 2014/2015 and discern the impact of victimisation on individuals' behavioural and security adaptations. The qualitative content analysis method was used to explore the factors affecting the likelihood of becoming an economic cybercrime victim.

This thesis applied Miles and Huberman (1994)'s three-stage process of qualitative data analysis. Miles and Huberman (1994, p. 10) argue that qualitative data analysis is a concurrent process of three activities, namely "data reduction", "data display" and "conclusion

drawing/verification". The following section explains the procedures applied while analysing the transcripts of semi-structured interviews and police reports.

Figure 4.10

*Data Analysis Process*




Miles and Huberman (1994)'s Interactive Model of Qualitative Data Analysis

### 4.7.1 Data Preparation

Interviews were transcribed verbatim immediately after conducting the interviews. Halcomb and Davidson (2006) underscore the essence of verbatim transcription for mixed methods researcher due to the iterative process of data analysis. Rather than hiring a professional transcriber, I transcribed the interviews myself. This self-transcription process enabled me to get closer to data (Britten, 1995; Oliver et al., 2005) and to get a sense of what respondents feel while speaking (Singh, 2007). However, the transcription process was cumbersome, as it was difficult to understand the local accents. I listened to conversations several times to understand the exact phrases quoted by participants. This difficulty turned into an advantage as it allowed me to spend more time with my data. I noted some preliminary thoughts and issues cited by participants while transcribing the recording. These memos

enabled me to engage with data actively. I also had the opportunity to compare my initial impression with those after analysis of the data.

Interview transcripts, together with police reports bearing 340 cyber-enabled fraud cases were uploaded to NVIVO qualitative analysis software. I utilised Crime Script Analysis Method to frame qualitative data analysis. Although this method is not used to analyse textual data while coding or constructing themes, it helped me to frame the analysis process in a systematic way (LeClerc and Wortley, 2013). The script Analysis method is used to analyse the sequence of events to gain an understanding of crime process (Cornish, 1994). This method divides the whole process into steps to enable researchers to examine the events that take place at each step Hutchings and Holt (2015, p. 115). {Burgard, 2013 #71 who applied it to cyber victimisation research created a three-step crime script, which is "getting hooked on, staying attuned and cooling out" Based on their template, I categorised the qualitative data into three sub-groups, which are being a target of an online attack, experiencing victimisation and post effects of victimisation experiences. After organising the dataset, I started the data reduction process.

### 4.7.2 Data Reduction

Data reduction is the phase where the data is reduced to its basic content in order to have a condensed material (Schilling, 2006). The data condensation procedure is a continuous and iterative process, including written summaries and coding (Berg et al., 2004). Hsieh and Shannon (2005) distinguish three approaches of coding in qualitative content analysis method: conventional content analysis, summative content analysis and directed/deductive content analysis The researcher derives the codes and categories from the data during the analysis of qualitative data in the *conventional content analysis method*. Keywords are derived from the literature review, and they can be identified either before or during the analysis process in

*summative content analysis approach*. *Directed or deductive content analysis approach* requires a theoretically informed research. Previous research findings or theory is used to derive codes (Hsieh and Shannon, 2005; Moretti et al., 2011).

Research questions, research aims, and research design shape the content analysis method (Krippendorff, 2004). Being a theoretically informed quantitatively driven mixed methods research, the qualitative data were used to triangulate quantitative research findings, explain the relationships appeared in quantitative analysis and explore the issues that quantitative analysis could not address. To these ends, directed/deductive content analysis method was used to triangulate and explain quantitative results. Thus, most of the categories that were utilised in content analysis were predefined by Lifestyle Routine Activities Theory and Approach Avoidance Coping Paradigm. Conventional content analysis approach was adopted to explore the emerging themes. Initially, the directed/deductive analysis process will be explained, and then the conventional content analysis approach will be presented.

Analysis started with creating a new NVIVO project and defining each respondent as a case. Afterwards, based on the theoretical frameworks, proximity and exposure to motivated offender, target suitability, online guardianship, approach and avoidance categories were created. Attributes such as the type of victimisation experienced (hacking, phishing, malware infection or multiple victimisations) and demographic characteristics (age, gender) were assigned to each case. Then, sub-categories were created as the analysis of the transcripts continued. For example, digital, personal and password management categories created under the main category of guardianship. The type of device utilised to access the Internet was another sub-category created under the main category of target suitability. This analysis was mainly based on less open-ended questions such as *"Have you provided your personal details to be eligible for a free Wi-Fi connection?"* or *"Which electronic devises did you use to access the Internet prior to your victimisation experience?"* Participants' responses were coded under

these sub-categories. After this iterative process which required assigning participants' responses to corresponding categories and sub-categories, a cross-tabulation analysis was conducted. Matrix coding query feature of NVIVO software was utilised to examine the relationships between respondents' online lifestyles, demographic characteristics and economic cybercrime victimisation.

Another NVIVO project was created to conduct conventional content analysis. This analysis aimed to explore the causes of being an economic cybercrime victim and understand the adverse post-victimisation impacts of victimisation experiences. This analysis was based on more open-ended questions like *"How your victimisation affected your online lifestyle?"* This analysis started with coding the textual data. Saldaña (2015, p. 3) defines a code as "a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data." Codes demonstrating similarities were grouped under upper-level parent categories. Later, these interrelated categories were grouped to discern the themes. Tables 4.9 and 4.10 and demonstrate the coding process applied while developing the concept of contextual vulnerabilities, which was one of the significant contributions of this thesis. Figure 4.11 illustrates analysis process.

Table 4.9
*Coding Process of Negative Life Events Category*

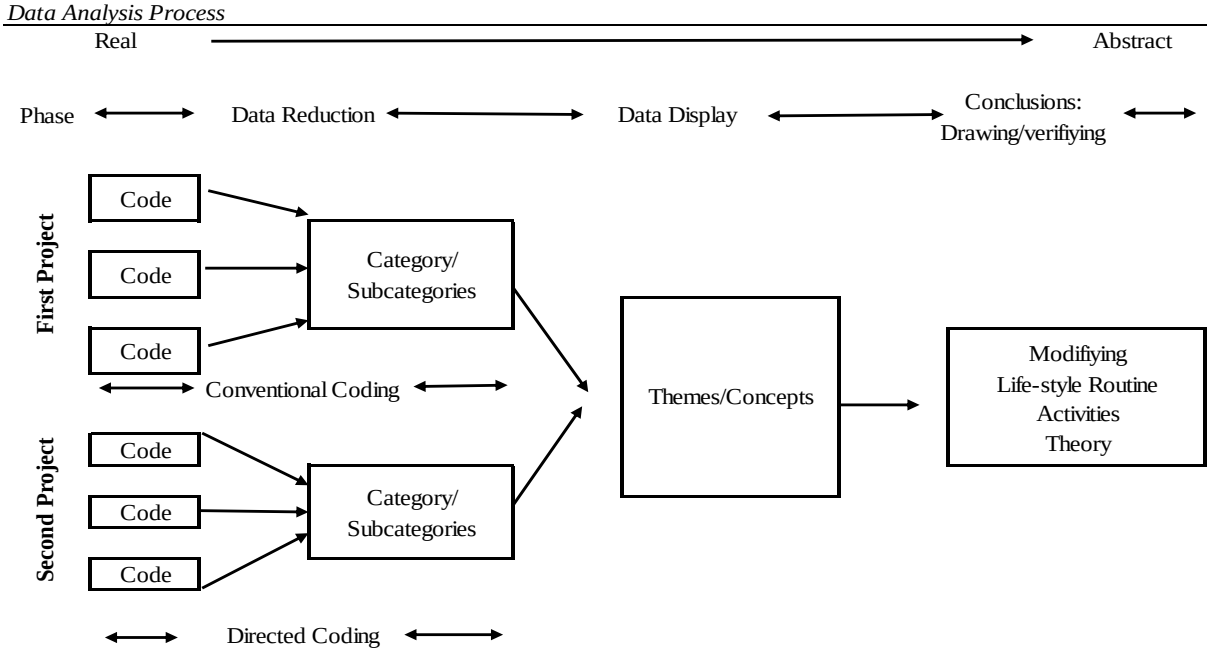
| | CODE | CATEGORY | THEME/CONCEPT |
|---|---|---|---|
| Interviewer: Could you please describe me your social, psychological and financial condition at the time of victimisation? | | | |
| Respondent 1: To be honest, it was when my nephew was in the hospital. So, we were all worried, and I had to buy many things with my card. So, I did not pay attention. We were living in a bubble. You go to hospital and see a sick boy. You cannot concentrate on what or where you buy it. Because we were there for seven weeks. And then once you got home you feel better and come back to yourself, become more cautious. It was quite an emotional, emotionally and physically draining, being at the hospital… Long days…So it was just a seven-week bubble. | Familial Problems | Negative Life Events | Contextual Vulnerabilities |
| Respondent 2: I have moved over B. to D., and I work in N.. I was settling up. I was getting an apartment through state agents, and there was various email back and forth. They needed personal information from me, which I exchanged via email. They also needed some bank details because I had to pay for a deposit and to set a direct debit with the landlord | Changing social settings | | |
| Respondent 3: I broke my long-time relationship just before that incident. It was really hard times as I had a bad relationship, which was about to cost my life. I was in a new place, making new friends. I was making a new life. I did not have financial issues. But socially and psychologically, I was not at my best point. I was just a girl who was trying to recover and trying to find a path again. | Psychologically down/Breaking Relationship | | |
| Respondent 4: I had just finished a long relationship. I have been looking for dating sites. At that time, perhaps I was not alert about that kind of thing, a little bit depressed about my situation. Because I have been in a long relationship and I was a little bit down. I think that was part of it. That might have been where somebody got the information from. Financially I was really well off. I got a good salary | Psychologically down/Breaking Relationship | | |

Table 4.10
*Coding Process of Contextual Vulnerabilities Concept*

| CODE | SUB-CATEGORY | SUB-CATEGORY | CATEGORY | THEME/CONCEPT |
|---|---|---|---|---|
| Cross-tabulation results | Age<br>Gender<br>Education Level<br>Household Income | Demographic Characteristics | Individual and Behavioural Vulnerabilities | Contextual Vulnerabilities |
| Confidence in getting a refund<br>Significance of shared information<br>Lack of Internet skills<br>Social benefits of self-disclosure<br>Interconnectedness<br>Building a professional network | Perceived Severity<br>Perceived Vulnerability<br>Self-efficacy<br>Perceived Rewards | Psychological Factors | | |
| Same password usage<br>Weak password usage<br>Problems with memorising passwords<br>A large number of online accounts | Password management | Password fatigue | | |
| Cross-tabulation results | Impact of electronic devices | Technological Vulnerabilities | Macro Vulnerabilities | |
| Installing unknown applications<br>Giving permissions to access the phone | Mobile applications | | | |
| Free Wi-Fi Risks<br>Public access Internet | Secure Internet connection | | | |
| Increased phishing attempts<br>Saving users' personal information<br>Insecure shopping websites | | Data Breaches of Companies | | |
| Familial problems<br>Changing social settings<br>Breaking up a relationship | | Negative life events | Socio-cultural Vulnerabilities | |
| Decreased attention<br>Tiredness<br>Fatigue | | Workload or fatigue | | |
| Living alone<br>Lack of Internet skills | | Availability of consultancy | | |

Figure 4.11

*Data Analysis Process*




Adopted from Miles and Huberman (1994) and Saldaña (2015)

### 4.7.2 Data Display

Miles et al. (2014, p. 7) define as display as "an organized, compressed assembly of information that allows conclusion drawing and action." Extended texts, tables, graphs and diagrams as well as direct quotes, can be utilised to present research findings (Miles and Huberman, 1994; Berg et al., 2004). As reading and evaluating extended texts can be a cumbersome process due to cognitive overload (Onwuegbuzie and Dickinson, 2008), tables, quotes and diagrams are increasingly utilised for visual representations (O'Flaherty and Whalley, 2004).

David and Sutton (2011) suggest numerical tables and non-numerical code search results as two display methods for qualitative researchers. This thesis utilised tables to summarise the participants' demographic characteristics, illustrate cross-tabulation results such as the relationships between the types of electronic devices utilised to access the Internet, free Wi-Fi usage and the type of victimisation experienced. Additionally, participants' coping

strategy adaption across age categories is also demonstrated through tables. Diagrams are also used to summarise and illustrate the victimisation models built as a result of qualitative analysis.

Besides these visual representations, direct quotes from victims' accounts were also heavily utilised throughout the qualitative result chapters. This thesis presented verbatim quotes to provide evidence for the interpretations made (reliability and validity), illustrating participants' views and improve the readability of the thesis (Corden and Sainsbury, 2006). Guest and MacQueen (2008) suggest presenting verbatim quotes to improve the validity of the research findings as quotes demonstrate the raw data that interpretations were based on. The quantity of verbatim quotes to be is one of the critical issues. Berg et al. (2004) argue that at least three independent quotations should be provided for each interpretation to illustrate researchers' interpretation. David and Sutton (2011, p. 586) argue that presentation of examples most of the times causes ambiguity about the representativeness of the examples given. Hence, researchers need to clarify the extent to which selected quotes represent the data, or the relative significance of selected extreme quotes for the particular interpretation should be explained. To address these concerns, I acknowledged the number of cases linked to the theme presented when the interpretations were discussed. Additionally, I also tried to provide at least three separate account for each theme exemplified by verbatim quotes.

### 4.7.3 Conclusion Drawing

This is the last phase in Miles and Huberman's (1994) three-step analysis process. This step is where analytic conclusions were made (Berg et al., 2004). Being a theoretically informed mixed methods research, quantitative analysis results of CSEW 2014/2105 were juxtaposed to the content analysis findings in the light of Lifestyle Routine Activities Theory and Approach-Avoidance Coping Paradigm to arrive conclusions.

## 4.8 Summary

The mixed methods approach has been increasingly employed in social sciences over the last two decades (Ivankova et al., 2006; Johnson et al., 2007; Greene, 2008), yet; it has rarely been used in cyber criminology studies. This research is one of the first studies that applied a mixed methods approach to study cyber criminology. This approach aiming to combine the strengths of two research paradigms (Stenbacka, 2001) provided tools with both to analyse large number sample size quantitative data and explore the underlying meanings of the quantitative analysis results through victims' accounts (Hesse-Biber and Johnson, 2015). The significance of application this application for criminology lies in its ability to incorporate generalizability of statistical analysis results with qualitatively enriched interpretations (Abbas and Charles, 2003), which enables gaining an in-depth understanding of the underlying causes of economic cybercrime victimisation (Clark and Creswell, 2014).

# Chapter 5 Quantitative Results

## 5.1 Introduction

This first empirical chapter presents the quantitative analysis results of the Crime Survey for England and Wales (CSEW) 2014/2015. The goal of this first empirical chapter was twofold: first, to test the applicability of LRAT to economic cybercrime empirically, which may allow us to develop a new theoretical framework for cybercrime research and, the second, discern online correlates of economic cybercrime victimisation. This chapter consists of four sections. The first section of the chapter introduces descriptive statistics of variables utilised in bivariate and multivariate analyses. This section aims to provide background information about the general state of economic cybercrime victimisation. The second section of this chapter illustrates bivariate and multivariate analysis results aimed to discern online lifestyle correlates of economic cybercrime victimisation and to test the applicability of LRAT concepts to economic cybercrime by testing hypotheses formulated. The penultimate section demonstrates the results of statistical analysis measuring the impact of the type of device utilised to access the Internet on the risk of experiencing economic cybercrime victimisation. The last section of this chapter examines the extent of fear of cybercrime in the UK.

Lifestyle Routine Activities Theory (LRAT) asserts that people's routine activities and lifestyles may have an impact on the risk of being a victim of a crime (Hindelang et al., 1978; Cohen and Felson, 1979). It is argued that "victimisation is not randomly distributed across time and space"; thus, individuals' lifestyles or routine activities put them into closer proximity to motivated offers and increase their exposure to would be offenders at risky times and places (Hindelang et al., 1978, p. 617). Cohen and Felson (1979) argue that crime is the product of three elements that congregate at the same time and place. These elements are motivated

offender, suitable target and absence of a capable guardian. The motivated offender is a given fact, which can be ignored in crime analysis, since a motivated offender may always be present (Osgood et al., 1996; Sasse, 2005). It is the individuals' behaviours and lifestyles that facilitate victimisation by increasing their target suitability (Hindelang et al., 1978). Hence, it would be argued that LRAT perspective implicitly put the onus of victimisation on victims (Eigenberg, 2008).

As it was discussed in the first Literature Review Chapter (Chapter Two) extensively, these theories were proposed to explain victimisation in the physical world; it is Grabosky (2001) who proposed that these theories can be used to explain the victimisation in the cyberspace for the first time. Since then, opportunity theories of victimisation perspective have been applied as a theoretical framework in cybercrime victimisation studies. However, explanation power and applicability of LRAT as a theoretical framework is a highly contested issue (Yar, 2005). A number of cybercrime studies, the result of which yielded mixed evidence, tested applicability of LRAT to cybercrime victimisation. Assessing the applicability LRAT for economic cybercrime victimisation was one of the aims of this thesis since this argues that testing applicability of LRAT may provide new insights, which in turn may enable proposing a new theoretical approach to better understand victimisation in cyberspace.

There is extensive research on cybercrime victimisation for example; online correlates of malware infection (Bossler and Holt, 2009; Holt and Bossler, 2013; Leukfeldt, 2015), phishing (Hutchings and Hayes, 2008; Leukfeldt, 2014), online identity theft (Paek and Nalla, 2015; Williams, 2015), online harassment (Marcum et al., 2010; Marcum, 2011; Reyns et al., 2011; Reyns et al., 2016), hacking (Choi, 2008; Choi et al., 2016) multiple forms of cybercrime (Ngo and Paternoster, 2011; van Wilsem, 2013b; Reyns et al., 2015) and online fraud (Pratt et al., 2010; van Wilsem, 2013a; Policastro and Payne, 2014) have been researched. However,

online lifestyle correlates of economic cybercrime victimisation have not been researched yet. Moreover, LRAT conceives peoples' online behaviours and lifestyles as the facilitator of victimisation. This thesis asserts that some other factors such as technological vulnerabilities might have an impact on the occurrence of the victimisation.

## 5.2 Descriptive Statistics:

This section of the chapter illustrates the results of key descriptive statistical analyses, which are about the variables used in quantitative analyses, to provide background information about the frequency of each construct in the sample population.

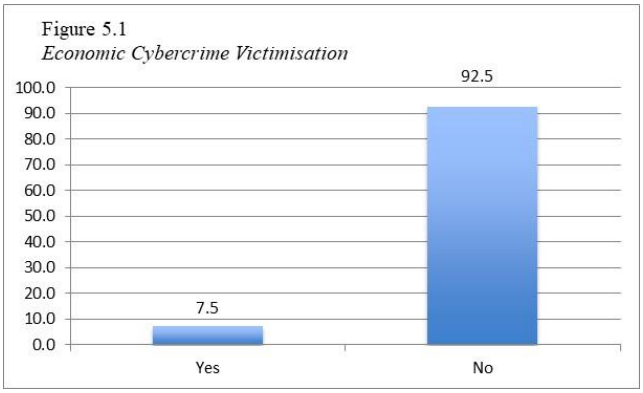
### 5.2.1 Outcome Variable:

The outcome variable of this analysis is *economic cybercrime victimisation*. Cybercrime is an umbrella term that encompasses various forms of online financial crimes (Levi, 2016). Variable economic cybercrime victimisation was obtained through a combination of variables representing financial loss through card-not-present fraud, online banking fraud, online identity fraud, and loss of money through responding communication (phishing). Statistical procedures while obtaining this variable were outlined in the Methodology Chapter (Chapter Four). As Table 5.1 illustrates, 5665 respondents answered Module D of Crime Survey for England and Wales 2014/2015. 7.5% of these participants reported experiencing at least one form of economic cybercrime.

Table 5.1
*Economic Cybercrime Victimisation*

| | *Frequency* | *Percent* |
|---|---|---|
| Yes | 424 | 7.5 |
| No | 5241 | 92.5 |
| Total | 5665 | 100.0 |

Figure 5.1
*Economic Cybercrime Victimisation*



### 5.2.2 Response Variables:

Table 5.2 displays descriptive statistics of response variables, namely online lifestyle activities variables. Online lifestyle variables were grouped into three categories to illustrate the constructs of the theory. Whereas online activities that require disclosure of personal financial information were operationalised as exposure to the motivated offender, those which do not necessarily require financial information disclosure were operationalised as proximity to motivated offenders. As can be seen from Table 5.2, using email/chat rooms (85%), browsing for news (80.7%) and buying goods or services online (80.5%) were the most popular reasons to access the Internet. Conversely, playing online games/doing quizzes and competitions was the least cited reason for accessing the Internet.

Table 5.2

*Frequency of Variables Representing Proximity and Exposure to Motivated Offender*

| Variable | N | % |
|---|---|---|
| Proximity and Exposure to Motivated Offender | | |
| Online Financial Activities | | |
| Online banking or managing finances (e.g. paying credit cards) (N=5665) | | |
| No | 1903 | 33,6 |
| Yes | 3762 | 66,4 |
| Buying goods or services (internet shopping, inc. music / film downloads) | | |
| No | 1107 | 19,5 |
| Yes | 4558 | 80,5 |
| Online Governmental Services (e.g. tax returns, DVLA, council tax, benefits) | | |
| No | 2297 | 40,5 |
| Yes | 3368 | 59,5 |
| Online Social Activities | | |
| Social networking (e.g. Facebook, Twitter) or blogging | | |
| No | 2163 | 38,2 |
| Yes | 3502 | 61,8 |
| E-mail, instant messaging, chat rooms | | |
| No | 849 | 15 |
| Yes | 4816 | 85 |
| Online Leisure Activities | | |
| Browsing for news or information (e.g. BBC, Wikipedia) | | |
| No | 1094 | 19,3 |
| Yes | 4571 | 80,7 |
| Playing online games/doing quizzes/competitions | | |
| No | 3760 | 66,4 |
| Yes | 1905 | 33,6 |

Table 5.3 demonstrates online security measures that respondents applied in the last 12 months. As discussed in the Methodology chapter of this thesis, guardianship measures were categorised into two main groups and relevant subcategories according to their intended usage. This categorisation is novel to this thesis since past research generally categorised security measures as digital and personal guardianship measures. When we look at the security measures applied by respondents to ascertain electronic devices' security, installing anti-virus software (68.8%) and deleting suspicious emails without opening them (71.2%) was the most frequently applied guardianship measures. Results pertaining to the security measures to protect personal data demonstrate that complex passwords (65.6%), only using well-known or trusted sites (61.6%) and logging out when finished (62.6%) were the most favourite safeguarding measures to ascertain personal data security. However, it is interesting that

personal data protection security measures, using different passwords for a different online account (38.5%) and adjusting website account settings (e.g. privacy settings) (25.7%) were the least preferred guardianship measures. Lack of these guardianship measures may lead to loss of personal data such as financial and identifying personal information. Implications of these results are checked here with statistical analysis and semi-structured interviews.

Table 5.3

*Frequency of Variables Representing Guardianship Measures*

| Variable | N | % |
|---|---|---|
| **Online Guardianship** | | |
| ***Protecting Electronic Devices Used to Access the Internet*** | | |
| Precautionary Guardianship Measures to Protect Electronic Devices Used to Access the Internet | | |
| Only downloaded known files or programs | 2598 | 45,9 |
| No | 3067 | 54,1 |
| Yes | | |
| Deleted suspicious emails without opening them | | |
| No | 1634 | 28,8 |
| Yes | 4031 | 71,2 |
| Protected your home wireless connection (wi-fi) with a password or been cautious using | | |
| No | 2472 | 43,6 |
| Yes | 3193 | 56,4 |
| Software-Based Guardianship Measures To Protect Electronic Devices Used to Access the Internet | | |
| Downloaded software updates and patches whenever prompted | | |
| No | 3069 | 54,2 |
| Yes | 2596 | 45,8 |
| Installed anti-virus or other security software, such as a firewall | | |
| No | 1770 | 31,2 |
| Yes | 3895 | 68,8 |
| Scanned computer regularly for viruses or other malicious software | | |
| No | 2868 | 50,6 |
| Yes | 2797 | 49,4 |
| ***Protecting Personal Data*** | | |
| Guardianship Measures to Protect Financial Information | | |
| Only used well-known or trusted sites | | |
| No | 2173 | 38,4 |
| Yes | 3492 | 61,6 |
| Checked for signs that a site is secure when buying online (closed padlock sign/https website | | |
| No | 2868 | 50,6 |
| Yes | 2797 | 49,4 |
| Guardianship Measures to Protect Personal Account Security | | |
| Used complex passwords (contain letters, numbers and symbols) | | |
| No | 1948 | 34,4 |
| Yes | 3717 | 65,6 |
| Used a different password for each different online account | | |
| No | 3485 | 61,5 |
| Yes | 2180 | 38,5 |
| Logged out of websites when you are finished | | |
| No | 2120 | 37,4 |
| Yes | 3445 | 62,6 |
| Adjusted website account settings (e.g. privacy settings) | | |
| No | 4211 | 74,3 |
| Yes | 1454 | 25,7 |
| Guardianship Measures to Protect Personal Privacy | | |
| Only added known persons as friends on social networks. | 2935 | 51,8 |
| No | 2730 | 48,2 |
| Yes | | |
| Been careful about putting personal details on social networking sites | | |
| No | 2389 | 41,6 |
| Yes | 3306 | 58,4 |

Table 5.4 illustrates figures for the frequency of Internet usage. As can be seen from Table 5.4, approximately 72% of Internet users accessed the Internet several times a day. This result confirms the European Commission report, which says that 75% of the British population access the Internet every day (European Commission Report, 2015). The figures for accessing the Internet once a day and less often once a day are very close, approximately 15% and 14% respectively.

Table 5.4

*Frequency of Internet Usage*

| | **N** | **%** |
|---|---|---|
| Several Times a Day | 4055 | 71.6 |
| Once a Day | 843 | 14.9 |
| Less often than Once a Day | 767 | 13.5 |

Table 5.5 displays the frequency of electronic device usage. The electronic devices used to access the Internet were categorised into two risk groups. Whereas the electronic devices used with a secure Internet connection were hypothesised as low-risk electronic devices, other electronic devices using relatively insecure Internet connections and those generally lacking some internal security measures like anti-virus software were conceptualised as high-risk devices. Descriptive statistics results demonstrate that laptop used at home/work/school/college (72.9%) and mobile phone/smartphone (68.7%) were the most preferred electronic devices used to access the Internet. Conversely (or something similar) public access computer (10.6%) and laptop used away from home/work/college/school (31.2%) were the least preferred electronic devices to access the Internet.

Table 5.5

*Frequency of Variables Representing Electronic Devices Used to Access the Internet*

| Variable | N | % |
|---|---|---|
| **Low Risk Electronic Devices** | | |
| Desktop computer (at home or work or school/college) | 2486 | 43,9 |
| No | 3179 | 56,1 |
| Yes | | |
| Laptop (at home or work or school/college) | | |
| No | 1538 | 27,1 |
| Yes | 4127 | 72,9 |
| **High Risk Electronic Devices** | | |
| Laptop (away from home and work or school/college) | | |
| No | 3898 | 68,8 |
| Yes | 1767 | 31,2 |
| Mobile phone or smartphone | | |
| No | 1774 | 31,3 |
| Yes | 3891 | 68,7 |
| Handheld computer (e.g. iPad, tablet, palmtop) | | |
| No | 2835 | 50 |
| Yes | 2830 | 50 |
| Public access computer (e.g. In a library, internet cafe) | | |
| No | 5066 | 89,4 |
| Yes | 599 | 10,6 |

### 5.3.3 Control Variables:

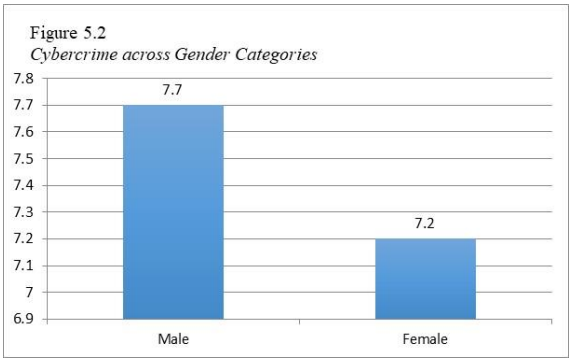
#### 5.3.3.1 Gender:

As Table 5.6 and Figure 5.2 illustrate, male Internet users faced economic cybercrime victimisation at a slightly higher frequency than female participants. This small difference may be interpreted as the lack of gender difference in economic cybercrime victimisation. However, descriptive statistics is not enough to draw the inference; this issue will be explored through bivariate and three-way analysis in the following section of this chapter.

Table 5.6
*Economic Cybercrime across Gender Categories*

| | | *Frequency* | *Percent* |
|---|---|---|---|
| Male | Yes | 237 | 7.7 |
| | No | 2830 | 92.3 |
| | Total | 3067 | 100.0 |
| Female | Yes | 187 | 7.2 |
| | No | 2411 | 92.8 |
| | Total | 2598 | 100.0 |

Figure 5.2
*Cybercrime across Gender Categories*



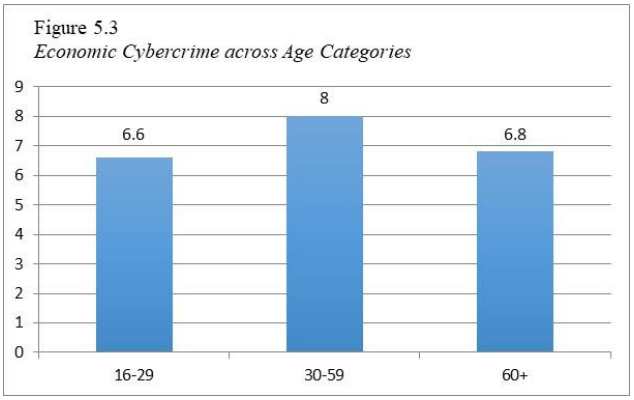

### 5.3.3.2 Age:

Ages of respondents were divided into three categories to examine the distribution of economic cybercrime victimisation through three generations of participants, namely young, middle-aged and elderly interviewees. Whereas young and elderly Internet users reported approximately similar victimisation figures, middle-aged Internet users reported the highest victimisation rates with 8% (Table 5.7 and Figure 5.3).

Table 5.7
*Economic Cybercrime across Age Categories*

| | | *Frequency* | *Percent* |
|---|---|---|---|
| 16-29 | Yes | 62 | 6.6 |
| | No | 874 | 93.4 |
| | Total | 936 | 100.0 |
| 30-59 | Yes | 262 | 8.0 |
| | No | 2999 | 92.0 |
| | Total | 3261 | 100.0 |
| 60+ | Yes | 100 | 6.8 |
| | No | 1368 | 93.2 |
| | Total | 1468 | 100.0 |

Figure 5.3
*Economic Cybercrime across Age Categories*



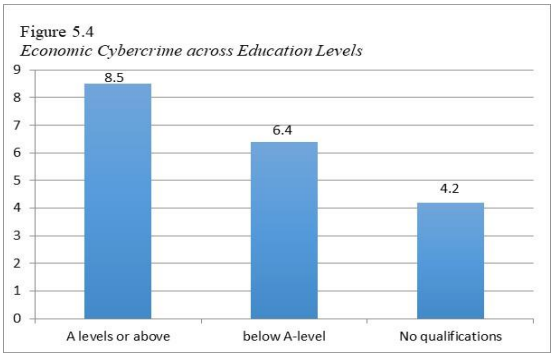

### 5.3.3.3 Education Level:

When the figures of the victimisation were examined across three strata of education level, it can be seen that there is a pattern of victimisation among Internet users: Internet users with higher education level reported highest victimisation percentages and figures of the victimisation decreases while education level decreases. Whereas Internet users with A Levels or above education reported 8.5% percentage of victimisation, those with no qualifications reported 4.2% percentage of victimisation. These figures appear to suggest that the education

level of individuals plays an essential role in the likelihood of experiencing economic cybercrime victimisation (Table 5.8 and Figure 5.4).

Table 5.8
*Economic Cybercrime across Education Categories*

| | | *Frequency* | *Percent* |
|---|---|---|---|
| A levels or above | Yes | 300 | 8.5 |
| | No | 3223 | 91.5 |
| | Total | 3523 | 100.0 |
| Below A-level | Yes | 98 | 6.4 |
| | No | 1425 | 93.6 |
| | Total | 1523 | 100.0 |
| No qualifications | Yes | 26 | 4.2 |
| | No | 593 | 95.8 |
| | Total | 619 | 100.0 |

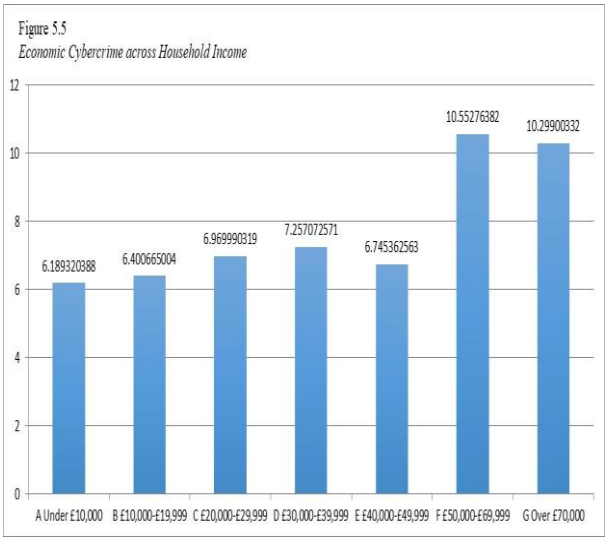



### 5.3.3.4 Household Income:

Distribution of economic cybercrime victimisation across different categories of household income illustrates that whereas Internet users who have a household income under £50,000 reported close victimisation percentages, those who have more than £50,000 household income reported significantly higher victimisation percentages. These results appear to suggest that those with £50,000 household income were at increased risk of experiencing economic cybercrime (Table 5.9 and Figure 5.5).

Table 5.9
*Economic Cybercrime across Household Income Categories*

| | | *Frequency* | *Percent* |
|---|---|---|---|
| A Under £10,000 | Yes | 51 | 6.2 |
| | No | 773 | 93.8 |
| | Total | 824 | 100.0 |
| B £10,000-£19,999 | Yes | 77 | 6.4 |
| | No | 1126 | 93.6 |
| | Total | 1203 | 100.0 |
| C £20,000-£29,999 | Yes | 72 | 7.0 |
| | No | 961 | 93.0 |
| | Total | 1033 | 100.0 |
| D £30,000-£39,999 | Yes | 59 | 7.3 |
| | No | 754 | 92.7 |
| | Total | 813 | 100.0 |
| E £40,000-£49,999 | Yes | 40 | 6.7 |
| | No | 553 | 93.3 |
| | Total | 593 | 100.0 |
| F £50,000-£69,999 | Yes | 63 | 10.6 |
| | No | 534 | 89.4 |
| | Total | 597 | 100.0 |
| G Over £70,000 | Yes | 62 | 10.3 |
| | No | 540 | 89.7 |
| | Total | 602 | 100.0 |



This section has examined the descriptive statistics of the economic cybercrime victimisation. Results indicate that whereas gender may not be a good predictor of the likelihood of experiencing economic cybercrime victimisation; age, household income and education level seem to be good predictors of the likelihood of experiencing economic cybercrime victimisation. The results appear to indicate that middle-aged Internet users (aged between 30 and 59), Internet users with higher education levels and higher household income were at increased risk of experiencing economic cybercrime victimisation. The next section of the chapter displays the results pertaining to online correlates of economic cybercrime victimisation.

## 5.3 Online Lifestyle Correlates of Economic Cybercrime Victimisation

This section of the chapter aims to find out the online activities that may have an impact on the risk of experiencing economic cybercrime victimisation. Testing the applicability of Lifestyle Routine Activities Theory (LRAT) is another goal of this section. The analysis process applied to achieve these goals is now briefly be explained. Initially, the relationships between constructs of LRAT, namely online activities and guardianship measures and the risk of facing economic cybercrime were examined through bivariate and three-way cross-tabulation analyses. This examination aimed to distinguish statistically insignificant variables since the omission of insignificant variables increases the predictive power of each variable included into the binary logistic regression analysis to be conducted in the next step (Agresti, 1996; Field, 2009). After discerning statistically significant correlates of economic cybercrime, the risk of victimisation posed by each element was assessed through binary logistic regression analysis.

Firstly, the results pertaining to bivariate analyses will be discussed, and then those related to multivariate analyses will be presented.

### 5.3.1 Bivariate Analyses

The relationship between online activities and the risk of experiencing economic cybercrime victimisation was examined through bivariate cross-tabulation analyses. Several cross-tabulation analyses were conducted to test the two hypotheses (null-$H_0$ and alternative-$H_a$). Whereas the null hypothesis denoted the absence of a relationship between lifestyle constructs and economic cybercrime, the alternative hypothesis referred to the presence of the relationship. Chi-square test was conducted to test the statistical significance of the relationship between variables. While P-values smaller than 0.05 enabled us to reject the null hypothesis and accept the alternative hypothesis, P-values greater than 0.05 let us accept the null hypothesis. Also, Phi test was done to assess the strength of the relationship between two variables. As the outputs of the test results would occupy big space, summaries of the results are displayed in the tables.

**Hypothesis 1:**

$H_0$= There is no relationship between online lifestyle and experiencing economic cybercrime victimisation.

$H_a$= There is a relationship between online lifestyle and experiencing economic cybercrime victimisation.

**Hypothesis 2:**

$H_0$= There is no relationship between the type of guardianship measures and experiencing economic cybercrime victimisation.

$H_a$= There is a relationship between the type of guardianship measures and experiencing economic cybercrime victimisation.

#### 5.3.1.1 Operationalisation of the LRAT Concepts

Operationalisation of the response variables according to the constructs of Lifestyle Routine Activities Theory is displayed in Tables 5.10 and 5.11. Online activities such as *using online banking*, *online purchasing* and *online government services* were operationalised as the exposure element of the theory since Internet users reveal their personal identifying information while accessing the Internet for those purposes. The frequency of Internet usage was also operationalised as the exposure element since the more time spent online; the more information is revealed (Hutchings and Hayes, 2008; Marcum, 2011; Leukfeldt, 2015).

Online activities, a*ccessing the Internet for social networking*, *e-mail/instant messaging/chatroom*, *browsing for news/information* and *playing online games*, were operationalised as the proxy measures of the proximity to motivated offender since Internet users do not have to reveal their financial information while accessing these services. However, using the Internet for those purposes still bears some risk as Internet users may disclose their non-financial personal information while accessing these websites.

Table 5.10

*Response Variables*

| *Variable Coding* | *Variable Name* |
|---|---|
| *Exposure to Motivated Offender* | |
| | *1. Online Financial Activities* |
| Eusint3a | Online banking or managing finances (e.g. paying credit cards) |
| Eusint3b | Buying goods or services (internet shopping, inc. music / film downloads) |
| | *2. Online Government Services* |
| Eusint3c | Online government services (e.g. tax returns, DVLA, council tax, benefits) |
| | *3. Frequency of the Internet Usage* |
| Recode_intern3 | Several Times a Day |
| | Once a Day |
| | Less often than Once a Day |
| *Proximity to Motivated Offender* | |
| | *3. Online Social Activities* |
| Eusint3d | Social networking (e.g. Facebook, Twitter) or blogging |
| Eusint3e | E-mail, instant messaging, chat rooms |
| | *4. Online Leisure Activities* |
| Eusint3f | Browsing for news or information (e.g. BBC, Wikipedia) |
| Eusint3g | Playing online games/doing quizzes/competitions |

Table 5.11

*Response Variables of Online Guardianship Measures*

| *Variable Coding* | *Variable Name* |
|---|---|
| *1. Guardianship Measures to Protect Electronic Devices' Security* | |
| | *1a. Precautionary Guardianship Measures to Protect Electronic Devices' Security* |
| Eprode4a | Only downloaded known files or programs |
| Eprode4g | Deleted suspicious emails without opening them |
| Eprode4l | Protected your home wireless connection (wi-fi) with a password or been cautious using |
| | *1b. Software-based Guardianship Measures to Protect Electronic Devices' Security* |
| Eprode4c | Downloaded software updates and patches whenever prompted |
| Eprode4j | Installed anti-virus or other security software, such as a firewall |
| Eprode4k | Scanned computer regularly for viruses or other malicious software |
| *2. Guardianship Measures to Protect Personal Data* | |
| | *2a. Guardianhip Measures to Protect Financial Information* |
| Eprode4b | Only used well-known or trusted sites |
| Eprode4f | Checked for signs that a site is secure when buying online (closed padlock sign/https website |
| | *2b. Guardianship Measures to Protect Personal Account's Security* |
| Eprode4d | Used complex passwords (contain letters, numbers and symbols) |
| Eprode4e | Used a different password for each different online account |
| Eprode4h | Logged out of websites when you are finished |
| Eprode4i | Adjusted website account settings (e.g. privacy settings) |
| | *2c. Guardianship Measures to Protect Personal Privacy* |
| Eprode4m | Only added known persons as friends on social networks. |
| Eprode4n | Been careful about putting personal details on social networking sites (e.g. date of birth,place of work) / not put personal details online |

### 5.3.1.2 The Results of Bivariate Analyses

**Exposure and Proximity to Motivated Offenders**

Table 5.12 summarises the cross-tabulation results for the association between online lifestyle variables and economic cybercrime victimisation. The chi-square test results demonstrate that all exposure to motivated offender variables were statistically significantly associated with the victimisation. The chi-square test values are as follow: using the Internet for *"online banking"* ($\chi^2$=23.587, p<0.001), *"buying goods or services online"* ($\chi^2$=25.754, p<0.001) and *"online government services"* ($\chi^2$=29.616, p<0.001). Yet, the Phi values ($\theta$=0.065, 0.067 and 0.072 respectively) indicate that the strength of the relationships was weak since the Phi values lower than 0.1 can be interpreted as a weak relationship (Healey, 2014).

With regards to proximity to motivated offender variables, *playing online games/doing quizzes/competitions* was not statistically significantly associated with victimisation ($\chi^2$=1.240, p>0.05). Yet, other proximity variables, using the Internet for *social networking* ($\chi^2$=4.714, p<0.05), *e-mail, instant messaging and chat rooms* ($\chi^2$=29.726, p<0.001) and *browsing for news or information* ($\chi^2$=5.321, p<0.05) were statistically significantly associated with the victimisation. The Phi values (θ=0.029, 0.072 and 0.030 respectively) indicate that the strength of these relationships was also weak.

Table 5.12

*Cross-tabulation Results for the Relationship between Online Activities and Experiencin Economic Cybercrime Victimisation*

| | *Phi* | *Chi-square Tests* |
|---|---|---|
| Exposure to Motivated Offender | | |
| Online banking or managing finances (e.g. paying credit cards) | 0,065 | 23.587* |
| Buying goods or services (internet shopping, inc. music / film downloads) | 0,067 | 25.754* |
| Online government services (e.g. tax returns, DVLA, council tax, benefits) | 0,072 | 29.616* |
| Proximity to Motivated Offender | | |
| Social networking (e.g. Facebook, Twitter) or blogging | 0,029 | 4.714** |
| E-mail, instant messaging, chat rooms | 0,072 | 29.726* |
| Browsing for news or information (e.g. BBC, Wikipedia) | 0,03 | 5.321** |
| Playing online games/doing quizzes/competitions | 0,015 | 1.240*** |

*=p ≤0.001 **=p ≤0.05 ***=p ≥0.05

Table 5.13 demonstrates the bivariate analysis result of the relationship between the frequency of Internet usage and experiencing economic cybercrime victimisation. The Chi-square test result demonstrates that there is a statistically significant relationship between the frequency of Internet usage and economic cybercrime victimisation ($\chi^2$=13.197, p<0.001). Yet, the Phi value (θ=0.048) indicates that the strength of this relationship is weak.

When we look at the percentages of usage, the figures suggest that frequent Internet users were more likely to experience the victimization. Internet users who accessed the Internet more frequently (several times a day and once a day) reported higher victimisation rates (8.1%

and 7.6% respectively). Less frequent Internet users acknowledged considerably lower victimisation percentages (4.3%).

Table 5.13

*The Relationship between Frequency of Internet Usage and Economic Cybercrime*

| *Frequency of Internet Usage* | *Contingency Table* | | *Chi-square Test* | *Phi* |
|---|---|---|---|---|
| | *Victimisation* | | | |
| | Yes | No | | |
| Several Times a Day | 8.1% | 91.9% | | |
| Once a Day | 7.6% | 92.4% | 13.197* | .048 |
| Less often than Once a Day | 4.3% | 95.7% | | |

*=p ≤0.001

This section of the chapter tested the relationship between Internet users' online lifestyles and experiencing economic cybercrime victimisation. Chi-square results give us enough evidence to reject the null hypothesis, which assumes the absence of the relationship between online lifestyle and economic cybercrime victimisation, thus, accept the alternative hypothesis stating that there is a relationship between online lifestyle and experiencing economic cybercrime victimisation. Based on these results it can be proposed that there is a statistically significant association between Internet users' online lifestyles and economic cybercrime victimisation.

#### 5.3.1.2 Absence of Capable Guardianship

Table 5.14 illustrates the bivariate analysis results for the relationship between applying online security measures and experiencing economic cybercrime victimisation. All **precautionary guardianship measures**, *only downloading known files* ($\chi^2$= 6.650, p<0.05), *deleting suspicious email without opening them* ($\chi^2$=24.373, p<0.001) and *protecting home wireless connection* ($\chi^2$= 14.204, p<0.001), which were applied to protect electronic devices security were statistically significantly associated with the victimisation. The **software-based**

**guardianship measures** like *installing security software* ($\chi^2$=25.633, p<0.001) or *scanning the computer regularly* ($\chi^2$=8.375, p<0.05), **the protection measures applied to secure online accounts** such as *using complex passwords* ($\chi^2$=5.369, p<0.05), *using different passwords for each online accounts* ($\chi^2$=6.119, p<0.05) and *adjusting website account settings* ($\chi^2$=7.809, p<0.05) emerged to be statistically significantly associated with economic cybercrime victimisation. However, these relationships appeared to be weak as the Phi values for all above-mentioned relationships were smaller than 0.1.

**The guardianship measures applied to secure personal privacy** such as *only adding known persons as friends on social networks* ($\chi^2$=2.838, p>0.05) or *being careful about putting personal information on social networking website* ($\chi^2$=3.235, p>0.05) were not statistically significantly associated with the victimisation. This result may be attributed to the fact that information provided to the social networking site may not necessarily contain financial details. Hence, economic cybercrime victims did not apply any privacy-related security measures for online networking websites.

Of the fifteen proxy variables of online guardianship, nine variables emerged to be statistically significantly associated with victimisation. Hence, it gives us enough evidence to reject the null hypothesis stating the absence of the relationship between online guardianship and economic cybercrime victimisation, thus, accept the alternative hypothesis presuming the presence of the mentioned relationship. Based on these results, it can be suggested that there is a statistically significant association between online guardianship measures and economic cybercrime victimisation.

Table 5.14

*Cross-tabulation Results for the Relationship between Guardianship Measures and Experiencing Economic Cybercrime*

| *Variable Name* | *Phi* | *Chi Square Tests* |
|---|---|---|
| *1. Guardianship Measures to Protect Electronic Devices' Security* | | |
| *1a. Precautionary Guardianship Measures to Protect Electronic Devices' Security* | | |
| Only downloaded known files or programs | 0.034 | 6.650** |
| Deleted suspicious emails without opening them | 0.066 | 24.373* |
| Protected your home wireless connection (wi-fi) with a password or been cautious using | 0.05 | 14.204* |
| *1b. Software-based Guardianship Measures to Protect Electronic Devices' Security* | | |
| Downloaded software updates and patches whenever prompted | 0.021 | 2.531*** |
| Installed anti-virus or other security software, such as a firewall | 0.067 | 25.633* |
| Scanned computer regularly for viruses or other malicious software | 0.038 | 8.375** |
| *2. Guardianship Measures to Protect Personal Data* | | |
| *2a. Guardianhip Measures to Protect Financial Information* | | |
| Only used well-known or trusted sites | 0.012 | 0.805*** |
| Checked for signs that a site is secure when buying online (closed padlock sign/https website | 0.026 | 3.941** |
| *2b. Guardianship Measures to Protect Personal Account's Security* | | |
| Used complex passwords (contain letters, numbers and symbols) | 0.031 | 5.369** |
| Used a different password for each different online account | 0.033 | 6.119** |
| Logged out of websites when you are finished | 0.005 | 0.147*** |
| Adjusted website account settings (e.g. privacy settings) | 0.037 | 7.809** |
| *2c. Guardianship Measures to Protect Personal Privacy* | | |
| Only added known persons as friends on social networks. | 0.022 | 2.838*** |
| Been careful about putting personal details on social networking sites (e.g. date of birth,place of work) / not put personal details online | 0.024 | 3.235*** |

*=p≤0.001 **=p≤0.05 ***=p≥0.05

LRAT posits that individuals' lifestyles facilitate victimisation (Cohen et al., 1981). One of the aims of this thesis was to test the applicability and explanatory power of LRAT as a theoretical framework for cybercrime victimisation. To that end, this section tested two hypotheses suggesting a relationship between LRAT's three constructs, namely proximity and exposure to the motivated offender and the absence of capable guardianship, and economic cybercrime victimisation. The results of Chi-square tests supported the proposition of the presence of a relationship between Internet users' online activities and economic cybercrime. However, all Phi values measuring the strength of the associations were weak. These weak associations suggest that there might be other factors moderating the risk of victimisation other than Internet users' online activities.

#### 5.3.1.3 Control Variables

This section of the chapter examines the relationship between the control variables, age, gender, education level and annual household income, and economic cybercrime victimisation. Past cybercrime research examined the relationship between demographic characteristics of Internet usage and the likelihood of experiencing different forms of cybercrime. Age, gender, education level and annual household income were the most frequently researched demographic characteristics. Results of previous empirical research pertaining to the correlation between the demographics of Internet users and the risk of experiencing cyber victimisation were controversial. Past research results suggest that **age** is correlated with experiencing cybercrime victimisation (Pratt et al., 2010; Ngo and Paternoster, 2011; Paek and Nalla, 2015; Choi et al., 2016; Leukfeldt and Yar, 2016) but (Bossler and Holt, 2009). **Being female** is also found to be associated with the increased risk of the victimisation (Bossler and Holt, 2009; Holt and Bossler, 2013; Choi et al., 2016); yet, Leukfeldt and Yar (2016) found no association between gender and risk of facing the victimisation. **Education level** is also found to be a statistically significant correlate of the victimisation (Pratt et al., 2010; van Wilsem, 2011, 2013a, 2013b; Paek and Nalla, 2015). **Internet users' income level** is the most controversial demographic characteristics. While some studies found that income is not associated with the victimisation (Leukfeldt, 2014; Policastro and Payne, 2014; Leukfeldt, 2015; Leukfeldt and Yar, 2016), other found a strong association between income and cyber victimisation (Reyns, 2013; van Wilsem, 2013a; Reyns et al., 2015).

Table 5.15 demonstrates the summary of the bivariate cross-tabulation results. As can be seen from the table, age ($\chi^2$=3.384, p>0.05) and gender ($\chi^2$=0.570 p>0.05) were not statistically significantly associated with victimisation. Education level ($\chi^2$=17.474, p<0.001) and income ($\chi^2$=19.964, p<0.05) were the statistically significant correlates of economic

cybercrime victimisation. It worth noting that the strength of these relationships was weak. The Phi values (θ) were 0.024, 0.010, 0.056 and 0.059 respectively.

The statistically insignificant association between age, gender and economic cybercrime victimisation is contrary to the expectations whereas the presence of age difference seemed logical when computer skills of different generations are taken into consideration. This issue will further be investigated through three-way analysis with the inclusion of the online activities as a third layer variable in the next section.

Table 5.15

*The Relationship between Demographic Characteristics of the Internet Users and Economic Cybercrime*

| *Variables* | | *Contingency Table* | | *Chi-square Test* | *Phi* |
|---|---|---|---|---|---|
| | | *Victimisation* | | | |
| | | Yes | No | | |
| Age | | | | | |
| | 16-29 | 6.6% | 93.4% | | |
| | 30-59 | 8.0% | 92.0% | 3.384*** | .024 |
| | 60+ | 6.8% | 93.2% | | |
| Gender | | | | | |
| | Male | 7.7% | 92.3% | 0.570*** | .010 |
| | Female | 7.2% | 92.8% | | |
| Education | | | | | |
| | A levels or above | 8.5% | 91.5% | | |
| | Below A-level | 6.4% | 93.6% | 17.474* | .056 |
| | No qualifications | 4.2% | 95.8% | | |
| Income | | | | | |
| | Under £10,000 | 6.2% | 93.8% | | |
| | £10,000-£19,999 | 6.4% | 93.6% | | |
| | £20,000-£29,999 | 7.0% | 93.0% | | |
| | £30,000-£39,999 | 7.3% | 92.7% | 19.964** | .059 |
| | £40,000-£49,999 | 6.7% | 93.3% | | |
| | £50,000-£69,999 | 10.6% | 89.4% | | |
| | Over £70,000 | 10.3% | 89.7% | | |

*=p ≤0.001 **=p ≤0.05 ***=p ≥0.05

### 5.3.2 Multivariate Analysis Results

This section of the chapter examines the impact of the online activities, the frequency of Internet usage and the online safeguarding measures on the risk of experiencing economic cybercrime victimisation. Binary logistic regression and three-way cross-tabulation analyses were conducted to research the effect of the aforementioned factors on the risk of facing the victimisation. Proxy variables, which emerged to be the statistically significant correlates of economic cybercrime in the previous bivariate analyses, were included in the analysis to improve the predictive power of the response variables. Enter method was selected as a proxy analysis to observe the performance of all response variables in the equation. The standard threshold, 0.05, was set to test the statistical significance of the association (Agresti, 1996). Firstly, the results of binary logistic regression will be discussed, and then the results of three-way cross-tabulation will be evaluated.

#### 5.3.2.1 Binary Logistic Regression Results

Table 5.16 displays the results for binary logistic regression analysis. As can be seen from the table, three online activities, *"buying goods or services"*, *"using online government websites"* and *"using e-mail/instant messaging/chat rooms"* appeared to be the statistically significant predictors of experiencing economic cybercrime victimisation. While holding impact of the other variables constant, Internet users who used the Internet to *buy goods or services online* were 1.4 times ($b=0.350$, $p<0.05$, Exp. (B) $=1.419$), to *use online government services* were 1.3 times ($b=0.275$, $p<0.05$, Exp. (B) $=1.316$) and to *use email/instant messaging/chatrooms* were 1.9 times ($b=0.659$, $p<0.01$, Exp. (B) $=1.934$) more likely to experience economic cybercrime victimisation than those who did not use the Internet for these purposes.

The results pertaining to buying goods or services online were in line with past cybercrime research. Leukfeldt (2015) and Leukfeldt and Yar (2016) found that online shopping increases the risk of malware infection. Similarly, Reyns (2013) found that online purchasing increased the probability of becoming a victim of identity theft by 30%. With regards to using e-mail/instant messaging/chatrooms, the past empirical research yielded mix results. While some researchers found that using chat rooms increase the risk of online harassment (Marcum et al., 2010; Marcum, 2011; Ngo and Paternoster, 2011), Bossler and Holt (2009) found no relationship between malware infection and using email/chat rooms on the risk of experiencing malware infection. However, van Wilsem (2013a) found that chat rooms increase the odds of facing diversified online victimisation.

Only installing anti-virus or other security software such a firewall emerged to be the statistically significant predictor of economic cybercrime victimisation. However, the direction of the relationship is just contrary to the expectations. This result indicates that installing security software increased the risk of victimisation by 50% ($b=0.408$, $p<0.05$, Exp. (B) =1.503). This means that software-based guardianship measures failed to protect electronic devices from virus infection and this type of guardianship increases the risk of experiencing computer virus infection. This result is in line with previous studies (Choi, 2008; Ngo and Paternoster, 2011; Holt and Bossler, 2013) yielding mixed evidence for the impact of online guardianship on the risk of experiencing cyber victimisation.

Table 5.16

*Binary Logistic Regression Analysis*

| *Variables in the Equation* | *B* | *S.E.* | *Exp(B)* |
|---|---|---|---|
| Exposure to Motivated Offender | | | |
| Online banking or managing finances (e.g. paying credit cards) | .186 | .140 | 1.204*** |
| **Buying goods or services (Internet shopping, inc. music/film downloads)** | **.350** | **.189** | **1.419**** |
| **Online government services (e.g. tax returns, DVLA, council tax, benefits)** | **.275** | **.131** | **1.316**** |
| Frequency of the Internet Usage | | | |
| Several Times a Day | .083 | .213 | 1.087*** |
| Once a Day | .237 | .229 | 1.267*** |
| Proximity to Motivated Offender | | | |
| Social networking (e.g. Facebook, Twitter) or blogging | .029 | .117 | 1.029*** |
| **E-mail, instant messaging, chat rooms** | **.659** | **.230** | **1.934**** |
| Browsing for news or information (e.g. BBC, Wikipedia) | -.130 | .156 | 0.878*** |
| Precautionary Guardianship Measures to Protect Electronic Devices' Security | | | |
| Only downloaded known files or programs | -.044 | .117 | 0.957*** |
| Deleted suspicious emails without opening them | .280 | .152 | 1.323*** |
| Protected your home wireless connection (wi-fi) with a password or been cautious using | .068 | .126 | 1.070*** |
| Software-based Guardianship Measures to Protect Electronic Devices' Security | | | |
| **Installed anti-virus or other security software, such as a firewall** | **.408** | **.145** | **1.503**** |
| Scanned computer regularly for viruses or other malicious software | -.084 | .123 | 0.919*** |
| Guardianhip Measures to Protect Financial Information | | | |
| Checked for signs that a site is secure when buying online (closed padlock sign/https website | -.201 | .122 | 0.817*** |
| Guardianship Measures to Protect Personal Account's Security | | | |
| Used complex passwords (contain letters, numbers and symbols) | -.197 | .133 | 0.821*** |
| Used a different password for each different online account | .075 | .110 | 1.077*** |
| Adjusted website account settings (e.g. privacy settings) | .101 | .126 | 1.106*** |
| **Constant** | **-4.041** | **.266** | **0.018*** |

*=p ≤0.001 **=p ≤0.05 ***=p ≥0.05

Table 5.17 displays the results of binary logistic regression analysis after the inclusion of demographic variables, annual household income and education level, into the analysis as control variables. After the inclusion of the control variables, exposure to motivated offender variables *buying goods or services* (b=0.329, p>0.05, Exp. (B) =1.390) and *using online government services* (b=0.246, p>0.05, Exp. (B) =1.279) lost their significance. Only two variables *using the Internet to access email, instant messaging, chat rooms* (b=0.628, p<0.05, Exp. (B) =1.874) and *installing anti-virus or other security software* (b=0.350, p<0.05, Exp. (B) =1.500) emerged to be statistically significant predictors of experiencing economic cybercrime victimisation. Although the inclusion of control variables did not change the effect of guardianship measure, it did change the risk of victimisation caused by using the Internet to

access e-mail, instant messaging and chat rooms. While the previous Exp (B) value was 1.934, the new Exp (B) value was 1.874 for using the Internet to access e-mail, instant messaging and chat rooms. This means that after controlling the effects of demographic variables, the risk of victimisation posed by using the Internet to access e-mail, instant messaging and chat rooms decreased by 6%. In other words, demographic characteristics, namely education level and income, increased the risk of the victimisation by 6% for those who access the Internet for e-mail, instant messaging and chat rooms.

Table 5.17

*Binary Logistic Regression Analysis*

| *Variables in the Equation* | *B* | *S.E.* | *Exp(B)* |
|---|---|---|---|
| Exposure to Motivated Offender | | | |
| Online banking or managing finances (e.g. paying credit cards) | .176 | .141 | 1.192*** |
| Buying goods or services (Internet shopping, inc. music/film downloads) | .329 | .190 | 1.390*** |
| Online government services (e.g. tax returns, DVLA, council tax, benefits) | .246 | .133 | 1.279*** |
| Frequency of the Internet Usage | | | |
| Several Times a Day | .035 | .215 | 1.036*** |
| Once a Day | .227 | .230 | 1.255*** |
| Proximity to Motivated Offender | | | |
| Social networking (e.g. Facebook, Twitter) or blogging | .057 | .119 | 1.059*** |
| **E-mail, instant messaging, chat rooms** | **.628** | **.231** | **1.874**** |
| Browsing for news or information (e.g. BBC, Wikipedia) | -.171 | .158 | 0.843*** |
| Precautionary Guardianship Measures to Protect Electronic Devices' Security | | | |
| Only downloaded known files or programs | -.064 | .118 | 0.938*** |
| Deleted suspicious emails without opening them | .263 | .153 | 1.301*** |
| Protected your home wireless connection (wi-fi) with a password or been cautious using | -.068 | .124 | 0.935*** |
| Software-based Guardianship Measures to Protect Electronic Devices' Security | | | |
| **Installed anti-virus or other security software, such as a firewall** | **.405** | **.146** | **1.500**** |
| Scanned computer regularly for viruses or other malicious software | -.068 | .124 | 0.935*** |
| Guardianhip Measures to Protect Financial Information | | | |
| Checked for signs that a site is secure when buying online (closed padlock sign/https website | -.207 | .122 | 0.813*** |
| Guardianship Measures to Protect Personal Account's Security | | | |
| Used complex passwords (contain letters, numbers and symbols) | -.209 | .133 | 0.811*** |
| Used a different password for each different online account | .078 | .111 | 1.081*** |
| Adjusted website account settings (e.g. privacy settings) | .089 | .126 | 1.093*** |
| Education | | | |
| A levels or above | .362 | .223 | 1.436*** |
| Below A-level | .253 | .231 | 1.288*** |
| No qualifications | | | |
| Income | | | |
| Under £10,000 | -.149 | .212 | 0.862*** |
| £10,000-£19,999 | -.186 | .189 | 0.830*** |
| £20,000-£29,999 | -.209 | .187 | 0.811*** |
| £30,000-£39,999 | -.243 | .194 | 0.785*** |
| £40,000-£49,999 | -.402 | .214 | 0.669*** |
| £50,000-£69,999 | .066 | .191 | 1.068*** |
| Over £70,000 | | | |
| **Constant** | **-4.017** | **.353** | **0.018*** |

*=p ≤0.001 **=p ≤0.05 ***=p ≥0.05

#### 5.3.2.2 Three-way Cross-tabulation Results

The previous bivariate cross-tabulation analyses results pertaining to the relationship between guardianship measures and economic cybercrime victimisation as well as the relationship between demographic characteristics of the Internet users and economic cybercrime victimisation indicated the need to conduct multivariate analysis to investigate issues further. Firstly, the results of the three-way cross-tabulation analysis for the relationship between guardianship measures and economic cybercrime victimisation will be discussed, and then those for the relationship between demographic characteristics of Internet users and economic cybercrime victimisation will be examined.

**Three-way Cross-tabulation Analysis Results for Guardianship**

The previous bivariate cross-tabulation analysis examining the relationship between security measures and economic cybercrime victimisation suggested that there may be a third variable that affected the relationship under examination since the Phi values of the associations indicated weak relationships. Hence, online activities were added as a third layer variable to observe the three-way relationship between the type of online activity, guardianship measure and risk of facing economic cybercrime victimisation. The basic premise of this assumption is that while some sort of online guardianship measures like using anti-virus software may be effective in preventing loss of money through hacking, it would not be a powerful tool in preventing loss of money through responding to communication (phishing). Hence, applying the type of online activity as third layer variable may elucidate some concerns aroused because of the weak association between security measures and the victimisation.

Above mentioned proposition was tested through three-way cross-tabulation analysis. While online activities (accessing the Internet for online banking, buying goods or services, social networking and e-mail, instant messaging and chat rooms) were included into the

analysis as response variables, online guardianship measures displayed in Table 5.11 were added as the outcome variables. Economic cybercrime variable was included as a third layer control variable into the analysis. Pearson Chi-square test was done to analyse the statistical significance of the relationship, and the Phi test was conducted to examine the strength of the relationship. Row percentages were also obtained to assess protection motivation of Cybercrime victims engaging with certain online activities. The outputs of the analysis for the relationship between the type of online activity and online security application within the sample of economic cybercrime victims are provided here as a sample of cross-tabulation analysis output (Table 5.18). Since a large number of output tables were obtained for each analysis, the results are summarised in Tables 5.19 and 5.20.

Tables 5.19 and 5.20 illustrate the three-way relationship between the online activities engaged and the security measures applied by economic cybercrime victims within the last 12 months. The cells that contain * sign indicate that there is no statistically significant relationship between two variables for the population of economic cybercrime victims. The results appear to indicate that victims' security intentions were mainly impacted by their online activities. As can be seen from the tables, while security patterns of the victims using the Internet for online banking and online shopping were alike, those of the victims mostly engaging with social networking were completely different from this group. Whereas economic cybercrime victims engaging with social networking mostly applied the security measures to protect personal privacy, those using the Internet mostly for financial reasons seemed to apply nearly all forms of the safeguarding measures.

Moreover, previous analysis result demonstrated that some security measures like *only adding known persons as friends on social networks* or *download software updates and patches whenever prompted* were not statistically significantly associated with cybercrime

victimisation, yet, when a third variable, online usage, was introduced into the analysis they emerged to be statistically significantly associated with victimisation for different online usage patterns.

The previous two-way analysis results showed that the relationships between economic cybercrime victimisation and applying guardianship measures were very weak; three-way analysis results demonstrate that three-way relationships were either moderate or very strong. The strongest relationship appeared to be between using the Internet for social networking and guardianship measures applied to protect personal privacy. While the Phi value was 0.546 for only adding known persons on social networking, it was 0.415 for being careful about putting personal details on social networking sites.

Another implication of these results is that it appears that the classification of guardianship measures provided by this thesis is supported. While previous research classified security measures as digital and personal, this thesis provided a more comprehensive classification: protection measures applied to safeguard devices and those to protect personal data. The results indicate that individuals are very selective when applying security measures. They appear to apply security measures that fit their needs or intended online usage.

Table 5.18

*Sample Bivariate Analysis Outputs*

**Crosstab**

| Experiencing Economic Cybercrime | | | | What typically do to keep yourself safe online: Download software updates and patches whenever prompted | | Total |
|---|---|---|---|---|---|---|
| | | | | no Download software updates and patches whenever prompted | Download software updates and patches whenever prompted | |
| No | What do you use the internet for: Online banking or managing finances | Yes | Count | 1538 | 1897 | 3435 |
| | | | % within What do you use the internet for: Online banking or managing finances | 44.8% | 55.2% | 100.0% |
| | | No | Count | 1317 | 489 | 1806 |
| | | | % within What do you use the internet for: Online banking or managing finances | 72.9% | 27.1% | 100.0% |
| | Total | | Count | 2855 | 2386 | 5241 |
| | | | % within What do you use the internet for: Online banking or managing finances | 54.5% | 45.5% | 100.0% |
| **Yes** | **What do you use the internet for: Online banking or managing finances** | **Yes** | **Count** | 148 | 179 | 327 |
| | | | **% within What do you use the internet for: Online banking or managing finances** | 45.3% | **54.7%** | 100.0% |
| | | No | Count | 66 | 31 | 97 |
| | | | % within What do you use the internet for: Online banking or managing finances | 68.0% | 32.0% | 100.0% |
| | Total | | Count | 214 | 210 | 424 |
| | | | % within What do you use the internet for: Online banking or managing finances | 50.5% | 49.5% | 100.0% |
| Total | What do you use the internet for: Online banking or managing finances | Yes | Count | 1686 | 2076 | 3762 |
| | | | % within What do you use the internet for: Online banking or managing finances | 44.8% | 55.2% | 100.0% |
| | | No | Count | 1383 | 520 | 1903 |
| | | | % within What do you use the internet for: Online banking or managing finances | 72.7% | 27.3% | 100.0% |
| | Total | | Count | 3069 | 2596 | 5665 |
| | | | % within What do you use the internet for: Online banking or managing finances | 54.2% | 45.8% | 100.0% |

**Chi-Square Tests**

| Experiencing Economic Cybercrime | | Value | df | Asymp. Sig. (2-sided) | Exact Sig. (2-sided) | Exact Sig. (1-sided) |
|---|---|---|---|---|---|---|
| No | **Pearson Chi-Square** | **378.194[c]** | **1** | **.000** | | |
| | N of Valid Cases | 5241 | | | | |
| Yes | Pearson Chi-Square | 15.531[d] | 1 | .000 | | |
| | N of Valid Cases | 424 | | | | |
| Total | Pearson Chi-Square | 395.057[a] | 1 | .000 | | |
| | N of Valid Cases | 5665 | | | | |

a. 0 cells (.0%) have expected count less than 5. The minimum expected count is 872.05.

b. Computed only for a 2x2 table

c. 0 cells (.0%) have expected count less than 5. The minimum expected count is 822.19.

d. 0 cells (.0%) have expected count less than 5. The minimum expected count is 48.04.

**Symmetric Measures**

| Experiencing Economic Cybercrime | | | Value | Approx. Sig. |
|---|---|---|---|---|
| No | Nominal by Nominal | Phi | -.269 | .000 |
| | | Cramer's V | .269 | .000 |
| | N of Valid Cases | | 5241 | |
| **Yes** | **Nominal by Nominal** | **Phi** | **-.191** | **.000** |
| | | **Cramer's V** | **.191** | **.000** |
| | N of Valid Cases | | 424 | |
| Total | Nominal by Nominal | Phi | -.264 | .000 |
| | | Cramer's V | .264 | .000 |
| | N of Valid Cases | | 5665 | |

Table 5.19

*Cross-tabulation Results for the Relationship between Guardianship Measures and Experiencing Economic Cybercrime*

| *Variable Name* | | Guardianhip Measures to Protect Financial Information | | Guardianship Measures to Protect Personal Account's Security | | | | Guardianship Measures to Protect Personal Privacy | |
|---|---|---|---|---|---|---|---|---|---|
| | | Only used well-known or trusted sites | Checked for signs that a site is secure when buying online | Used complex passwords | Used a different password for each different online account | Logged out of websites when you are finished | Adjusted website account settings | Only added known persons as friends on social networks. | Been careful about putting personal details on social networking sites |
| Online banking or managing finances (e.g. paying credit cards) | Percentage | * | 58.1% | 75.2% | 47.4% | * | 36.4% | 54.7% | * |
| | Phi Value | | 0.151 | 0.181 | 0.122 | | 0.199 | 0.096 | |
| **Buying goods or services (Internet shopping, inc. music/film downloads)** | Percentage | * | 57.2% | 72.4% | 46.2% | 65.4% | 33.9% | * | * |
| | Phi Value | | 0.192 | 0.110 | 0.125 | 0.118 | 0.160 | | |
| Social networking (e.g. Facebook, Twitter) or blogging | Percentage | * | * | 75.6% | * | * | 38.5% | 71.4% | 76.7% |
| | Phi Value | | | 0.151 | | | 0.218 | 0.546 | 0.415 |
| **E-mail, instant messaging, chat rooms** | Percentage | 64.9% | 55.4% | * | 45.9% | 65.4% | 32.8% | * | * |
| | Phi Value | 0.102 | 0.111 | | 0.142 | 0.163 | 0.126 | | |

Table 5.20

*Cross-tabulation Results for the Relationship between Guardianship Measures and Experiencing Economic Cybercrime*

| *Variable Name* | | Precautionary Guardianship Measures to Protect Electronic Devices' Security | | | Software-based Guardianship Measures to Protect Electronic Devices' Security | | |
|---|---|---|---|---|---|---|---|
| | | Only downloaded known files or programs | Deleted suspicious emails without opening them | Protected your home wireless connection (wi-fi) with a password or been cautious using | Downloaded software updates and patches whenever prompted | Installed anti-virus or other security software, such as a firewall | Scanned computer regularly for viruses or other malicious software |
| Online banking or managing finances (e.g. paying credit cards) | Percentage | 64.2% | 85% | 68.4% | 54.7% | 82% | * |
| | Phi Value | 0.153 | 0.162 | 0.131 | 0.191 | 0.102 | |
| **Buying goods or services (Internet shopping, inc. music/film downloads)** | Percentage | 62.2% | 82.9% | 67.2% | 51.4% | 80.6% | * |
| | Phi Value | 0.125 | 0.103 | 0.131 | 0.114 | 0.064 | |
| Social networking (e.g. Facebook, Twitter) or blogging | Percentage | * | * | 70.7% | * | * | * |
| | Phi Value | | | 0.166 | | | |
| **E-mail, instant messaging, chat rooms** | Percentage | 62.2% | 83.7% | 67.7% | 51.6% | 81% | * |
| | Phi Value | 0.164 | 0.217 | 0.216 | 0.168 | 0.123 | |

## Three-way Cross-tabulation Analysis for Demographic Characteristics

The relationship between demographic characteristics of the Internet users and economic cybercrime victimisation was examined in the previous section of this chapter. The results indicated that age and gender were not statistically significantly associated with victimisation. This section will examine whether the inclusion of third layer variable, online activities, will impact the aforementioned relationship.

Constructing three-way conditional association tables is an effective way of examining the relationships between two variables across strata of a third variable (Agresti, 1990; Azen and Walker, 2011). These tables are called as the conditional table since they examine the conditional associations between two categorical variables on the level of a third control variable (Andy, 2007; Azen and Walker, 2011). Two-way associations between demographic characteristics of Internet users and experiencing economic cybercrime will be examined across online financial activities. As it was expected that economic cybercrime victimisation would be associated with online financial activities, two online financial activities variables, using the Internet for online banking and buying goods or services online, were combined into one variable with the help of Syntax Editor of SPSS. This combination procedure was explained in the Methodology chapter in details. Age, gender, household income and education level were the demographics used in analyses.

All bivariate test results are summarised in one table for the ease of examination. Whereas contingency tables will be used to compare the victimisation tendencies across the strata of demographic characteristics; risk estimates (RE) will be interpreted to assess the impact of using particular online activity on the risk of experiencing victimisation. Total rows in contingency tables denote the average percentage of experiencing economic cybercrime victimisation. These rows will be used as a reference in interpreting victimisation percentages

of each conditional table. The results in contingency and the risk estimate tables will be illustrated with graphs to enhance visual examination of tables.

The marginal association table (Table 5.21) displays the result of the bivariate analysis results about the relationship between online financial activities and economic cybercrime victimisation. This table is presented here as a reference for further analyses. As can be seen from the table Internet users who accessed the Internet for online financial services reported 8.3% victimisation percentage, and it is higher than average victimisation rate with 7.5%. Risk estimate result shows that Internet users who accessed the Internet for financial activities were 2.9 times more likely to experience the victimisation than those who did not access the Internet for online financial services. This section will examine this relationship in light of the demographic characteristics of Internet users.

Table 5.21

*The Relationship between Using the Internet to Access Online Financial Activities and Experiencing Economic Cybercrime*

| | *Contingency Table* | | | | | |
|---|---|---|---|---|---|---|
| *Online Activity* | | *Victimisation* | | *Chi-square Tests* | *Phi* | *Odds Ratio* |
| | | Yes | No | | | |
| Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 8,3% | 91,7% | 28,692 | 0,071 | 2.926* |
| | No | 3,0% | 97,0% | | | |
| | Total | 7,5% | 92,5% | | | |

*=p ≤0.001

**Age:**

Firstly, inferential statistical analyses were conducted to observe the average effect of age on the relationship between using the Internet for online financial activities and experiencing economic cybercrime. Breslow-Day and Cochran's test results indicate that the relationship between online financial activity usage and experiencing crime across different levels of age can be statistically significantly summarised with a common odds ratio (Table 5.22). As Mantel-Haenszel common odds ratio indicates, after controlling for age, Internet users who accessed the Internet for online financial services were 2.8 times more likely to

experience victimisation than those who did not use the Internet for financial purposes. However, the odds ratio for this relationship in marginal association table was 2.9 (Table 5.21), this means that age has a slight but statistically significant impact on the relationship between using the Internet for online financial services and experiencing victimisation.

Table 5.22

*Three-way Cross-tabulation Table Controlling Age*

| *Tests of Homogeneity of the Odds Ratio* | | *Tests of Conditional Independence* | | *Mantel-Haenszel Common Odds Ratio Estimate* | |
|---|---|---|---|---|---|
| Breslow-Day ( $\chi 2$) | 2.795* | Cochran's ($\chi 2$) | 27.813** | Estimate | 2.885** |

*=p ≥0.05 **=p ≤0.01

Secondly, chi-square and risk estimate tests were conducted to observe the relationship for different levels of age groups (Table 5.23). All age groups who used the Internet for financial activities were statistically significantly associated with experiencing victimisation. Results in Table 5.23 were illustrated with line graphs to observe relations clearly.

As Figure 5.6, which summarises the contingency table, indicates, respondents who accessed the Internet mostly for online financial activities reported slightly higher victimisation percentages than average victimisation rates for age groups 16-29 and 30-59. However, those who were over 60 years reported considerably higher victimisation percentages than average victimisation percentages (8.2% compared to 8.5%). Those who were aged between 30-59 years reported the highest victimisation with 8.5%. The trend in Figure 5.6 appears to suggest that age category 30-59 was more vulnerable to experience the victimisation when compared to other age categories. However, when the second Figure (Figure 5.7), which demonstrates the relative risk of experiencing victimisation for online financial users, was examined it can be seen that trend was reversed for Internet users who accessed the Internet for online financial services. Although age categories 16-29 years and over 60 years reported lower victimisation percentages than age category 30-59 years, the relative risk caused by online financial service

usage was higher for these two groups. Based on these results it can be alleged that those two age groups were more vulnerable to experiencing economic cybercrime victimisation due to accessing online financial services. Although online financial users who were aged between 30-59 years reported the highest victimisation percentage with 8.2%, non-online financial users at those ages also reported the high victimisation with 2.5%. The relative risk (RE=2.063) for this age category may suggest that this age group may have faced victimisation mainly due to other factors rather than online financial usage when compared to other age categories.

Based on these results it can said be that whereas Internet users who were over 60 years old and used the Internet for online financial services were approximately 3.3 times (RE=3.322) more likely to experience victimisation than those who were over 60 years old and did not use the Internet for online financial services; Internet users who were between 30-59 years and used the Internet for online financial services were 2 times (RE=2.063) more likely to experience victimisation than those who were between 30-59 years and did not use the Internet to access online financial services.

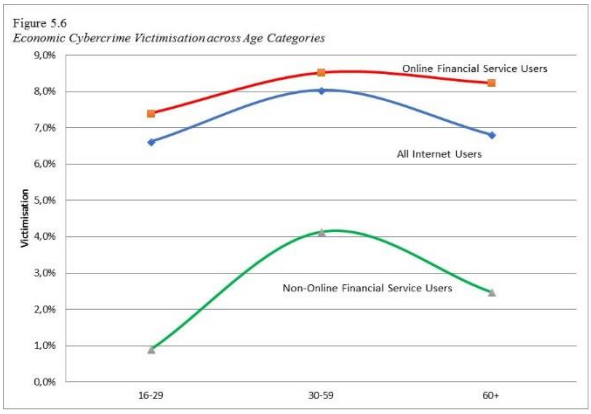
The bivariate cross-tabulation analyses results indicated the absence of the relationship between demographic characteristics, age and gender, and economic cybercrime victimisation. Yet, when online financial activities variable was included in three-way analyses, these aforementioned relationships became statistically significant. Moreover, the inferential statistical results indicated that the online financial service usage is a risk factor and different age categories face the different risk of victimisation due to online financial activity usage. The results in partial association tables appear to imply that those belonging to age categories under 30 and over 60 years old were more vulnerable to experience economic cybercrime due to online financial service usage when compared to middle age Internet users.

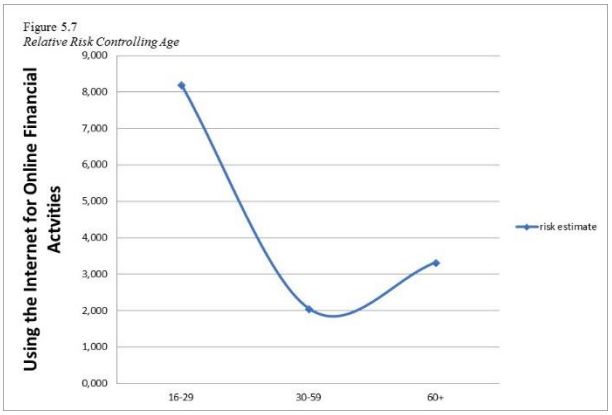
Table 5.23

*Three-way Cross-tabulation Controlling Age*

| | | *Contingency Table* | | | | | |
|---|---|---|---|---|---|---|---|
| *Age* | *Online Activity* | | *Victimisation* | | *Chi-square Tests* | *Phi* | *Relative Risk* |
| | | | Yes | No | | | |
| 16-29 | Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 7,4% | 92,6% | 6,669 | 0,084 | 8.207** |
| | | No | ,9% | 99,1% | | | |
| | | Total | 6,6% | 93,4% | | | |
| 30-59 | Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 8,5% | 91,5% | 8,417 | 0,051 | 2.063** |
| | | No | 4,1% | 95,9% | | | |
| | | Total | 8,0% | 92,0% | | | |
| 60+ | Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 8,2% | 91,8% | 14,261 | 0,099 | 3.322* |
| | | No | 2,5% | 97,5% | | | |
| | | Total | 6,8% | 93,2% | | | |

*=p ≤0.01 **=p ≤0.05




## Gender:

Inferential statistics test results of Breslow-Day and Cochran's tests in Table 5.24 demonstrate that one statistically significant common odds ratio can be produced to depict the relationship between online financial usage and experiencing economic cybercrime after controlling gender. Mantel-Haenszel common odds ratio indicates that after controlling for gender, those who used online financial services were 2.9 times more likely to use online financial services when compared to those who did not use online financial services (Table 5.24). The corresponding marginal association odds ratio for this relationship was 2.926 (Table

5.21), which means that overall gender has a very slight impact on the relationship between online financial usage and experiencing online economic crime.

Table 5.24

*Three-way Cross-tabulation Table Controlling Gender*

| *Tests of Homogeneity of the Odds Ratio* | | *Tests of Conditional Independence* | | *Mantel-Haenszel Common Odds Ratio Estimate* | |
|---|---|---|---|---|---|
| Breslow-Day ( $\chi 2$) | .696* | Cochran's ($\chi 2$) | 28.700** | Estimate | 2.927** |

*=p ≥0.05 **=p ≤0.01

Table 5.25 illustrates the results of three-way cross-tabulation for the relationship between gender of the Internet users who used the Internet for online financial activities and experiencing economic cybercrime victimisation. As can be seen in Figure 5.8, online financial users reported slightly higher victimisation percentages when compared to average victimisation percentage. Contingency table results that are illustrated in Figure 5.9 indicate that male Internet users who access the Internet for financial purposes reported slightly higher victimisation percentages when compared to female Internet users who accessed the Internet for financial purposes (8.5 % and 8%).

Yet, when the effect of using the Internet for financial purposes on the risk of victimisation was compared for each gender, the relative risk results show that female Internet users who used the Internet for online financial activities were at increased risk of victimisation when compared to male Internet users who used the Internet for financial activities. This trend can be seen more clearly in Figure 5.9. Female respondents who accessed the Internet for financial purposes were 3.5 times more likely to experience victimisation than female respondents who did not use the Internet for financial purposes. This result indicates that female Internet users were more vulnerable to experience victimisation due to online financial activity usage.

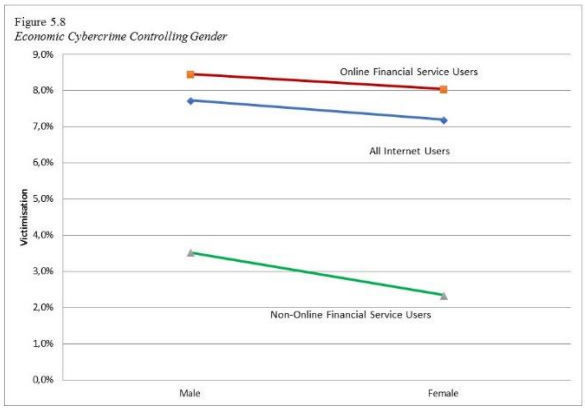
Although the previous bivariate analyses results indicated the absence of gender differences in economic cybercrime victimisation; introduction of financial activity variable as the third layer variable demonstrated that there is a gender difference for economic cybercrime victims when online financial activities are taken into consideration.

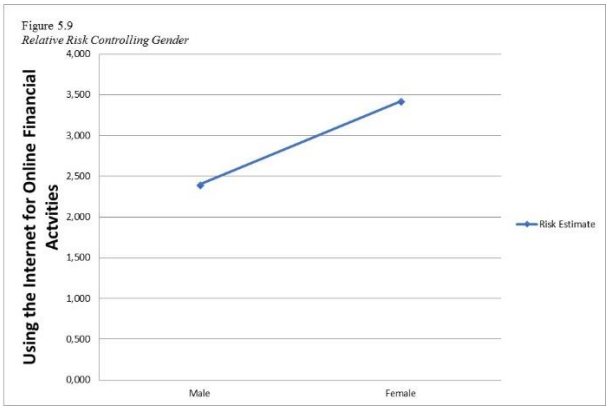
Table 5.25

*Three-way Cross-tabulation Controlling Gender*

| | | *Contingency Table* | | | | | |
|---|---|---|---|---|---|---|---|
| *Gender* | *Online Activity* | | *Victimisation* | | *Chi-square Tests* | *Phi* | *Relative Risk* |
| | | | Yes | No | | | |
| Male | Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 8,5% | 91,5% | 13,203 | 0,066 | 2.400* |
| | | No | 3,5% | 96,5% | | | |
| | | Total | 7,7% | 92,3% | | | |
| Female | Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 8,0% | 92,0% | 15,806 | 0,078 | 3.420* |
| | | No | 2,3% | 97,7% | | | |
| | | Total | 7,2% | 92,8% | | | |

*=p ≤0.01




## Education Level:

The inferential statistics test results of Breslow-Day and Cochran's tests in Table 5.26 indicate that one statistically significant common odds ratio can be produced to summarise the relationship between using the Internet for online financial activities and experiencing online economic cybercrime after controlling for Internet users' education level. Mantel-Haenszel test results indicate that after controlling for education level, those who use the Internet for online financial services were approximately 2.5 times more likely to experience economic cybercrime victimisation than those who did not use the Internet to access online financial

activities. The corresponding odds ratio for the marginal association was 2.926 (Table 5.21), which means that Internet users' educational level has a significant impact on the risk of experiencing economic cybercrime for online financial usage.

Table 5.26

*Three-way Cross-tabulation Table Controlling Educaton Level*

| *Tests of Homogeneity of the Odds Ratio* | | *Tests of Conditional Independence* | | *Mantel-Haenszel Common Odds Ratio Estimate* | |
|---|---|---|---|---|---|
| Breslow-Day ( $\chi 2$) | 3.103* | Cochran's ($\chi 2$) | 21.405** | Estimate | 2.537** |

*=p ≥0.05 **=p ≤0.01

Table 5.27 was produced to examine the relationship between using the Internet for online financial purposes and experiencing economic cybercrime for each stratum of education level. When the victimisation percentages in the contingency table are examined, it can be seen that Internet users who accessed the Internet for online financial services reported higher victimisation percentages than average victimisation percentages. This trend was more pronounced for those with no qualification (6.1% and 4.2%). Victimisation figures in contingency table appear to suggest a trend: those with higher education level reported higher victimisation percentages and these victimisation percentages decrease when education level decreases. Figure 5.10 displays this trend more clearly. Yet, it can also be observed that victimisation percentages among non-financial users were also high, which means that there might be other factors that cause higher victimisation percentages rather than online financial service usage.

When the relative risk of using online financial services was examined, it can be seen that the trend was reversed. Risk estimate test results display this trend more clearly in Figure 5.11. While the relative risk of using online financial services for those with "A Level or above" was 1.88, it was 2.537 for "Below A level" and 6.99 for "No Qualification" level. Hence,

Internet users who had no qualification and accessed the Internet for online financial services were 6.9 times more likely to experience economic cybercrime victimisation than those who had no qualification and did not use online financial activities.

Overall, education level appeared to be a significant factor for the relationship between using the Internet to access online financial services and experiencing economic cybercrime. Internet users with no qualification were more vulnerable to experience victimisation due to online financial activity usage when compared to those with qualification. On the other hand, besides low relative risk, high victimisation figures for both online financial users and non-online financial users for those with A Level or Above education level appear to suggest that there were some other factors rather than online financial service usage that caused victimisation for this education strata.

Table 5.27

*Three-way Cross-tabulation Controlling Education Level*

| | | *Contingency Table* | | | | | |
|---|---|---|---|---|---|---|---|
| *Education Level* | *Online Activity* | | *Victimisation* | | *Chi-square Tests* | *Phi* | *Relative Risk* |
| | | | Yes | No | | | |
| A Levels or Above | Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 8,9% | 91,1% | 6,090 | 0,042 | 1.888* |
| | | No | 4,7% | 95,3% | | | |
| | | Total | 8,5% | 91,5% | | | |
| Below A Level | Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 7,3% | 92,7% | 8,138 | 0,073 | 2.537* |
| | | No | 2,9% | 97,1% | | | |
| | | Total | 6,4% | 93,6% | | | |
| No Qualifications | Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 6,1% | 93,9% | 9,906 | 0,127 | 6.997* |
| | | No | ,9% | 99,1% | | | |
| | | Total | 4,2% | 95,8% | | | |

*=p ≤0.05

Figure 5.10
*Economic Cybercrime Controlling Education Level*

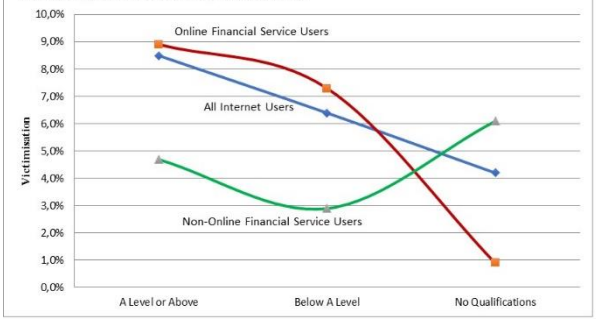



Figure 5.11
*Relative Risk Controlling Education Level*

**Household Income:**

Table 5.28

*Three-way Cross-tabulation Table Controlling Household Income*

| *Tests of Homogeneity of the Odds Ratio* | | *Tests of Conditional Independence* | | *Mantel-Haenszel Common Odds Ratio Estimate* | |
|---|---|---|---|---|---|
| Breslow-Day ( $\chi 2$) | 4.184* | Cochran's ($\chi 2$) | 23.789** | Estimate | 2.697** |

*=p ≥0.05 **=p ≤0.01

The inferential statistics test results of Breslow-Day and Cochran's tests in Table 5.28 indicate that after controlling for household income, one statistically significant common odds ratio can be produced to present the relationship between using the Internet for online financial services and experiencing economic cybercrime. Mantel-Haenszel test result implies that after controlling for household income, those who use the Internet for online financial services were 2.6 times more likely to experience online economic cybercrime than those who did not use the Internet for online financial services. The corresponding odds ratio for marginal relationship was 2.920 (Table 5.21). This result implies that household income has a significant impact on the relationship between using the Internet for online financial services and experiencing economic cybercrime.

Table 5.29 was produced to examine the above-mentioned relationship for each stratum of income level. The chi-square test results indicate that the relationship between using the Internet for online financial activities and experiencing economic cybercrime was statistically significant for three income levels, namely income levels under £30,000, which means that household income has no impact on the relationship between online financial activity usage and likelihood of experiencing economic cybercrime victimisation for other household income levels.

As the contingency table displays, those who have a household income under £30,000 reported higher victimisation percentages when compared to average victimisation

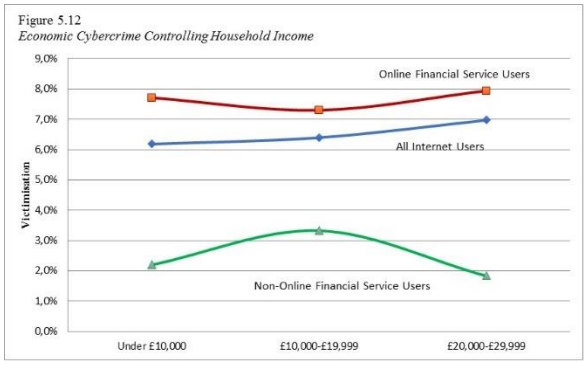
percentages. This result can be seen more clearly in Figure 5.12. Risk estimate test results, which were illustrated in Figure 5.13, indicate that those who have a household income under £10,000 and £20,000-£29,000 were more vulnerable to experiencing economic cybercrime while using online financial services. For instance, those with £20,000-£29,999 household income and used the Internet for online financial activities were 4.3 times more likely to experience economic cybercrime victimisation than those who did not use the Internet for online financial activities.

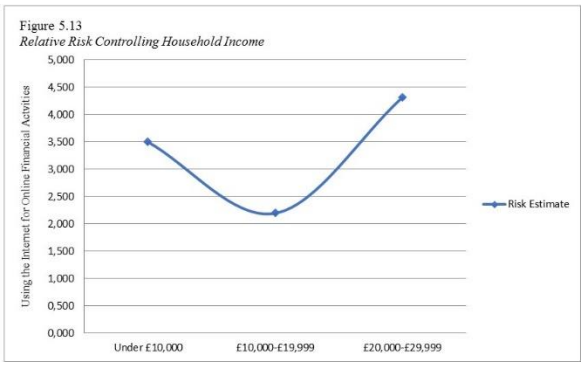
Table 5.29

*Three-way Cross-tabulation Controlling Household Income*

| | | *Contingency Table* | | | | | |
|---|---|---|---|---|---|---|---|
| *Household Income* | *Online Activity* | | *Victimisation* | | *Chi-square Tests* | *Phi* | *Risk Estimate* |
| | | | Yes | No | | | |
| Under £10,000 | Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 7,7% | 92,3% | 8,576 | 0,102 | 3.498* |
| | | No | 2,2% | 97,8% | | | |
| | | Total | 6,2% | 93,8% | | | |
| £10,000-£19,999 | Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 7,3% | 92,7% | 5,538 | 0,068 | 2.197* |
| | | No | 3,3% | 96,7% | | | |
| | | Total | 6,4% | 93,6% | | | |
| £20,000-£29,999 | Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 7,9% | 92,1% | 7,854 | 0,087 | 4.309* |
| | | No | 1,8% | 98,2% | | | |
| | | Total | 7,0% | 93,0% | | | |
| £30,000-£39,999 | Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 7,5% | 92,5% | 0,816 | 0,032 | 1.563** |
| | | No | 4,8% | 95,2% | | | |
| | | Total | 7,3% | 92,7% | | | |
| £40,000-£49,999 | Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 6,9% | 93,1% | 0,208 | 0,019 | 1.374** |
| | | No | 5,0% | 95,0% | | | |
| | | Total | 6,7% | 93,3% | | | |
| £50,000-£69,999 | Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 10,9% | 89,1% | 0,922 | 0,039 | 1.899** |
| | | No | 5,7% | 94,3% | | | |
| | | Total | 10,6% | 89,4% | | | |
| Over £70,000 | Online Financial Activities (e.g. online bankig, buying goods or services) | Yes | 10,6% | 89,4% | 2,130 | 0,059 | - |
| | | No | | 100,0% | | | |
| | | Total | 10,3% | 89,7% | | | |

*=p ≤0.05 **=p ≥0.05




This part of the chapter attempted to discover determinants of economic cybercrime victimisation through utilising constructs of Lifestyle Routine Activities Theory. The next section will look at the correlates of economic cybercrime victimisation through applying contextual vulnerabilities approach.

## 5.4 Discerning the Determinants of Economic Cybercrime through the Lenses of the Contextual Vulnerabilities Approach

The contextual vulnerabilities approach proposed by this thesis posits that although individuals' online activities or online lifestyles may have an impact on the risk of experiencing economic cybercrime victimisation, there might be other factors that may affect the chance of the victimisation. Due to the lack of relevant questions in CSEW 2014/2015, only the impact of technological vulnerabilities will be examined through statistical analysis of CSEW 2014/2015. The type of electronic device used to access the Internet was used as a proxy variable of technological vulnerabilities.

### 5.4.1 Technological Vulnerabilities

Cyberspace is a digital environment consisting of three layers, namely physical, logical and social layers and five components, geographic, logical network, physical network, persona and cyber persona components (Pamphlet, 2010). Electronic devices used to access the Internet are part of the physical network components of the physical layer. Electronic devices such as

desktop computers, laptops, tablets or smartphones are used to access the Internet. However, each of these devices bears some security risks (Ghosh and Swaminatha, 2001; Landman, 2010; A. Harris and P. Patten, 2014). This thesis asserts that the security risks caused by electronic devices may have an impact on the risk of facing economic cybercrime victimisation. Up to date, no research has examined the impact of these devices on the risk of experiencing cybercrime. Discerning the relationship between the types of electronic device used to access the Internet and the risk of experiencing different forms of economic cybercrime was the main goal of this section.

This thesis categorises the electronic devices used to access the Internet into two distinct groups, low-risk and high-risk, according to the risk they may pose on their users. Internal digital security measures and Internet connection security were two criteria used to differentiate between devices. On the one hand, internal security measures refer to digital solutions such as firewalls or anti-virus software. The latest Microsoft security intelligence report indicates that more than three-quarters of computers connected to the Internet are protected with a real-time security software (Anthe et al., 2016). Hence, electronic devices such as laptops and desktop computers used at home/work/college were hypothesised to be low-risk devices due to their relatively high-security measures compared to handheld computers or mobile phones/smartphones.

On the other hand, laptop computer used away from home/work/college, mobile phone or smartphone and handheld computers such as IPad bear some internal and external vulnerabilities. Firstly, laptop computers used away from home/work/college are vulnerable to external threats due to insecure Internet connections (Gold, 2012; Watts, 2016). People usually use these devices at airports or shopping malls where there are freely distributed Wi-Fi connections. Fraudsters usually offer free Wi-Fi connection to steal personal information of

individuals at these locations (Noor and Hassan, 2013; Straw, 2013). Mobile phone and smartphones are also vulnerable to the same sort of threats caused by free Wi-Fi usage.

Moreover, mobile application usage may be another source of threat (Jain and Shanbhag, 2012). There are many freely distributed applications for mobile phone or smartphones and handheld computers. Research results (Felt et al., 2012; Leontiadis et al., 2012) demonstrate that most of the mobile device users install these applications without careful consideration . Some freely distributed applications are also used to infiltrate mobile devices to steal information. Hence, laptop computer used away from home/work/college, mobile phone or smartphone and handheld computers are hypothesised to be high-risk devices. Table 5.30 displays categorisation of electronic devices into risk groups.

Table 5.30

*Categorisation of Electronic Devices Used to Access the Internet into Risk Groups*

| |
|---|
| *High-Risk Devices* |
| Laptop (away from home and work or school/college) |
| Mobile phone or smartphone |
| Handheld computer (e.g. iPad, tablet, palmtop) |
| Public access computers |
| *Low-Risk Devices* |
| Desktop computer (at home or work or school/college) |
| Laptop (at home or work or school/college) |

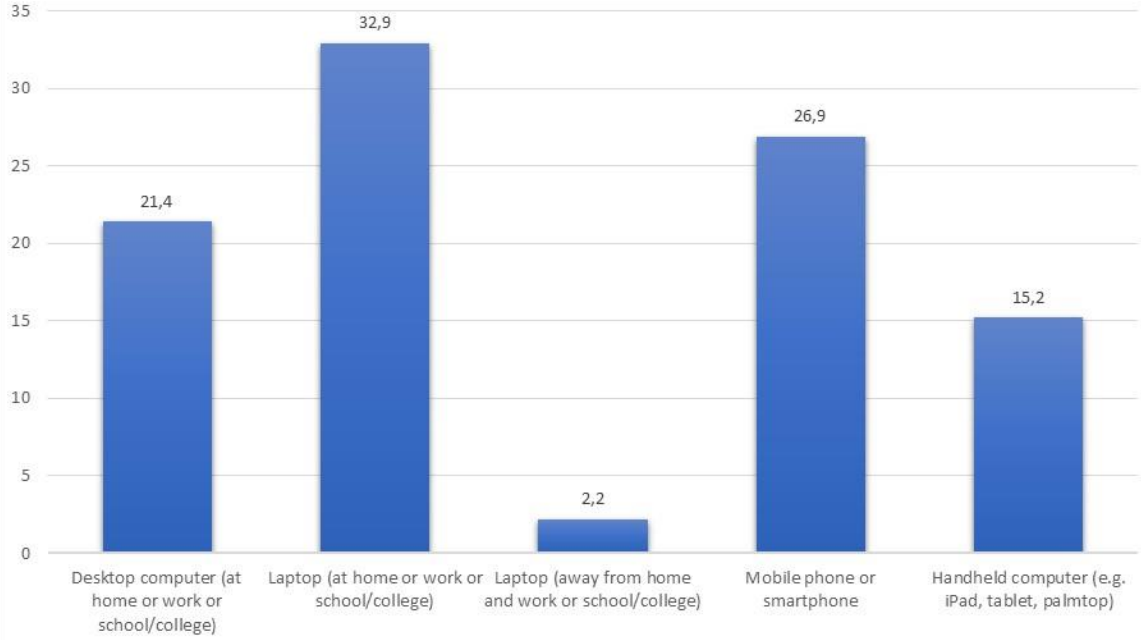
As it was discussed in somewhere else in this thesis, economic cybercrime is an umbrella term encompassing various forms of online financial crime (Levi, 2016). To distinguish the impact of electronic device usage on the risk of facing victimisation for different types of economic cybercrime; variables, card-not-present fraud, online identity fraud, online banking fraud and loss of money through virus infection, were included into analyses as the

outcome variables. The results of descriptive statistics, bivariate and three-way cross-tabulation will now be examined.

#### 5.4.1.1 Descriptive Statistics

The descriptive statistics pertaining to the usage of electronic devices utilised to access the Internet are illustrated in Figure 5.14. As can be seen from the figure, whereas *laptop used at home/work/college* (32.9%) and *mobile phone or smartphone* (26.9%) were the two most popular electronic devices used to access the Internet, *laptop used away from home/work/college* (2.2%) was the least preferred device to access the Internet. This result contradicts European Commission study on Cybercrime, which found that desktop computer was the most preferred electronic device to access the Internet in the UK in 2014 (European Commission Report, 2015).

Figure 5.14
*Frequency of Electronic Device Usage*



#### 5.4.1.2 Bivariate Analysis:

Cross-tabulation analyses were conducted to examine the relationship between the types of device used to access the Internet and four types of economic cybercrime. Relative risk and strength of association (Phi) were reported. Relative risk is the comparison of the probability of an event occurring in a group to probability of an event occurring in another group. It is obtained by dividing probability of an event happening for a group A to the probability of an event happening for a group B (Azen and Walker, 2011).

Table 5.31displays bivariate analyses results. As can be seen from the table none of the electronic devices was statistically significantly associated with *loss of money through virus infection* and *online identity theft*. This result indicates that the type of device used to access the Internet does not matter for the loss of money through virus infection and online identity theft. *Mobile phone/smartphone usage* was associated with online banking fraud victimisation. Whereas four out of five devices were statistically significantly associated with card-not-present fraud victimisation, all devices were statistically significantly associated with economic cybercrime victimisation.

Relative risk estimates of card-not-present fraud victimisation demonstrate that *mobile phone or smartphone* and *laptop used away from home/work/college* pose a higher risk than other devices. Whereas Internet users who used mobile phone or smartphone to access the Internet were approximately 69% more likely to be victim of card-not-present fraud (RR=1.685), Internet users who used *laptop away from home/work/college* were 45% more likely to experience victimisation (RR=1.442) when compared to those who did not use these devices to access the Internet.

The risk estimates of economic cybercrime illustrate *that mobile phone users* are at the increased risk of experiencing economic cybercrime. Internet users who used mobile phones

or smartphones to access the Internet were 71% more likely to face economic cybercrime victimisation (RR=1.716) when compared to those who did not use mobile phone or smartphone to access the Internet.

Bivariate analyses result in Table 5.31 demonstrated that loss of money through virus infection was not statistically significantly associated with the type of device used to access the Internet. However, it was expected that the loss of money through virus infection should be associated with three types of devices, desktop used at home/work/college, laptop used at home/work/college and laptop used away from home/work/college since these devices are more vulnerable to virus or malware infection (Symantec, 2015). Then it was proposed that the relationship might become significant with the introduction of a third variable as it is argued that a spurious relationship may become significant after inclusion of a third variable into analysis (Malhotra and Birks, 2012). Hence, a guardianship variable, *"scanning the computer regularly for viruses or other malicious software"*, was added as a layer variable. As Table 5.32 displays, after the introduction of the third variable, the relationship became significant for *"desktop used at home/work/college"* and *"laptop used at home/work/college"*. Risk estimate results indicate that Internet users who accessed the Internet via these two electronic devices and scanned their electronic devices regularly for viruses or malicious software were approximately 41% less likely to lose money through virus infection (RE= 0.595 and 0.586) respectively. This result suggests that scanning computers regularly can be an efficient safeguarding measure against loss of money through computer virus infection.

This section of the chapter looked at the role of electronic device usage on the risk of economic cybercrime victimisation. Whether age as a demographic characteristic had any impact on the relationship between the type of device usage and economic cybercrime will now be addressed.

Table 5.31

*The Relationship between Electronic Device Used to Access the Internet and and Experiencing Various Forms of Economic Cybercrime*

| *Electronic Device Used to Access the Internet* | *Loss of Money through Computer Virus Infection* | | | *Loss of Money through Identity Theft* | | | *Online Banking Fraud* | | | *Card-not-present Fraud* | | | *Economic Cybercrime* | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Chi-square Tests* | *Phi* | *Relative Risk* | *Chi-square Tests* | *Phi* | *Relative Risk* | *Chi-square Tests* | *Phi* | *Relative Risk* | *Chi-square Tests* | *Phi* | *Relative Risk* | *Chi-square Tests* | *Phi* | *Relative Risk* |
| Low Risk Devices | | | | | | | | | | | | | | | |
| Desktop computer (at home or work or school/college) | 0,284 | | 1.138*** | 0,296 | | 1.333*** | 0,002 | | 1.020*** | **5,612** | **,032** | **1.366**** | **14,223** | **,050** | **1.443*** |
| Laptop (at home or work or school/college) | 0,283 | | 0.862*** | 0,773 | | 1.436*** | 1,367 | | 1.545*** | 0,972 | | 1.158*** | **6,302** | **,033** | **1.326**** |
| High Risk Devices | | | | | | | | | | | | | | | |
| Laptop (away from home and work or school/college) | 0,11 | | 1.077*** | 1,333 | | - | 0,875 | | - | **8,089** | **,039** | **1.442*** | **16,04** | **,053** | **1.462*** |
| Mobile phone or smartphone | 0,118 | | 1.094*** | 1,023 | | 1.812*** | **4,457** | **0,072** | **3.290**** | **11,51** | **,046** | **1.685*** | **22,713** | **,063** | **1.716*** |
| Handheld computer (e.g. iPad, tablet, palmtop) | 0 | | 0.998*** | 1,431 | | 1.797*** | 2,344 | | 1.977*** | **5,759** | **,033** | **1.359**** | **15,659** | **,053** | **1.453*** |

*=p ≤0.001 **=p ≤0.05 ***=p ≥0.05

Table 5.32

*The Relationship between Electronic Devices Used to Access the Internet, Guardianship Measures and Experiencing Loss of Money Through Virus Infection*

| *Electronic Device Used to Access the Internet* | *Guardianship* | *Chi-square tests* | *Phi* | *Relative Risk* |
|---|---|---|---|---|
| Desktop Computer (at home or work or school/college | Scanned computer regularly for viruses or other malicious software | 3,778 | -0,66 | 0.595* |
| Laptop (at home or work or school/college | Scanned computer regularly for viruses or other malicious software | 4,677 | -0,66 | 0.586* |
| Laptop (away home or work or school/college | Scanned computer regularly for viruses or other malicious software | 1,724 | | 0,628 |

*=p ≤0.05 **=p ≥0.05

#### 5.4.1.3 The Impact of Age on Electronic Device Related Risk of Victimisation

Results of previous research (Kang and Yoon, 2008; Lee et al., 2011; Olson et al., 2011) demonstrate different age groups have different electronic device preference to access the Internet. Anshari et al. (2016) found that those who are under 30 years old are more likely to access the Internet via smartphones when compared to those who are over 30 years old. Similarly, research conducted by Ipsos MediaCT (2012) indicates that smartphone usage is more popular among young people in five leading economies (US, UK, Germany, France and Japan). However, no research has examined how age differences in device preferences affect the risk of becoming a victim of economic cybercrime. This section aimed to discern the relationship between age, device preferences and risk of facing economic cybercrime. Three-way cross-tabulation analyses were conducted to examine the aforementioned relationships. Chi-square, Phi and relative risk were reported. For the ease of examination, only statistically significant associations were included in the table.

Table 5.33 displays the results of three-way cross-tabulation analyses. Loss of money through virus infection was not statistically significantly associated with any type of electronic device used to access the Internet. Hence, analyses results were not included in the table. Although the relationship between online identity fraud and laptop used away from home/school/college was not statistically significant for the overall population, as can be seen from the table, the relationship was statistically significant for age category 30-59. 45% of Internet users who were between 30-59 years old and accessed the Internet via laptop used away from home/work/college reported victimisation. This was considerably higher than average which was 37.4%. The strength of the relationship was moderate ($\theta$=0.151). Risk estimate result indicates that those who were between 30-59 years and access the Internet via laptop away from home/work/college were approximately 48% more likely to be victim of

online identity theft when compared to those who were at the same age group but did not use laptop away from home/work/college (RE=1.478).

When the relationship between the type of device used to access the Internet and the risk of experiencing online banking fraud was examined across the age categories, the relationship was significant for the age group over 60 years old. Internet users who were over 60 years old and used the laptop away from home/work/college reported 55% online banking fraud victimisation when compared to 33% average victimisation for this age group. The strength of the relationship was close to strong ($\theta$=0.241). Risk estimate results indicate that those who were over 60 years old and used the laptop away from home/work/college to access the Internet were 2 times more likely to experience victimisation than those who were at the same age group but did not use the laptop away from home/work/college (RE=2.008).

The handheld computer was statistically significantly associated with online banking fraud victimisation across age group 30-59. The strength of association was moderate ($\theta$=0.126). Internet users who were between 30-59 years and used handheld computers such as tablets to access the Internet were approximately 50% more likely to experience online banking fraud victimisation when compared to those who were at the same age group but did not use handheld computers to access the Internet (RE=1.514).

With regards to card-not-present fraud, using the laptop away from home/work/college and mobile phone or smartphone to access the Internet was statistically significantly associated with victimisation for the age category 30-59 years old. The strength of both relations was weak ($\theta$=0.047 and 0.043). As relative risk results indicate, using a mobile phone or smartphone to access the Internet was riskier than using the laptop away from home/work/college. While elderly Internet users who used a mobile phone to access the Internet was 3.8 times more likely

to experience victimisation, those used laptop away from home/work/college were 1.5 times more likely to face victimisation.

Concerning economic cybercrime, most of the devices were statistically significantly associated with victimisation across age categories. The most striking result can be the relationship between mobile phone or smartphone usage and victimisation for the age group 16-29. Internet users who were between 16-29 years and used a mobile phone to access the Internet were 6.6 times more likely to experience at least one form of economic cybercrime victimisation than those who were at the same age group and did not use mobile phone or smartphone to access the Internet.

This section examined the relationship between technological vulnerabilities and risk of experiencing economic cybercrime victimisation. Type of electronic devices used to access the Internet was used as a proxy variable for technological vulnerabilities. Analyses results indicate that high-risk electronic devices, mobile phone and handheld computer, emerged as a risk factor for the economic cybercrime victimisation. Age of Internet users emerges to be a significant factor for the relationship between the type of device used to access the Internet and economic cybercrime. The impact of technological and other contextual vulnerabilities will further be examined through qualitative analysis of semi-structured interviews in the next chapters.

Table 5.33

*The Relationship between Using the Internet to Access Online Banking or Managing Services and Experiencing Online Banking Fraud after Controlling Most Frequently Used Device to Access the Internet*

| | | *Contingency Table* | | | | | |
|---|---|---|---|---|---|---|---|
| *Age Group* | *Device Used to Access the Internet* | | *Victimisation* | | *Chi-square* | *Phi* | *Relative Risk* |
| Identity Fraud | | | Yes | No | | | |
| 30-59 | Laptop, away from home and work or school/college | Yes | 45,2% | 54,8% | 4,134 | ,151 | 1,478 |
| | | No | 30,6% | 69,4% | | | |
| | | Total | 37,4% | 62,6% | | | |
| Online Banking Fraud | | | | | | | |
| 60+ | Laptop, away from home and work or school/college | Yes | 55,0% | 45,0% | 5,383 | ,241 | 2,008 |
| | | No | 27,4% | 72,6% | | | |
| | | Total | 33,3% | 66,7% | | | |
| 30-59 | Handheld computer | Yes | 35,3% | 64,7% | 3,798 | ,126 | 1,514 |
| | | No | 23,3% | 76,7% | | | |
| | | Total | 30,8% | 69,2% | | | |
| Card-not-present Fraud | | | | | | | |
| 30-59 | Laptop, away from home and work or school/college | Yes | 6,0% | 94,0% | 7,037 | ,047 | 1,533 |
| | | No | 3,9% | 96,1% | | | |
| | | Total | 4,7% | 95,3% | | | |
| 30-59 | Mobile phone or Smartphone | Yes | 5,1% | 94,9% | 5,828 | ,043 | 3,823 |
| | | No | 2,9% | 97,1% | | | |
| | | Total | 4,7% | 95,3% | | | |
| Economic Cybercrime | | | | | | | |
| 16-29 | Desktop computer (at home or work or school/college) | Yes | 8,4% | 91,6% | 5,636 | ,078 | 1,847 |
| | | No | 4,6% | 95,4% | | | |
| | | Total | 6,6% | 93,4% | | | |
| 30-59 | Desktop computer (at home or work or school/college) | Yes | 9,0% | 91,0% | 6,599 | ,045 | 1,382 |
| | | No | 6,5% | 93,5% | | | |
| | | Total | 8,0% | 92,0% | | | |
| 30-59 | Laptop, away from home and work or school/college | Yes | 10,1% | 89,9% | 10,13 | ,056 | 1,458 |
| | | No | 6,9% | 93,1% | | | |
| | | Total | 8,0% | 92,0% | | | |
| 60+ | Laptop, away from home and work or school/college | Yes | 9,7% | 90,3% | 3,947 | ,052 | 1,561 |
| | | No | 6,2% | 93,8% | | | |
| | | Total | 6,8% | 93,2% | | | |
| 16-29 | Mobile phone or Smartphone | Yes | 7,2% | 92,8% | 5,057 | ,074 | 6,649 |
| | | No | 1,1% | 98,9% | | | |
| | | Total | 6,6% | 93,4% | | | |
| 30-59 | Mobile phone or Smartphone | Yes | 8,9% | 91,1% | 11,197 | ,059 | 1,754 |
| | | No | 5,1% | 94,9% | | | |
| | | Total | 8,0% | 92,0% | | | |
| 60+ | Mobile phone or Smartphone | Yes | 9,5% | 90,5% | 9,031 | ,078 | 1,773 |
| | | No | 5,4% | 94,6% | | | |
| | | Total | 6,8% | 93,2% | | | |
| 30-59 | Handheld computer | Yes | 8,9% | 91,1% | 8,514 | ,095 | 2,159 |
| | | No | 4,1% | 95,9% | | | |
| | | Total | 6,6% | 93,4% | | | |
| 30-59 | Handheld computer | Yes | 9,0% | 91,0% | 5,172 | ,040 | 1,317 |
| | | No | 6,9% | 93,1% | | | |
| | | Total | 8,0% | 92,0% | | | |

## 5.5 Fear of Cybercrime

Fear of crime is a negative emotional reaction to present or anticipated danger or threat (Ferraro, 1995; Henson and Reyns, 2015). It is argued that negative life events such as victimisation experiences may have adverse impacts on victims' psychological well-being and social lives (Yin, 1980; Skogan, 1986). This thesis aims to explore the extent of fear of economic cybercrime and its behavioural adaptations and security intention. This issue will be examined through a statistical analysis of CSEW 2014/2015 and semi-structured interviews conducted with the victim and non-victim control group participants. Firstly, descriptive statistics pertaining to identity theft, credit card fraud and cybercrime in the UK will be presented and then bivariate and multivariate analyses result about the gender and age differences in fear of cybercrime will be displayed.

Table 5.34 illustrates descriptive statistics about the extent of fear of cybercrime, credit card fraud and Identity Fraud. As can be seen, fear of identity fraud (65,7%) is significantly more prevalent than fear of credit card fraud (49,9%) and fear of cybercrime (43,3%). Since identity fraud and credit card fraud are types of economic cybercrime, it may be suggested that fear of economic cybercrime is more prevalent than fear of cybercrime among Internet users.

Table 5.34
*Fear of Crime*

| | *Frequency* | *Percent* | *Frequency* | *Percent* | *Frequency* | *Percent* |
|---|---|---|---|---|---|---|
| | Cybercrime | | Credit Card Fraud | | Identity Fraud | |
| Very worried | 538 | 9,7 | 745 | 13,7 | 1335 | 23,6 |
| Fairly worried | 1924 | 34,6 | 1975 | 36,2 | 2384 | 42,1 |
| Not very worried | 3099 | 55,7 | 2247 | 41,2 | 1540 | 27,2 |
| Not at all worried | | | 485 | 8,9 | 386 | 6,8 |
| Not Applicable | | | | | 14 | ,2 |
| Total | 5561 | 100,0 | 5452 | 100,0 | 5659 | 100,0 |

### 5.5.1 Gender Differences in Fear of Cybercrime

Fear of traditional crime studies suggested that fear of crime is more prevalent among females than males (Schafer et al., 2006; Jennings et al., 2007; May et al., 2010; Gutt and Randa, 2016). Fear of cybercrime studies yielded mixed results about gender differences in cybercrime. The results of fear of online interpersonal crime research (i.e. online harassment or cyberbullying) indicated that female Internet users reported higher levels of fear when compared to males (Henson et al., 2013; Pereira et al., 2016; Virtanen, 2017). However, the results of Roberts et al. (2013) who researched fear of online identity theft and those of Yu (2014) who examined fear of cybercrime among college students found no gender differences in fear of cybercrime. Table 5.35 illustrates bivariate cross-tabulation results about the relationship between gender and fear of cybercrime. As can be seen, the figures illustrating the percentages of worries among females and females are very close. Moreover, p-value representing Chi-square tests, which examine the presence of a relationship between variables, is bigger than the significance threshold. This result illustrates the absence of a statistically significant association between gender and fear of cybercrime. In other words, there is no gender difference in fear of cybercrime.

Table 5.35

*Gender Difference in Fear of Cybercrime*

| | *Contingency Table* | | | | *Chi-square Tests* |
|---|---|---|---|---|---|
| *Online Activity* | | *Worry* | | | |
| | | Not Worried | Fairly Worried | Very Worried | |
| Gender | Male | 55,7% | 34,9% | 9,4% | *0.679** |
| | Female | 55,8% | 34,2% | 10,0% | |
| | Total | 55,7% | 34,6% | 9,7% | |

*=p ≥0.05

A multivariate analysis was conducted with the introduction of the third layer variable, economic cybercrime victimisation, to observe the impacts of previous economic cybercrime victimisation on the gender difference in fear of cybercrime (Table 5.36). P-values of Chi-square tests, which are smaller than 0,001, demonstrate a statistically significant association between gender, previous cybercrime victimisation and fear of cybercrime. These results suggest that there is a gender difference among Internet users who experienced economic cybercrime victimisation for fear of cybercrime. As can be seen, males are more fearful than females (21,6% and 17,3% respectively). These results are interesting since female Internet users who did not experience economic cybercrime victimisation reported higher levels of worry when compared to males who did not face economic cybercrime. These results are of significant importance; firstly, contrary to previous fear of crime studies, these results indicate that males are more fearful of cybercrime when compared to females due to direct victimisation experiences. Indirect victimisation experience, which refers to an image of cybercrime shaped by media representation of crime or stories heard from other individuals (Silverman and Kennedy, 1985), may be an explanation for the higher levels of concern among females who did not have a prior economic cybercrime experience.

Table 5.36

*Impact of Previous Economic Cybercrime Victimisation on Gender Differences in Fear of Cybercrime*

| | | *Contingency Table* | | | | *Chi-square Tests* |
|---|---|---|---|---|---|---|
| *Gender* | *Previous Experience* | | *Worried* | | | |
| | | | Not Worried | Fairly Worried | Very Worried | |
| Male | Economic Cybercrime | Yes | 33,1% | 45,3% | 21,6% | 72,046* |
| | | No | 57,6% | 34,0% | 8,4% | |
| | | Total | 55,7% | 34,9% | 9,4% | |
| Female | Economic Cybercrime | Yes | 40,5% | 42,2% | 17,3% | 22,638* |
| | | No | 57,0% | 33,6% | 9,4% | |
| | | Total | 55,8% | 34,2% | 10,0% | |

*=p ≤0.001

### 5.5.2 Age Differences in Fear of Cybercrime

Age is another demographic characteristic that proposed to be influencing the presence and the extent of the fear of crime. Empirical results of traditional fear of crime indicates that older citizens are more fearful than younger generations (Ortega and Myles, 1987; Covington and Taylor, 1991; Moore and Shepherd, 2006; Boateng, 2016). However, past cybercrime studies researching age differences yielded no statistically significant relationship between age and fear of cybercrime (Henson et al., 2013; Roberts et al., 2013; Yu, 2014). Bivariate analysis results presented in Table 5.37 suggest a statistically significant association between age categories and fear of crime. These results indicate that older Internet users are more fearful of experiencing cybercrime victimisation. This result is in line with the traditional fear of crime studies researching fear of crime resulted from physical world interactions. But, contradicts previous cybercrime victimisation studies.

Table 5.37

*Age Differences in Fear of Cybercrime*

| *Online Activity* | *Contingency Table* | | | | *Chi-square Tests* |
|---|---|---|---|---|---|
| | | *Worry* | | | |
| | | Not Worried | Fairly Worried | Very Worried | |
| Age Categories | 16-29 | 70,0% | 23,7% | 6,3% | *92,676** |
| | 30-59 | 53,0% | 36,9% | 10,2% | |
| | 60+ | 52,7% | 36,6% | 10,8% | |
| | Total | 55,7% | 34,6% | 9,7% | |

*=p ≤0.001

The impacts of previous cybercrime victimisation on fear of crime across age categories were examined through multivariate analyses with the introduction of economic cybercrime victimisation as the third layer variable (Table 5.38). Chi-square test results indicate a statistically significant relationship between variables. The results suggest that middle-aged Internet users who experienced economic cybercrime victimisation were more fearful than

other age groups. While 34,9% of middle-aged participants reported no worry, 65,1% of them acknowledged a degree of worry. If we are to compare the intensity of fear of cybercrime victimisation due to prior economic cybercrime victimisation, it seems that it is more pronounced among young Internet users. Whereas 19,4% of young Internet users who experienced economic cybercrime were very worried to be a victim of cybercrime, only 5,4% of non-victim participants were very worried to be a victim of cybercrime.

Table 5.38

*Impact of Previous Economic Cybercrime Victimisation on Age Differences in Fear of Cybercrime*

| | | *Contingency Table* | | | | *Chi-square Tests* |
|---|---|---|---|---|---|---|
| *Gender* | *Previous Experience* | | *Worried* | | | |
| | | | Not Worried | Fairly Worried | Very Worried | |
| 16-29 | Economic Cybercrime | Yes | 48,4% | 32,3% | 19,4% | 24,236* |
| | | No | 71,5% | 23,0% | 5,4% | |
| | | Total | 70,0% | 23,7% | 6,3% | |
| 30-59 | Economic Cybercrime | Yes | 34,9% | 42,9% | 22,2% | 61,001* |
| | | No | 54,5% | 36,4% | 9,1% | |
| | | Total | 53,0% | 36,9% | 10,2% | |
| 60+ | Economic Cybercrime | Yes | 32,7% | 54,1% | 13,3% | 17,423* |
| | | No | 54,1% | 35,3% | 10,6% | |
| | | Total | 52,7% | 36,6% | 10,8% | |

*=p ≤0.001

## 5.6 Summary

This first empirical chapter presented the results of the first phase of the research process, the quantitative analysis of Crime Survey for England and Wales (CSEW) 2014/2015. The first phase of the research had two goals: testing the applicability of LRAT to economic cybercrime and providing a starting point for the qualitative phase of the research. To these ends, initially, the applicability of LRAT to economic cybercrime victimisation was tested through the statistical analysis of CSEW 2014/2015. The analyses result testing two hypotheses illustrated statistically significant associations between LRAT constructs and economic

cybercrime victimisation. These results suggested that LRAT elements can be applied to economic cybercrime research as a conceptual framework. However, Phi-values of tests indicated that the relationships between LRAT constructs and economic cybercrime victimisation were weak. These weak associations can be interpreted as the presence of other factors, other than Internet users' online activities, affecting the likelihood of becoming a victim of economic cybercrime. These results indicate that the explanatory power of LRAT as a theoretical framework to discern the causes of economic cybercrime needs further examination.

Discerning the online lifestyle correlates of economic cybercrime victimisation was another goal of this phase. Binary logistic regression analysis results suggested "buying goods or services", "using online government websites" and "using e-mail/instant messaging/chat rooms" as risk factors for economic cybercrime victimisation. Online safeguarding measure installing anti-virus or other security software also emerged as a risk increasing factor. Moreover, three-way multivariate analysis results indicated a relationship between demographic characteristics of Internet users and the risk of victimisation. Age, gender, education level and annual household income were associated with victimisation.

The third section of the chapter presented the results pertaining to the relationship between the type of electronic device utilised to access the Internet and the risk of victimisation. The analyses results suggested some electronic devices as a risk factor for victimisation. The analysis results demonstrated in the last section of the chapter, which examined the extent of fear of cybercrime, suggested age and gender differences in fear of economic cybercrime victimisation.

The qualitative second phase of the research aimed to understand and extend these mentioned results. The following three qualitative findings chapters present the outcomes of the second phase of this doctoral research.

## 6.1 Introduction

The previous chapter aimed to find out the online lifestyle correlates of economic cybercrime as well as to test the applicability of Lifestyle Routine Activities Theory (LRAT) to economic cybercrime victimisation through quantitative analysis of the Crime Survey for England and Wales 2014/2015. Quantitative analysis results indicated that Internet users' online activities, for example using online government websites, shopping online and online banking increased the likelihood of facing economic cybercrime victimisation. This chapter and the following three chapters will present and discuss the findings of qualitative data analysis pertaining to causes of economic cybercrime victimisation.

This chapter addresses the first research question*: "What are the factors which render Internet users susceptible to be the target of an online attack?"* This chapter investigates whether online behaviours, both normal and deviant, were associated with the risk of being a target of economic cybercrime.

A recent Eurostat report, which is based on the 2017 Community Survey on ICT[10]results, demonstrates that 95% of the UK population accessed the Internet and 87% of UK Internet users made online purchases in 2016 (Eurostat, 2016). While some of those Internet users became the target of online fraudsters, others used the Internet without facing any threat. The discriminating factors between these two groups of the Internet users are at the

[10] Community Survey on Information and Communication Technologies (ICT) is conducted by Eurostat annually since 2002. The survey collects data about the Internet usage, e-government and electronic skills. Data is collected from individuals aged 16 to 74 years and households in member countries. For more information please see: https://ec.europa.eu/eurostat/statistics-explained/index.php/Main_Page

heart of our understanding of economic cybercrime victimisation since being a target of an online attack is the necessary condition for being a victim of economic cybercrime. Past research (Holtfreter et al., 2008; Pratt et al., 2010; Policastro and Payne, 2014) attempted to address the issue of being targeted by fraudsters online. Although these studies researching telemarketing or consumer fraud targeting yielded conflicting results, they provided good insight into our understanding of being targeted online. Online shopping and frequent use of the Internet were found to be associated with an increased risk of fraud targeting (Holtfreter et al., 2008; Pratt et al., 2010). The results of Policastro and Payne (2014) suggested that neither age nor online routine activities were associated with the risk of being targeted.

Both victim and control group participants were asked whether they had been a target of an email phishing attack or they had experienced email phishing victimisation in the last twelve months to explore the factors that facilitate being a target of an online attack. While six participants experienced economic cybercrime victimisation due to email phishing, ten victims and four control group participants acknowledged being the target of an email phishing attack. Those participants who successfully thwarted phishing attacks were considered as the control group for this particular analysis. Interviews with control group participants were utilised to understand the impacts of online lifestyle differences on the likelihood of experiencing economic cybercrime victimisation through the comparative analysis of online lifestyles of the victim and non-victim participants.

A crime script analysis method was utilised to frame the analysis of the data including semi-structured interviews and police reports related to economic cybercrime incidents which occurred in the North-East of the UK in 2015. It is argued that crime is a multistage event that is comprised of various situation-based sequences of decisions and actions (Haelterman, 2016). Crime scripts analysis, which perceives crime as a process rather than a single event, is applied

to examine each step of a crime to get a better sense of actions taken at each step (Cornish, 1994). This examination enables researchers to distinguish points of intervention (Hutchings and Holt, 2015) and predict individuals' behaviours (Chiu et al., 2011). One of the advantages of crime script analysis is that it provides a template for the systematic analysis of any crime (LeClerc and Wortley, 2013). Herman-Stabl et al. (1995) proposed a three-stage examination of crime events. The first phase, precursors, refers to both socially accepted lawful behaviours and contextual factors that congregate victims and offenders (Herman-Stabl et al., 1995). Following this line of logic, this chapter presents precursor events of becoming a victim of economic cybercrime. While the first part of this chapter deals with the determinants of being a target of phishing attacks, the second part looks at the antecedents of being a victim of a hacking attack. Respondents' comments are provided as verbatim quotations while presenting the findings for the purpose of reflecting participants' voices and illustrating evidence for the interpretation of data (Corden and Sainsbury, 2006). As it was described in the Methodology Chapter (4$^{th}$ Chapter), participants' names are anonymised to protect interviewees' identity.

## 6.2 The Determinants of being a Phishing Attack Target

The constructs of Protection Motivation Theory (PMT) (Rogers, 1975) were utilised to assess the Internet users' information disclosure decisions. Rogers (1975) proposed PMT to account for individuals' reactions to fear appeals, later Rogers (1983) and Prentice-Dunn and Rogers (1986) extended this theory to examine people's reactions to inter-personal communication (Floyd et al., 2000; Norman et al., 2005). Although this theory was initially utilised as a theoretical framework in health studies, it has been increasingly used in Internet security studies (Anderson and Agarwal, 2010; Ifinedo, 2012; Lowry et al., 2017).

Perceived severity, perceived vulnerability, self-efficacy and calculus of behaviour are the main elements of PMT (Floyd et al., 2000; Norman et al., 2005; Chenoweth et al., 2009).

In a cyber context, perceived severity refers to individuals' perception about the seriousness of the consequences when engaged with the online activity (Lwin et al., 2012; Mohamed and Ahmad, 2012; Chen and Zahedi, 2016). For instance, the decision of downloading a file or a movie from unreliable sources for free depends on the Internet users' perceived severity of consequences stemming from the illegal downloading. While Internet users who perceive the risk of illegal downloading as low may continue the action, those who perceive it as a high-risk activity may stop at the point of confirming the download. Perceived vulnerability denotes Internet users' perception of the likelihood of facing a negative experience as a consequence of their online actions (Piko, 2001). Self-efficacy refers to Internet users' self-assessment related to their knowledge and capabilities to engage with online activities and overcome threats faced (Eastin and LaRose, 2000; Hsu and Chiu, 2004; Tsai et al., 2016) . It is expected that Internet users with high self-efficacy would be more relaxed about disclosing personal information as they are knowledgeable about adjusting the privacy settings of social networks (H. Akhter, 2014; Chen and Chen, 2015). Calculus of behaviour refers to weighing the cost and benefit of engaging with online activity (Krasnova and Veltri, 2011; Fife and Orjuela, 2012). It is argued that risk-benefit analysis affects the decision of yielding personal information online (Xu et al., 2011; Morton, 2014; Lee et al., 2015).

Voluntary and involuntary personal information disclosure emerged as two broad themes of personal information disclosure. Firstly, the findings pertaining to voluntary personal information will be discussed, and then those related to involuntary personal information disclosure will be considered.

### 6.2.1 Voluntary Personal Information Disclosure

Interviews suggest that Internet users provided their personal identifying information to many platforms with consent. Social networking sites (SNS), online advertising websites and free Wi-Fi providers appeared to the most common platforms where respondents revealed their personal information.

**Social Networking Sites (SNS)**

Social media, which has become an integral part of our lives, increasingly occupies big space in our daily routines (Lin and Lu, 2011; Noguti et al., 2018; Shi et al., 2018). SNS can be used for various reasons ranging from social ones such as entertainment (Wang et al., 2015; Park et al., 2018), socialising (Afseer, 2017; Power et al., 2018), self-presentation (Ong et al., 2011; Nadkarni and Hofmann, 2012; Seidman, 2013a), opinion sharing (Livingstone, 2008; Jansen et al., 2011) to financial ones like establishing connections with colleagues (Ramirez Jr and Bryant, 2014; Grabher and König, 2017), finding jobs or creating profiles for employees (Carmack and Heiss, 2018; Evuleocha and Ugbah, 2018; Mehdi, 2018). Yet, this kind of multifaceted application of the Internet is not free from its problems. Literature suggests that these platforms have also become an essential source of information scraping (Oxley, 2011; Algarni et al., 2017). 13 out of 16 participants who were target of a phishing attempt acknowledged sharing personal identifying information such as email addresses. Two quotes are provided to illustrate social platforms that participants shared their personal information. Findings of this thesis indicate that personal information like email addresses posted on SNS increased the risk of being the target of a phishing attack. It appears that online perpetrators gather personal information through social media platforms and SNS to conduct financially motivated phishing attacks. This finding suggesting SNS as the potential source of information for fraudsters is in line with those of (Alwagait et al., 2015; de Jesus et al., 2018).

*"I didn't post anything, but my email address can be found online since I posted it on education websites such as LinkedIn or ResearchGate."* (Sophie, 32 years old female victim).

*"Probably I received phishing emails due to social media. I suppose Facebook is a very powerful thing. You sometimes click on an add. They ask your email address on shopping websites for a newsletter. ...I received some tax-related emails after posting adds. But I am quite visible. My details can be seen through LinkedIn."* (Mia, 29 years old female victim).

Although new online communication methods are introduced, email usage is still prevalent due to its convenience to establish communication with others (Narang et al., 2017). Most of the online platforms require email input for the registration, which makes yielding email address a routine thing that we do without really pondering about it. Increased visibility is the downside of yielding the email addresses to third parties, which appears to increase the risk of being targeted. The news about LinkedIn phishing attacks appears to support this finding (Cucu, 2017; Weise, 2017). As the content of the news indicates, LinkedIn users received phishing emails asking for their CVs. The information obtained through these CVs may be used to conduct more sophisticated spear-phishing attacks. Creating new email addresses that do not contain any personal information like name and surname would be a solution to this kind of threat. Those email addresses would be provided to less important platforms while the real email addresses may be used in essential communications.

**Selling Goods Online**

Selling second-hand goods online has gained popularity with the establishment of online auction sites like eBay or advertising websites like Gumtree (Nieminen, 2016; Sihvonen and Turunen, 2016). Internet users either sell unwanted items or buy desired second hand or new products for compatible prices via these platforms. According to eBay stats, the site has reached more than 179 million active users in the first quarter of 2018 (Statista, 2018).

Interviews with victims suggest that selling goods online was a risk factor for being targeted online. 7 phishing victims and 4 control group participants reported posting personal information on advertisement websites. 2 victims' and 1 control group participants' accounts are provided to illustrate the type of information participants shared online. It appears that fraudsters monitor auction websites to gain information about Internet users since sellers submit their personal identifying information like email addresses and mobile phone numbers to these websites. Although participants' accounts indicated that they perceived such information as insignificant, online perpetrators gather apparently trivial information from these sources in order to conduct spear phishing attacks (Iovan and Dinu, 2014; Poulter, 2017). This finding is backed up with the official announcement of Gumtree, which warned their users to be aware of phishing attacks since fraudsters acquired their users' email addresses (Duxbury, 2016; Staymartonline, 2016). The results of the study conducted by Williams (2015) who has also found that online auction website usage increased the risk of facing online identity theft victimisation also confirms this finding.

*"I posted an ad to sell my previous car. I posted an ad on Gumtree. I posted my cell phone number and email address"* (Harrison, 32 years old male victim).

*"I used eBay and Gumtree to sell items. I try to include very little information such as my mobile phone number and email address."* (Jessie, 35 years old female victim).

However, it should be noted that posting personal information to sell something online does not necessarily lead to victimisation. Some control group participants also posted advertisements to sell something online, but they have not faced victimisation. Posting advertisements online should be considered just as one factor that boosts the visibility of Internet users' personal information. Whether their information will be used to target them depends on the fraudsters' tactics.

*"I use Freecycle and sometimes rarely Gumtree. … Just email address and telephone number, nothing else"* (Mikey, 34 years old male, control group).

## Disclosing Personal Information to Access Free Wi-Fi

The widespread use of the Internet in our daily routines appear to stimulate Internet users' desire to access the Internet anywhere at any time. This desire of connectivity has motivated many public places such as shopping malls, hotels, restaurants or cafés offer free Wi-Fi to attract more consumers or enable them to spend more time away from home (Bulchand-Gidumal et al., 2011; Lambert et al., 2018). Omnipresent connectivity appears to cast a threat for the privacy of Internet users. It is argued that fraudsters increasingly set up their own Wi-Fi hotspots mimicking the real ones at public places (Latha and Vasantha, 2015; Dahiya and Gill, 2017; O'Donnell, 2017) to access Internet users' personal and financial information.

Interviews indicated that both victim and control group participants accessed free Wi-Fi several times a day. 23 participants acknowledged accessing free Wi-Fi. 12 of these participants were targeted by a phishing attempt. 3 participants' accounts are presented as an example of participants' perceptions about the information they provided to be eligible for free Wi-Fi. It seems that most participants did not perceive a significant threat stemming from sharing personal information to register for free Wi-Fi. This can be attributed to the relative insignificance of personal information provided, as most people are more vigilant about personal financial information (Bryce and Fraser, 2014). A trade-off between the risk of losing personal information and benefits of free Wi-Fi may be another explanation for yielding personal information to network providers (Workman, 2007).

*"I sometimes use free Wi-Fi in an airport or in café. I think they do not ask for very important personal information, so I am not very worried about providing them"* (Tilly, 28 years old female victim).

*"I used several types of free or public Wi-fi such as those offered in café' or airport. Actually, I do not pay attention to the type of information they asked me to sign in. I just type what they ask."* (Harrison, 32 years old male victim).

*"I do understand that they may misuse it, but the worst-case scenario is that they may sell my email address."* (Kyle, 30 years old, control group).

These findings suggest that rewards or benefits decreased the perceived vulnerability of joining to an unknown network. Although most participants were aware that joining to insecure networks may result in personal information loss, they preferred accessing free Wi-Fi. Similarly, privacy calculus, denoting individuals' assessment about the benefits and consequences of sharing personal information (Culnan and Armstrong, 1999), alleviated the perceived severity of sharing personal information to unknown Internet providers. Findings appear to support the proposition that rogue Wi-Fi hotspots facilitate data collection for identity theft or social engineering attacks (Sood and Enbody, 2013; Brenza et al., 2015; Fang et al., 2016).

This section of the chapter introduced the findings related to the effect of voluntary personal information disclosure on the risk of being targeted online. It appears that disclosing personal information to SNS, advertising websites and free Wi-Fi providers significantly run the risk of being targeted online. The decision of personal information disclosure seems to be affected by Internet users' privacy calculus, which in turn decreased perceived severity and perceived vulnerability of personal information sharing. Anticipated benefits and privacy concerns are two important constructs of privacy calculus (Dinev and Hart, 2006; Krasnova et

al., 2012). It appears that interviewees' anticipated benefits outweighed privacy concerns. Findings of this research indicate that financial gain through selling goods online, accessing free Internet and rewards of participating in social networking sites emerged to be anticipated benefits of personal information disclosure. When it comes to privacy concerns, it appears that respondents did not perceive sharing information such as e-mail address or mobile phone number as threats to their personal information privacy. In other words, they did not put too much value on such information. The next section will look at how involuntary personal information disclosure effect the chance of being an online attack.

### 6.2.2 Involuntary Personal Information Disclosure

Online vendors like Amazon or eBay as well as other bodies such as government agencies or private firms collect and store personal information on their databases, which renders Internet users vulnerable to the risk of personal information loss (Lustgarten, 2015; Jain et al., 2016; Kanyan and Mehra, 2018). The personal information submitted to these online platforms ranges from addresses to financial information like credit card numbers. From the qualitative data collected, it was evident that 5 participants were targeted as their personal information was lost due to the data breaches of big companies (Koyame-Marsh and Marsh, 2014; Wheatley et al., 2016; Gupta, 2017). 3 participants' accounts are provided to illustrate how participants associated their cases with data breaches of large companies. Unfortunately, private companies do not share the real extent of personal information lost due to data breaches (Skroupa, 2017). It appears that companies jeopardize Internet users' financial security while trying to save their reputation. Literature suggests that problems with online vendors' data storage and protection policies (Zhao et al., 2013; Sen and Borle, 2015; Cram et al., 2017) and the unwillingness of big online traders to invest more money on security (Angst et al., 2017;

Larrimore, 2018; Weishäupl et al., 2018) may be considered as the facilitator of data breaches, which in turn enhances online shoppers' visibility to fraudsters.

*"I received many phishing emails, and they increased dramatically after the TalkTalk hack. ... My email account seemed to be something like everybody in the world knows it."* (Patrick, 42 years old male victim).

*"So, what is happened, when TalkTalk was hacked, somehow my card details were saved there. I never save my card details online. ... That website, Groupon saved my card details without my permission."* (Chole, 62 years old female victim).

*My Vodafone account and my online bank account had the same password… I hear lot news about Vodafone hacking. I also use Virgin Media and there is some news about it as well.* (Yasmin, 46 years old female victim).

This section of the chapter has reviewed the findings pertaining to the determinants of being a phishing attack target. Personal information disclosure emerged to be the main reason for being a phishing attack target. Whereas sharing personal information like email address over social networking sites, online advertising websites and free Wi-Fi providers appeared to be risk factors for voluntary information disclosure, data breaches of third parties appeared to boost the odds of receiving a phishing email. The next section of this chapter will look at the determinants of being a hacking attack target.

## 6.3 The Determinants of being a Hacking Attack Target

### 6.3.1 Deviant Online Behaviour

Some online activities like accessing online pornography, peer to peer sharing (P2P), watching free live-streaming and illegal downloading have been labelled as deviant online activities (Bossler and Holt, 2009; Holt and Bossler, 2013; Leukfeldt, 2015). Analysis of qualitative data suggests accessing adult websites, illegal downloading and free streaming increased the risk of being targeted (Bossler and Holt, 2009; Holt and Bossler, 2013; Leukfeldt, 2015). This kind of online usage emerged to be more prevalent among young Internet users. Of the 9 participants who declared engaging with deviant online behaviours, 6 of them were under 30 years old. Examples are displayed to illustrate participants' engagement with online deviancy.

*"Yes, I watch porn. I watched free porn movies and clips before and after the incident. I access a lot of porn for free, so I did not provide any personal details, but there were some pop-up websites when you click on the movies or video clips. There are also some chat room pop-ups as well."* (Alisa, 28 years old female victim).

*"I sometimes watch movies from illegal sources. I used to use torrents to download movies or programs. I would still stream. I do not know how they could make me vulnerable because I never gave my account details. But I guess there could be viruses, which came with torrents."* (Samuel, 28 years old male victim).

*"The victim was accessing the website quoted and then clicked on a link to a site advertised as a "free live-cam website". In doing so, the victim was confronted by a message, alleging it was from UK Police and quoting the victim's Name. It said: "Attention – Your device has been blocked" and quoted breached regulations. The message asked the victim to make a*

*£200 payment to Cheshire Police Authority and quoted various means of doing so." (Police report, G)*

*"The victim was online (Thompsons Holidays) when a message locked his PC which purported to be from Interpol. The message demands that £100 be paid via Ukash following the allegation of the viewing of illegal content, including child pornography. …The last 3 websites that the victim used was 3 of the following: …Xvideos.com"* (Police report, H).

It seems that websites that offer *deviant online activities* like accessing adult content or free streaming may be considered as *hotspots of cyberspace* as these websites generally contain drive-by-download codes, which are hidden scripts embedded in legitimate or legitimate looking websites (McAfee, 2013; Balestrat, 2016). The drive-by download happens when Internet users visit the website. Malicious codes are downloaded to target electronic devices automatically upon entering the website containing the codes (Narvaez et al., 2010; Soltani et al., 2014). This means that the mere presence on the website is enough for malware infection.

Participants were further asked about their perceptions and the reasons for accessing free live streaming websites to watch movies or live games. Two participants' views are provided to illustrate their rationale for accessing free live streaming.

*"I find it quite unfair. They are asking too much money for subscription… I cannot afford that amount of money."* (Samuel, 28 years old male victim).

*"You know you sometimes want to watch a football match at home. But because of the silly broadcasting rules, I cannot watch the games on Saturday. So I go online and find a live stream."* (Joshua, 25 years old male victim).

Higher fees charged by broadcasting companies and the regulations over broadcasting of football matches emerged as two common reasons for accessing free streaming websites.

These results are in line with David and Millward (2012) whose empirical research findings indicated the prevalence of accessing free football live streaming among Wigan Athletic fans in the UK. Their research suggested social factors such as creating a fun culture which enables fans to watch the games in a more entertaining way (i.e. consuming alcohol while watching football games) and financial factors, BSkyB's subscription fees, as the main reasons for accessing free live football streaming.

Interviews with the control group participants suggest that accessing above-mentioned contents does not necessarily lead to hacking victimisation. Five out of twelve non-victim participants also reported engaging with these online activities. All the non-victim participants who engaged with deviant online activities were under 60 years old. As can be observed from control group participants' accounts, using anti-virus programs or ad blockers appeared to be a capable guardian, which apparently prevented victimisation.

*"Typically, I do free streaming. I did not have any bad issue as I have an ad blocker. I do not mind a lot about pop-ups."* (Arthur, 28 years old male, control group).

*"I do online streaming. I have an ad blocker, so it does not cause any problem."* (Kara, 23 years old female, control group).

*"Yes, I do. I use an ad blocker, which is extremely strong; there is no pop-up.*

*I am concerned about being infected, but I run virus scans regularly. I used to use a torrent to download files."* (Preston, 26 years old male, control group).

It appears that the benefits of engaging with deviant online activities like watching free movies or downloading free files influenced Internet users' vulnerability and threat perceptions. Young Internet users especially who benefited from deviant online activities applied security measures like pop up blockers, yet, they persisted using these online actions.

## 6.4 Summary

This first qualitative findings chapter strived to find out why while some Internet users were targeted online, some others were not while accessing the Internet. Distinguishing the antecedents of becoming a target of a phishing and a hacking attack was the primary goal of this chapter. It appears that while personal information disclosure, either voluntary or involuntary, emerged as the main determinant of receiving a phishing attack, engaging with deviant online activities emerged as the main reason of becoming a hacking attack target.

Social networking sites (SNS), online advertising websites and free Wi-Fi providers were the most cited platforms of voluntary personal information disclosure. It appears that privacy calculus is a key factor in Internet users' perception about which information can be shared online. Respondents did not perceive any vulnerability that may be the outcome of submitting their email addresses to the aforementioned platforms. Perceived severity also appeared to be influencing privacy calculus. The possibility of their information being traded between fraudsters and social engineers/hackers was perceived as the worst consequence of personal information sharing. Low perceived severity and perceived vulnerability rendered personal information sharing a low-risk online action. The trade-off between expected risk and benefit appeared to impact Internet users' decision of personal information disclosure. Such trade-off generally occurred in situations where Internet users submitted their personal information in exchange for personal benefits like selling an unwanted product or accessing free Wi-Fi. It appeared that young Internet users were more likely to provide their personal information where a trade-off is present. Data breaches of big companies emerged to be the source of involuntary personal information disclosure. Respondents' accounts indicate increased phishing attacks after the data breaches of big companies.

Engaging with deviant online behaviours emerged to be the main reason for being targets of a hacking attack. Free streaming, illegal downloading from peer to peer or torrent sites and access to adult content seemed to be deviant online behaviours that lead to increased risk of being the target of a hacking attack. High self-efficacy appeared to have a moderating impact on the decision of engaging with deviant online activities. Although most of the interviewees were aware of the possible negative consequences of free streaming or illegal downloading, they still engaged with those activities as they mostly perceived themselves capable of thwarting the attacks. The trade-off between accessing the desired content for free and the risk of malware infection also appeared to impact Internet users' decision of engaging with deviant online activities. Figure 6.1 summarises the process of being a target on an online attack.

This chapter dealt with the first phase of the victimisation to find out antecedents of being a target of phishing or hacking attack. The next chapter will focus on the occurrence of the victimisation.

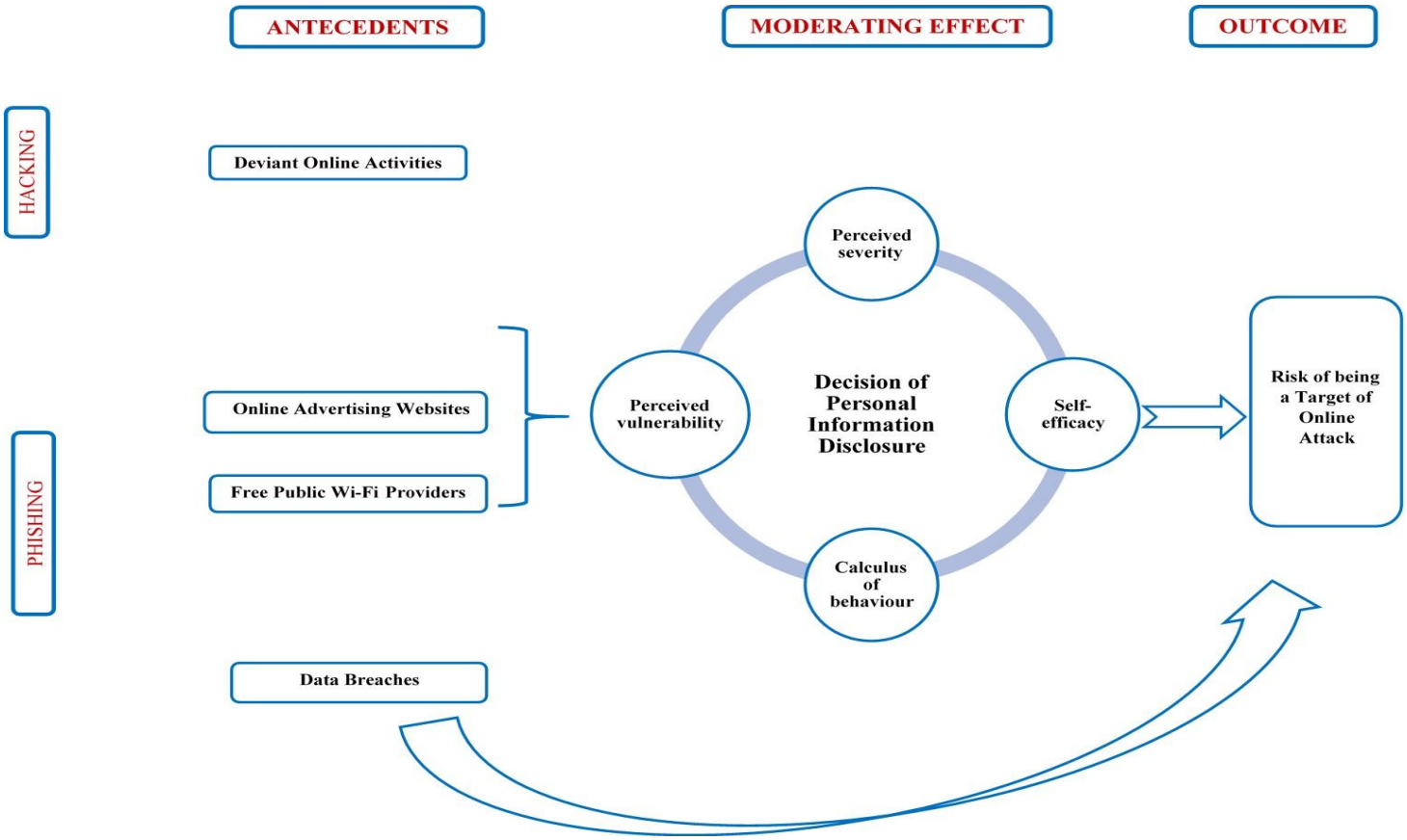



Figure 6.1: *Process of being a Target of an Online Attack*

The previous chapter endeavoured to discern the factors that render Internet users targets of online attacks. This chapter aims to explore the causes of being a victim of economic cybercrime. The main goal of this second qualitative findings chapter is to address the central research question: *What are the factors that facilitate economic cybercrime victimisation at the individual level in the UK?* To that end, the first part of this chapter examines the process of falling victim to economic cybercrime which was identified as the second phase of economic cybercrime victimisation where Internet users were exposed to perpetrators' deceptive actions. The second part of the chapter critically evaluates the impact of Internet users' online lifestyles and contextual vulnerabilities on the risk of experiencing economic cybercrime victimisation.

## 7.1 Factors Affecting Internet Users' Decision-Making Processes

Phishing cases were chosen to be examined in the content analysis since phishing victims were more aware of their victimisation process when compared to hacking victims. Interviews with participants suggested that hacking victims generally became aware of their victimisation through a notification from their banks or other bodies holding their financial information. Unfortunately, most of the hacking victims had no idea about how it happened to them. Nineteen (19) interviews with phishing victims as well as fifty (50) police reports related to phishing victimisation were included in the analysis. Whereas six (6) participants lost money due to email phishing, thirteen (13) of them suffered financial loss as a result of website phishing. While forty-one (41) of Police reports were related to website phishing victimisation nine (9) of them were about email phishing incidents. This first part of the chapter addresses the second of the key research questions: *What factors affect Internet users' decision making-*

*system when they face an online threat?* As email phishing and website phishing employs different modus operandi, they will be discussed separately.

### 7.1.1 Email Phishing

Phishing emails including socially engineered tactics and technical subterfuge increasingly target both individuals and private companies (Cui et al., 2017b; Darya Gudkova et al., 2017; Seals, 2017). The Anti-Phishing Working Group (APWG) is an international consortium that monitors phishing trends and provides advice for business, government agencies and other organizations. Their latest report illustrates that phishing attacks increased 65% in 2016 when compared to 2015 (APWG Report, 2017). It is estimated that 1 in 131 emails contained malware in 2016 (Symantec, 2017). These figures suggest a large volume of email phishing threat. This section of this chapter aims to discern the factors affecting Internet users' decision-making processes when they are exposed to email phishing attempts.

It is argued that there are two types of decision-making processes when individuals face a threat. Whereas the heuristic or system 1 decision-making process produces quick and spurious decisions, systematic or system 2 decision process yields more carefully evaluated decisions (Maheswaran and Chaiken, 1991; Schwarz, 2000). Literature suggests that perpetrators apply sophisticated social engineering methods to increase email users' perceived threat and lead them to make decisions with system 1 or heuristic system processing rather than system 2 or systematic decision-making process (Vishwanath et al., 2011; Wright et al., 2014).

My research identified two main themes, internal and external vulnerabilities, affecting Internet users' decision-making processes when they experienced phishing attempts. While *personal involvement, fear appeals* and *believability cues* like names of big brands were identified as the external vulnerabilities that affected email users' decision-making processes,

Internet self-efficacy and demographic characteristics emerged to be internal vulnerabilities influencing threat assessment processes.

#### 7.1.1.1 External Vulnerabilities

**Personal Involvement**

Cranor (2008) suggests that successful online communication commences with grabbing internet users' attention. Internet users receive many emails, but they read a few relevant ones carefully. Celsi and Olson (1988) define this kind of relevance as felt involvement, which determines individuals' reactions to received messages.

The interview data suggest that two types of personal involvement may be perceived: **direct involvement**, where specific personal information such as last four digits of a credit card was mentioned in the email and **indirect involvement,** where non-personal but relevant information like a notice about bank account was included into phishing email. The first type of personal involvement occurred as spear phishing attacks, where fraudsters included email users' some personal information into phishing emails. Wang et al. (2012) found that felt involvement increased cognitive effort to evaluate phishing emails. Cheshire et al. (2010) assert that direct personal involvement boosts guardianship behaviour, which prevents future victimisation; yet, findings of my research indicate that increased personal involvement made Internet users more susceptible to phishing attacks. As my victim participants whose accounts are presented below acknowledged, it was relevant personal information that increased the believability of the phishing emails. This finding is supported by the results of Harrison et al. (2016) who examined individual factors in phishing email processing. The results of their study indicate that although individuals showed increased attention to emails, they lacked the elaboration of the facts presented in the phishing emails, which led them to respond to those

emails. Examples are provided to illustrate what kind of information used to in spear-phishing attack to convince individuals.

*"… Well, I was really surprised that* ***they know my details,*** *so that made me believe that email was real."* (Alice[11], 29 years old female victim).

*"…****they mentioned something that I can relate my transactions etc.*** *They mentioned something that made me believe that it is true."* (Amelia, 29 years old female victim).

*"…They had my email address and* ***had a part of my credit card number. Just the stars but they had the last four digits. My name and surname were also included in an email".*** (Jessie, 35 years old female victim).

**Fear Appeals**

Email phishing literature suggests that fraudsters employ influence methods (Wright et al., 2014; Silic and Back, 2016; Oliveira et al., 2017; Williams et al., 2017) as well as fear appeals (Witte, 1992; Liang and Xue, 2010; Jansen, 2015; Jansen and Leukfeldt, 2016), time pressure (Kahneman, 2011; Zhang et al., 2012; Greitzer et al., 2014; Saqib and Chan, 2015) and urgency cues (Wang et al., 2012; Alsharnouby et al., 2015; Ferreira and Lenzini, 2015; Harrison et al., 2016) to lure or coerce email users into disclosing personal or financial credentials. This thesis identified only fear appeals as risk factor for responding phishing emails.

[11] All participants names are anonymised. Names used to represent participants were chosen randomly from an online baby name dictionary.

Analysis of the interviews suggested fear appeals such as the threat of paying for unwanted items or account closure appeared to be effective in forcing participants to make urgent decisions based on heuristic processing.

Fear appeals are persuasive messages prompting both a fear-provoking menace and a suggestion to thwart a threat. (Witte, 1992; Williams, 2012). Fear appeals are composed of two parts: statements indicating imminent threat and statements suggesting a recommendation to cope with threat (Vance et al., 2013). Findings of this thesis related to the effectiveness of fear appeals in coercing Internet users to divulge personal information are in line with previous research (Workman, 2008; Sharma, 2010; Jansen and van Schaik, 2018) who found a correlation between fear appeals and getting phished. Victims' accounts indicate fear appeals (i.e. the threat of economic loss) coerced them to make quick decisions based on heuristic decision-making and follow the proposed recommendations which appeared to be the best solution to resolve the problem (clicking on the link and fillings the forms). This finding also lends support to Goel et al. (2017) who found that Internet users were more likely to respond to emails related to protecting assets. Apart from the anxiety about losing money, distraction may also be an explanation of why fear appeals lead Internet users to be the prey of email phishing. It is argued that disproportionate attention to fear appeals may distract Internet users attention from the real task which impedes a sound evaluation of the fabricated scenario (Vishwanath et al., 2011; Ferreira et al., 2015; Ferreira and Lenzini, 2015). Two examples are provided to illustrate the fear appeals perpetrators used to target Internet users' decision-making systems.

*"I received an email from Apple saying that my Apple ID was used to purchase a game and if I want to cancel the purchase, I should follow the link and fill the cancellation form. I guess I felt a little bit anxious about paying for something that I did not really want. I did not*

*buy a game, but my daughter used my iPad, so I thought she might have bought it mistakenly."* (Alice, 29 years old female victim).

*"I received an email from* ***PayPal saying that there are some problems with my account****, so I need to change my details. I clicked on the link. They asked for financial details such as bank account number and sort code. I filled everything. I clicked on the next button, and then they asked my other details such as home address."* (Amelia, 29 years old female victim).

Interviews with control group participants suggested whereas low fear appeals did not produce the required stimuli to respond to phishing emails. High fear appeals intensified attention to other parts of messages like URL address line or name, which in turn helped email users to thwart the threat. Similarly, House (2013) found that strong fear appeals decreased response rates as they made email users focus on other cues to investigate the originality of emails. This finding supported fear appeal literature suggesting that only the right amount of fear appeals produce intended persuasion (Keller and Block, 1996; Witte and Allen, 2000; Viljoen et al., 2010; Manyiwa and Brennan, 2012).

*"I received many dodgy emails, but the PayPal one was really good, except they used my email address instead of my name. The email was very convincing; I nearly clicked on it. Because I was really worried about it. Then I said no it is not my name"* (Faith, 45 years old female, control group).

**Believability Cues**

Names of big brands appeared to be another factor that enhanced the believability of emails. Bowen et al. (2011) argue that believability is the key factor in overcoming users' defensive reactions. Findings of this thesis support results of empirical researches (Devarajan

et al., 2012; Schuetz et al., 2016; Silic and Back, 2016) stating that inclusion of reputable or trusted brands' names into email messages increased email users' susceptibility to divulging personal information.

*It was strange since they were also asking for a three-digit security code.* ***But I said it is OK since the mail was from Apple****."* (Alice, 29 years old female victim).

*"I got an email from PayPal saying that* ***somebody had bought some music from iTunes*** *for £19.9 and I need to confirm the payment. So, I clicked on the email link. It asked me for my details, which I gave."* (Jessie, 35 years old female victim).

#### 7.1.1.2 Internal Vulnerabilities

**<u>Internet Self-Efficacy</u>**

Internet self-efficacy emerged to be another factor that increased Internet users' susceptibility to phishing attacks. Of the six email phishing victims, four respondents indicated that they lack Internet knowledge about online threats.

*"I am not very knowledgeable about online threats. But if I face something, I usually ask my friends about it."* (Amelia, 29 years old female victim).

*"No, I am not very knowledgeable about online threats."* (Jessie, 35 years old female victim).

Control groups' accounts also support the supposition that Internet self-efficacy is an essential factor in thwarting fishing attacks.

*"I often get emails supposedly from banks, saying that bank accounts have a problem if I click on the link, they will try to sort it out. … In earlier times if you did click the link, you*

*went on a website, which was fairly obvious that it was not an official bank. But in recent times it did become a little bit sophisticated. … I also had a number of similar attempts with PayPal, which says my PayPal account was accessed by someone else. If you click on the link, this will be sorted out. But when I clicked on the link, the supposedly PayPal was not real PayPal. It was so easy to tell it was a scam."* (Mike, 34 years old male, control group).

**Demographic Characteristics**

Previous studies researching Internet users' susceptibility to email phishing attacks suggested demographic differences in the likelihood of responding a phishing email (Sheng et al., 2010; Sumner et al., 2011; Darwish et al., 2012; Wang et al., 2012). Recruitment criteria to be a victim participant was losing money due to unauthorised access to banking card information, online financial accounts like PayPal or online banking accounts for this research. Thus, the type of victimisation experienced such as hacking, email phishing or website phishing was random among participants. Cross-tabulation of the type of victimisation and demographic characteristics of participants suggest a gender difference in responding to phishing emails (Table 7.1). Four out of six email phishing victims were female. This findings is in line with previous research suggesting female Internet users to be more susceptible to email phishing attempts (Sheng et al., 2010; Blythe et al., 2011; Halevi et al., 2013a; Halevi et al., 2013b; Pollacia et al., 2014; Halevi et al., 2015). Though, Oliveira et al. (2017) found that older women participants were more susceptible to spear phishing attacks. It should also be noted that some other empirical studies (Wang et al., 2012; Benenson et al., 2017) have not found any significant impact of gender differences on the risk of responding to a phishing email.

Analysis of interviews indicated that young Internet users are more susceptible to responding to phishing emails. Five out of six email phishing victims were young Internet users. This finding supports the results of past empirical studies indicating young Internet users

as a risk group for email phishing (Darwish et al., 2012; Mohebzada et al., 2012; Zielinska et al., 2014; Sarno et al., 2017).

Table 7.1
*Demographics of Phishing Victims*

| Usage | Age | | | Gender | |
|---|---|---|---|---|---|
| | Young (Under 30) | Middle Aged (31-60) | Elderly (60+) | Male | Female |
| Email | 2 | 1 | 1 | 0 | 4 |
| Website | 1 | 4 | 7 | 6 | 6 |
| Multiple (Email) | 0 | 2 | 0 | 2 | 0 |
| Multiple (Website) | 0 | 1 | 0 | 0 | 1 |
| Total | 3 | 8 | 8 | 8 | 11 |

### 7.1.2 Website Phishing

An extensive review of phishing victimisation literature illustrated that website phishing victimisation, which refers to submitting personal or financial information to bogus or fraudulent websites, is understudied. This thesis is one of the first thesis researching website phishing victimisation. Cross-tabulation results presented in Table 7.1 indicate that website phishing is a more serious problem than email phishing, especially for elderly[12] Internet users. As can be seen from the table, elderly participants reported considerably higher website victimisation when compared to young participants. Analysis of semi-structured interviews and police reports suggest low Internet self-efficacy and malware infection as the factors affecting the chance of being a victim of website phishing.

[12] Elderly participants are those who were aged over 60 years at the time of the interviews. The word elderly represents the age group over 60 throughout this thesis.

**Low Internet Self-efficacy**

Low Internet self-efficacy emerged as one of the reasons for becoming a website phishing victim (Table 7.2). Participants who experienced economic cybercrime through website phishing were further asked whether they knew how to differentiate between bogus and original websites. Most of the respondents (nine out of thirteen) acknowledged a lack of basic knowledge such as checking padlock to identify fake websites. As can be seen from the table illustrating an excerpt of victim participants' accounts, participants provided their financial details to websites that pretend to be legitimate traders or official government websites. Lack of knowledge differentiating bogus websites from the official websites emerged a reason for being a website phishing.

**Malware Infection**

Analysis of police reports indicates that stimulating fear appeals with pop-up messages was an effective method to coerce Internet users to yield personal financial information. It appears that pop-up messages purporting to be from police forces provoked Internet users to reveal their personal financial information. Although the claims made through pop-up messages were fake; they were successful in coercing Internet users to divulge personal financial information. It appears that fear appeals were successful in creating high levels of perceived severity about the outcomes of the messages displayed on the screen. This finding is in line with previous studies (i.e. Auer and Griffiths, 2016; du Preez et al., 2016; Ginley et al., 2017; Harris et al., 2018) researching the impact of pop-up messages as fear appeal tools on online gambling behaviour. The results of these studies indicate that fear-provoking pop-up messages were successful in promoting responsible gambling as most of the online gamblers followed the instructions shown on the pop-up windows.3 examples are provided to illustrate the relationship between malware infection caused by engaging with online deviancy facilitated website phishing victimisation.

Table 7.2
*The Relationship between Low Internet Self-efficacy and Website Phishing*

| Participant | Participant Account | Researcher Note | Theme |
|---|---|---|---|
| Joy, 45 years old female | My son plays a game called Minecraft, and there is a special download. But I do not know how it works. I searched Google and find a site that allows me to download it. It was something around £20. So, while downloading I put my credit card details as well. Later my bank called me and said that there are some suspicious transactions and they wanted to check if I was the one who did transactions. | Pay insecure website<br><br>Lack of knowledge about bogus websites. | Low Internet Self-efficacy |
| Police report, case X | The victim found the suspect website to watch a film; the website had free films and films which would require payment to watch. To use the website, the victim had to put their debit card number in the details for identification. Subsequently when the victim watched, what was clearly labelled as a 'free film', a few days afterwards the company took a sum out of her bank account | Pay insecure website. | |
| Sophie, 32 years old female | I used online government service to apply for national insurance number. … I searched the Web and found a website about it. … I filled the forms and paid £55 for it. …Two months later my husband found another job, so he gave his national insurance number, but his boss said that it is not a real national insurance number. He gave us the exact website address. I saw that the one we used and the real one was different. So, I was tricked into a bogus website. | Lack of knowledge about government website. | |
| Florence 75 years old female | …I thought instead of waiting for my daughter, as she does every time, everything we need she does. … We (she and her husband) opened the Internet and wrote "visa America", and we get the first one. All came up; we filled the form, answered all the questions. They asked for the bank details. I remember from the last time that it was something like £20 for each. After we gave the bank details, then it flashed up it was £220 for both of us. | Pay bogus website. Lack of knowledge about pretending to be official website. | |
| Jamie, 76 years old male | …It was looking like an official government website. You go to the site thinking that it is a government website, but it is not. You end up paying something not a lot for them to do it yourself. | | |

*"The victim was on his computer when he was logged into AOL website. A Cheshire police message came up on the screen advising that he had been downloading or looking at inappropriate material."* (Police report, case A)

*"Victim has received a screen showing pictures of naked women and men having sex with a logo of 'Naughty America' after receiving a cold call from a suspect posing as Microsoft."* (Police report, case B).

*"The victim was on a website when a pop up appeared advising to be from Interpol and the police advising the victim that has been looking at child porn."* (Police report, case C).

Receiving these pop-up messages can be explained with malware infection, which may be the outcome of engaging with deviant online activities. The previous chapter (Chapter Six), which examined the antecedents of being targeted online, suggested that engaging with deviant online activities like free streaming or viewing adult content increased the risk of being a target. These results appear to support this finding as most pop-up messages threatened the victims with viewing illegal sexual content like child abuse. Police reports indicated that victims facilitated victimisation processes through their deviant online actions as most of those victims' Internet history contained adult websites.

This first part of the chapter examined phishing victimisation process to discern factors influencing Internet users' decision of revealing their personal financial information to fraudsters. The process of email phishing was examined, and website phishing victimisation processes were evaluated. Based on victims' accounts, a phishing victimisation model was built to illustrate and account for phishing victimisation process (Figure 7.1).

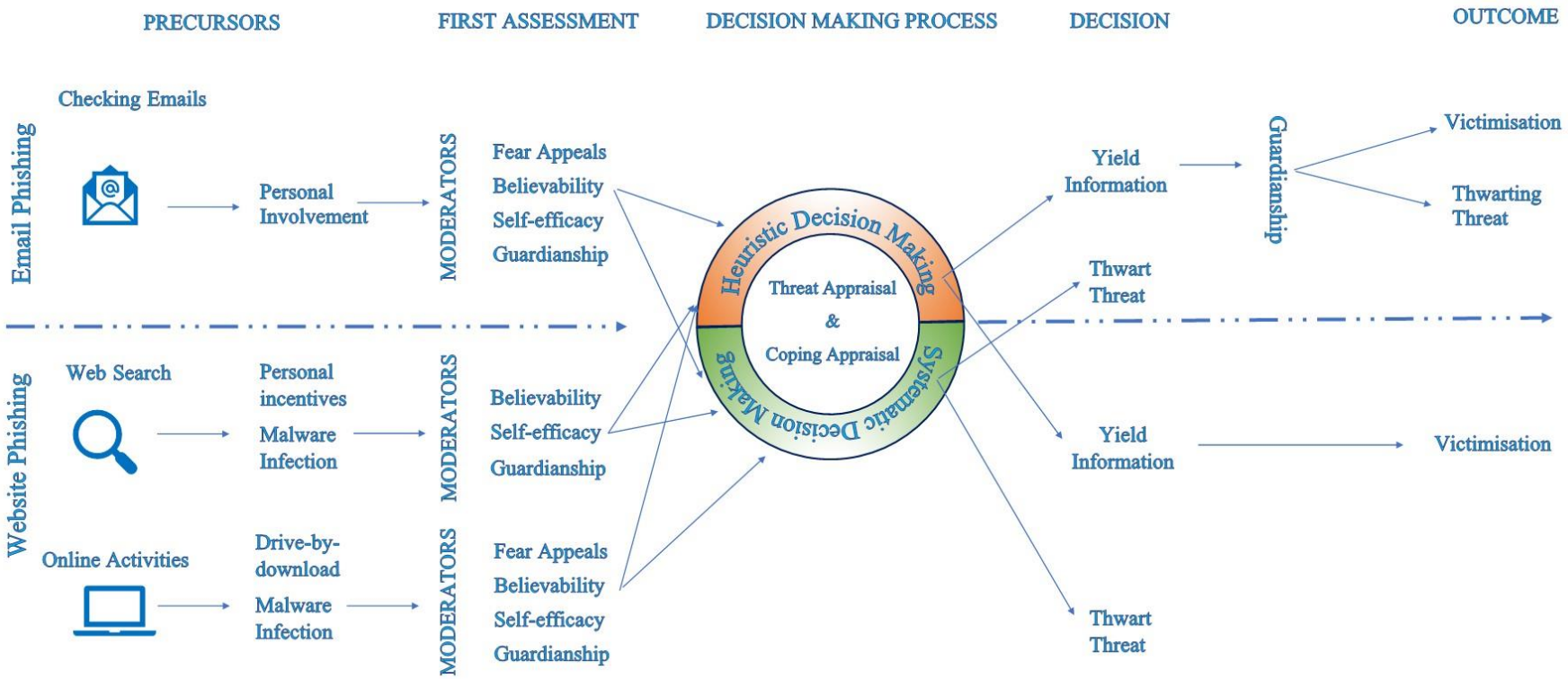



Figure 7.1: *Phishing Victimisation Process*

## 7.2 Correlates of Economic Cybercrime Victimisation

The previous first part of the chapter explored the cognitive and personal and behavioural factors facilitating economic cybercrime victimisation through phishing. A phishing victimisation model, which depicts the phishing victimisation process was introduced at the end of the first part. This second part of the chapter aims to discern the effect of Internet users' online lifestyles and contextual vulnerabilities on the risk of experiencing economic cybercrime victimisation. Initially, the relationship between Internet users' online activities and the likelihood of facing economic cybercrime will be discussed, and then contextual vulnerabilities approach of this thesis will be introduced.

### 7.2.1 Online Lifestyle Correlates

#### Engaging with "ordinary" Online Activities

The results of past empirical research (Bossler and Holt, 2009; Ngo and Paternoster, 2011; Reyns et al., 2015; Leukfeldt and Yar, 2016)suggested that Internet users' daily ordinary online activities increased the risk cybercrime victimisation. Likewise, analysis results of the Crime Survey for England and Wales 2014/2015 presented in Chapter Five indicated that ordinary online activities like shopping online or accessing online banking were associated with increased risk of economic cybercrime victimisation. Yet, it was not clear why ordinary online activities enhanced the risk of economic cybercrime victimisation.

To examine whether ordinary online activities had an impact on the risk of victimisation, both victim and control group participants were asked to list most frequently engaged online activities. *Using the Internet for social networking, leisure activities, financial activities, checking emails* and *browsing for information* was the most cited online activities. Analysis of interviews appears to indicate that when participants' age increased, the variety of

online lifestyle decreased. Whereas younger participants accessed the Internet for a wide range of purposes covering all above-mentioned activities, elderly victim participants limited their Internet usage to a few of those online activities. Social networking, leisure activities such as playing online games and online banking was the most frequently engaged online activities for elderly participants.

Interviews with control group participants yielded similar results. Non-victim Internet users belonging three age groups, namely young, middle-aged and elderly participants, showed similar Internet usage patterns with victims.

There appears to be no difference between the online lifestyles of the victim and non-victim participants. Interviews suggest that ordinary online activities do not pose a risk of becoming a victim of economic cybercrime. This finding contradicts past research results (Bossler and Holt, 2009; Ngo and Paternoster, 2011; Reyns et al., 2015; Leukfeldt and Yar, 2016) who argue that ordinary online activities like using email, shopping online or using online banking increase risk of victimisation.

**Deviant Online Behaviour**

Findings presented in Chapter Six have shown that engaging with deviant online behaviours like free streaming, illegal downloading via Torrent or Peer-to-peer sharing programs and accessing adult content emerged to be risk factors for being a target of hacking attacks. Hence, this issue will not be addressed here again. Implications of these findings will be discussed extensively in the Discussion Chapter (Chapter Nine).

### 7.2.2 Contextual Vulnerabilities

The extensive review of the cybercrime victimisation literature indicates that past cybercrime victimisation research that applied LRAT as theoretical framework conceived Internet users' online behaviours and demographic characteristics as the main facilitators of cybercrime victimisation. For instance the results of studies suggested that using online banking or online shopping was a risk factor for experiencing cybercrime (Ngo and Paternoster, 2011; Reyns et al., 2011; van Wilsem, 2011; Leukfeldt and Yar, 2016), however, these studies failed to account for why online shopping was a risk for some Internet users and not others. Internet users' social and psychological conditions, which are usually influx, are downplayed. These studies assume that individuals are always at the same psychological mood and their social life conditions never change. This thesis proposes that although Internet users' online lifestyles may have an impact on the risk of victimisation, some other factors such as technological, social or personal vulnerabilities may also affect the risk of experiencing cybercrime victimisation. These vulnerabilities are conceptualised as ***"contextual vulnerabilities"*** since semi-structured interview results suggest that the emergence of these vulnerabilities is highly context-dependent in most cases. Initially, the effect individual and behavioural vulnerabilities on the likelihood of experiencing economic cybercrime victimisation will be presented. Then the impact of socio-cultural vulnerabilities on the chance of becoming victim will be discussed before examining the effect of macro vulnerabilities on the risk of victimisation.

#### 7.2.2.1 Individual and Behavioural Vulnerabilities

Analysis results pertaining to internal vulnerabilities that render Internet users susceptible to email phishing has illustrated that Internet self-efficacy and demographic characteristics (age and gender) were individual vulnerabilities that increased the likelihood of

experiencing economic cybercrime victimisation. Likewise, PMT constructs perceived vulnerability, perceived severity and perceived rewards were other individual vulnerabilities that impacted the chance of becoming a victim of economic cybercrime. Hence, these findings will not be presented here again. Problems related to password management emerged to be another individual vulnerability that facilitated victimisation. This section of the chapter presents findings pertaining to influence of password management on the risk of experiencing victimisation.

## Password Management

Problems with password management appeared to be one of the reasons for online personal account protection. Respondents were asked about their password management strategies to protect their both personal and financial accounts. Whereas 26 victim participants acknowledged using complex passwords to protect their accounts, 21 victim participants reported using the same passwords for a different online account. Similarly, nearly half of the non-victim participants also used the same passwords for different online accounts. Table 7.3 illustrates some excerpts from victims' accounts related to password management This finding complies with Das et al. (2014) who find that 43-51% of Internet users use the same passwords for different online accounts.

As can be observed from the Table 7.3 password fatigue, which is being overwhelmed with loads of digital identities and identity-related passwords (Jøsang et al., 2007; Corre et al., 2017; Dasgupta et al., 2017), appeared to be one of the main reasons for using the same password for different online accounts. Increased volume of password appeared to increase the risk of password fatigue

Table 7.3
*Password Management*

| Participant | Participant Account | Researcher Note | Category/Theme |
|---|---|---|---|
| Sophie, 32 years old female victim | I use the same password for my accounts, so that is why my email account was hacked. | Same password for several online accounts | Password fatigue/Password management |
| Kai, 32 years old male victim | I think I used the same password for this application and PayPal account. Because it is very handy, this can also be an explanation. | Same password for several online accounts | |
| Kyle, 30 years old male, control group | I am not very good at password management. I use the same password for multiple online accounts." | Same password for several online accounts | |
| Kian, 33 years old male victim | I try to use different passwords for my online accounts, but it is difficult to keep them in mind. So, I mostly use one or two passwords for all of my accounts. | Difficulties memorising multiple passwords | Password fatigue/Password management |
| Tilly, 28 years old female victim | Considering password, I have difficulties in remembering different passwords, so I use one password for all of my online accounts including my Facebook and email account. | Difficulties memorising multiple passwords | |
| Mikey, 34 years old male, control group | I tend to use similar passwords for similar things. I know that I need to use different passwords. It is about remembering them. You forget passwords. | Difficulties memorising multiple passwords | |

**Internet Users' Perceptions and Knowledge about Online Security**

Protection Motivation Theory posits that individuals' decision of applying security measures is highly dependent on their perceived risk and response efficacy (Rogers, 1975, 1983). Interviews suggest that Internet users' perception about the protection capability of their electronic devices, the efficacy of guardianship measures in thwarting attacks and a sense of security impacted their decision of applying guardianship measures. Excerpts from participants' accounts are displayed in Table 7.4.

As can be seen from the table Apple users believed that Apple products could not be infected, or they are better protected against viruses when compared to Windows-based operating systems This misperception about the ability of Apple products in maintaining secure online environment appears to affect the likelihood of applying a security measure adversely.

Response efficacy also emerged to be a factor impacting Internet users' decision of applying a security measure. Interviews suggested that some participants did not apply any security measure as they believed that these measures would not prevent victimisation. Similarly, past empirical research indicate decision of using security software (Chenoweth et al., 2009), securing wireless protection at home (Woon et al., 2005) using a strong password and backing up data (Crossler, 2010) is highly dependent on perceived response efficacy.

A false sense of security appeared to be another risk factor for facing economic cybercrime victimisation. Ngo and Paternoster (2011) suggest that security software creates a false sense of security, which encourages Internet users to engage with riskier online activities. Especially young Internet users repeatedly cited that using pop up blockers or other forms of software-based security measures protect them while they engaged with deviant online behaviours such as downloading materials illegally or watching movies through live streaming websites. However, the ability of software-based security measures may be drastically impeded

when Internet users install virus containing shareware software like peer-to-peer sharing software (Kwok et al., 2002; Johnson et al., 2008).

#### 7.2.2.2 Socio-cultural (Context Specific) Vulnerabilities

Previous research on physical world scams or frauds finds out that life events such as divorcing, having a baby, or sudden unemployment had increased the risk of becoming a victim of a financial crime (Taylor, 2009; Deevy et al., 2012; Harvey et al., 2014). Although cybercrime studies have researched the impacts of physical world outdoor activities such as going to bars or meeting friends on the risk of experiencing cyber victimisation (van Wilsem, 2011{Broadhurst, 2017 #1341)}, no research has examined the role of social, personal and psychological conditions of Internet users on the risk of experiencing economic cybercrime victimisation. This next section discusses the impact of the intersection of some social and personal vulnerabilities that prepared suitable conditions for economic cybercrime victimisation.

**Peak Sale Periods**

Peak sales periods and high demand for popular products appeared to be social vulnerabilities exploited by fraudsters to socially engineer Internet users into revealing their financial details. During the peak sales periods such as Christmas or Valentine's Day Internet users rush to buy gifts for their beloved ones (Close and Zinkhan, 2009). Research on Valentine's Day illustrates that more than $20 billion was spent to purchase gifts such as flowers or greeting cards in the US in 2018 (Mende et al., 2019). Interviews indicate that Internet users' desire to buy something special or extraordinary may be a source of vulnerability. It seems that when this kind of social vulnerability coincides with a lack of knowledge about demarcating genuine websites from bogus websites victimisation occurs.

Table 7.4
*Security Measures Avoidance*

| Participant | Participant Account | Researcher Note | Theme |
|---|---|---|---|
| Ruby, 24 years old female victim | I do not have anti-virus in my computer, which is really bad I know. I still have this image, you know, there are no viruses on Mac. So, I do not have any anti-virus. | Misperception about Apple products' security | Security Measures Avoidance |
| Joshua, 25 years old male victim | I have a Mac, which is good stuff. It looks more secure than having a Windows. Just base things without doing extra protection. | Trust in Mac OS | |
| Jessie, 35 years old female victim | I do not have anti-virus programme as I only use my iPad and iPhone to access the Internet. | Trust in IOS | |
| Archie, 62 years old male victim | I have a virus checker on the computer, but with iPad, there is no anti-virus program. | Trust in IOS | |
| Harrison, 32 years old male victim | I believe that perpetrators can get your personal information when they want. So, there is no need to be worried about it. | Response efficacy/Omnipotent hacker | |
| Alice, 29 years old female victim | I think if someone wants to target you, it would be very easy to get your information through hacking into your computers. | Response efficacy/Omnipotent hacker | |
| Arthur, 28 years old male, control group | …typically, free streaming. I did not have any bad issue as I have an ad blocker. I do not mind a lot about pop-ups. | A false sense of security | |
| Alisa, 28 years old female victim | I use McAfee anti-virus program, which I bought online. … there were some pop-up websites when you click on the movies or video clips. There are also some chat room pop-ups as well." | A false sense of security | |

**Negative Life Events**

Negative life events emerged to be another contextual vulnerability impacting the likelihood of experiencing cybercrime victimisation (Table 7.5). Breaking up of a long-lasting relationship, having familial problems and changing social environment appeared to be negative live events decreasing Internet users' vigilance. Additionally, financial problems appear to force young Internet users engage with online deviancy. Although participants did not mention that they engaged with deviant online activities for financial gain, which in turn facilitated their victimisation, two of the participants appeared to have somehow faced victimisation due to their online lifestyles.

Findings related to the impact of engaging with deviant online behaviours on the risk of becoming a target of economic cybercrime were examined in the previous chapter (Chapter Six). Interviews appeared to suggest that Internet users' decisions of engaging with risky online activities are not only shaped by personal preferences but may sometimes be determined by sudden or dramatic changes in the Internet users lives.

Table 7.5
*Socio-cultural Vulnerabilities*

| | Code | Category | Category | Theme/Concept |
|---|---|---|---|---|
| I broke my long-time relationship just before that incident. It was really hard times as I had a bad relationship, which was about to cost my life. I was in a new place, making new friends. I was making a new life. … socially and psychologically I was not at my best point. I was just a girl who was trying to recover and trying to find a path again | Psychologically down/Breaking Relationship | Negative Life Events | Socio-cultural Vulnerability | Contextual Vulnerabilities |
| I had just finished long relationship about fifteen years. I have been looking for dating sites. At that time, perhaps I was not alert about that kind of thing, a little bit depressed about my situation. Because I have been in a long relationship and I was a little bit down." | Psychologically down/Breaking Relationship | | | |
| Both times happened when I was struggling for the money. | Financial problems | | | |
| Internet is also a money-making machine for young people through YouTube or other platforms. Also, some young people engage with amateur pornography. | Financial problems | | | |
| … it was when my nephew was in the hospital. So, we were all worried, and I had to buy many things with my card. So, I did not pay attention to. We were living in a bubble. You go to the hospital and see a sick boy. You cannot concentrate on what or where you buy it. ... And then once you got home, you feel better and come back to yourself, become more cautious. | Familial problems | | | |
| I saw that transactions were made in Japan through my debit card…. I have been to Japan one month before the victimisation, but I did not use my debit card, I made all payments with cash. However, I accessed my online banking account to transfer money to my father. I used the hotel's Wi-Fi for these transactions. | Changing social settings | | | |
| I have moved over B.to D. and I work in N. I was settling up. I was getting an apartment through state agents and there were various email back and forth. They needed personal information from me, which I exchanged by email. They also needed some bank details because I had to pay for deposit and to set a direct debit with the landlord | Changing social settings | | | |
| … It was my son… I could not resist him, and as he urged me to buy it, I did not concentrate well. I feel like a stupid. | Decreased attention | | | |
| I was really busy. The deadlines and music there is no extension for the deadlines. You could have become forgetful. Maybe that made it vulnerable to make a mistake | Decreased attention | | | |

#### 7.2.2.3 Macro Vulnerabilities

Up to date, online victimisation studies framed by LRAT have used individual level (micro level) data to examine victimisation in cyberspace. However, victimisation is a complex phenomenon, which can be the outcome of complex interactions between individual and aggregate level factors Hope (2012). Economic cybercrime victimisation can be the result of both individual and environmental (technological) factors. {Miethe, 1993 #212 argue that multi-level contextual analyses can act as a bridge between two levels. Hence a contextual vulnerabilities approach, which considers both individual and aggregate level factors as a potential source of victimisation, aims to address this gap in the literature.

Previous sections examined the impact of individual-level contextual vulnerabilities on the risk of becoming victim to economic cybercrime. Research findings appeared to suggest that technological vulnerabilities, social and personal vulnerabilities may create suitable conditions for victimisation. Additionally, interviews with both victim and non-victim participants indicated that there might be other vulnerabilities beyond Internet users' control. Findings presented in Chapter Six indicate that data breaches of big companies or security issues of big brands presented the risk of being a target of phishing attacks. Apart from the aforementioned factors, banks' refund policies and poor security management of online merchants emerged to be vulnerabilities that are beyond the control of Internet users. These kinds of vulnerabilities are named as macro vulnerabilities. This next section of the chapter will evaluate the impact of macro vulnerabilities on the chance of becoming an economic cybercrime victim.

## Technological Vulnerabilities

The technological vulnerability is generally defined as the risk of experiencing adverse consequences due to the failure of technological systems (Martin, 1996). For my research purposes, technological vulnerabilities are conceived as the risk of facing economic cybercrime victimisation as a result of exploited features of Internet technologies. This section of the chapter addresses the third key question: *How technological vulnerabilities impact the chance of being a victim of economic cybercrime?*

This thesis identified the type of electronic devices utilised to access the Internet, Wi-Fi hotspots and mobile applications as technological vulnerabilities that facilitated victimisation. Effect of these technological vulnerabilities will be critically assessed at this juncture of the chapter.

## Impact of Electronic Device Preferences on the Risk of Facing Victimisation

With recent technological developments, it is now possible to access the Internet via a wide range of electronic devices (Tsetsi and Rains, 2017; Marler, 2018). Whereas desktop computers and laptops were the only means of accessing the Internet in the past, mobile phones, tablets, TVs and even gaming consoles can be used to currently access the Internet (Duggan and Smith, 2015; van Deursen and van Dijk, 2015). Chapter Five examined the impact of electronic device preferences on the risk of becoming an economic cybercrime victim through statistical analysis of the Crime Survey for England and Wales 2014/2015. It was hypothesised that accessing the Internet via electronic devices such as mobile phones or handheld computers would increase the risk of economic cybercrime victimisation while conducting statistical analysis in Chapter Five. The results of quantitative analyses appeared to support this hypothesis. The results indicated that electronic devices, which were labelled as risky devices, such as mobile phones or smartphones, laptops being used away from home/work/college and

tablets increased the risk of experiencing economic cybercrime. The aim of this section is to triangulate quantitative results and explore factors affecting Internet users' electronic device preferences while accessing the Internet.

This section of the chapter presents findings related to the impact of device preferences on the risk of victimisation and motives affecting Internet users' device preferences. The victim and non-victim participants were asked about their most preferred electronic devices utilised to access the Internet and to do financial actions such as online shopping. Interviews demonstrated that nearly all participants used multiple devices to access the Internet. Nevertheless, Internet users had a certain device preference to engage with online financial activities. Interviews with both victims and control group participants indicated that while laptop computers and mobile phones were the most preferred electronic devices for victims, laptop computers were the most preferred device for control group participants (Table 7.6).

As can be seen from the Table 7.6, while 28% of victim participants preferred mobile phones/smartphones as a medium to access financial content, approximately 17% of non-victim participants used mobile phone or smartphone to access the Internet. There seems to be an association between smartphone usage and economic cybercrime victimisation. This finding appears to support authors, who argue that security breaches of mobile phones may cause loss of personal financial information (Mobile Iron, 2016; Ponemon Institute, 2016).

Table 7.6
*Preference of Electronic Devices Used for Financial Purposes*

| Type of Electronic Device | Victim | Non-victim |
|---|---|---|
| Desktop PC | 5 (%15.6) | 1 (% 8.3) |
| Laptop | 11 (%34.3) | 7 (%58.3) |
| Mobile Phone | 9 (%28.1) | 2 (%16.6) |
| Multiple Devices | 1 (%3.1) | 0 |
| Tablet | 6 (%18.7) | 2 (%16.6) |

Victim participants were asked about the rationale behind their electronic device preferences for online financial activities. While ease of use and having a large screen was the most cited rationale for using desktop and laptop computers to engage with online financial activities (Penny et al., 2016; Bröhl et al., 2018); mobility, convenience and ability to use mobile applications was the most repeated reasons for preferring mobile or smartphone to purchase goods online (Huang et al., 2017).

*"I prefer the computer for the convenience of using a keyboard and large screen*." (Harrison, 32 years old male, victim).

*"I have a laptop at home, and I used that for most of the things because I can type more easily."* (Parker, 63 years old male, victim).

*"I use my phone to shop online as I configured all my accounts."* (Alisa, 28 years old female victim).

*"It is actually easier to do these things on my phone rather than Laptop."* (Mia, 23 years old female victim).

Interestingly security as a cause of preference was cited only for tablets. Tablets were perceived as more secure electronic devices to access the Internet. This perception was mainly based on beliefs about Apple products. It is argued that It seems that such wrong perceptions increase the odds of becoming a victim of economic cybercrime.

*"I use only my iPad to access online banking and online shopping since I feel it is more secure."* (Sophie, 32 years old female victim).

*"I use iPad because you do not usually get viruses on iPad."* (Archie, 62 years old male victim).

Participants' electronic device preferences to engage with online financial activities were cross-tabulated with the type of victimisation via the Matrix Coding Query option of NVIVO qualitative analysis software. As Table 7.7 demonstrates, participants who faced hacking victimisation preferred to engage with online financial activities via laptop or mobile phone/smartphone. Phishing victim participants mainly used Laptop and Tablets to engage with online financial activities. Those who faced multiple victimisation experiences preferred mobile phone for online financial reasons. These findings appear to support the results of Quantitative Analysis Chapters as laptops, and mobile phones emerged as risky devices for online financial activities. It is also interesting that individuals mainly favoured one type of electronic device to do financial activities. Given the ample opportunities to access multiple devices, it was expected that multiple device usage would be higher. These results should be interpreted cautiously in the light of guardianship behaviours and the impact of other technological vulnerabilities such as free public Wi-Fi usage.

Table 7.7
*The Relationship between Type of Device for Financial and Type of Victimisation*

| | Type of Electronic Device | | | | |
|---|---|---|---|---|---|
| Type of Victimisation | Desktop PC | Laptop | Mobile Phone | Tablet | Multiple Devices |
| Hacking | 1 | 2 | 3 | 1 | 1 |
| Phishing | 3 | 8 | 2 | 3 | 0 |
| Multiple Victimisation | 1 | 1 | 4 | 2 | 0 |

**Free Public Wi-Fi Usage**

As previously discussed, free public Wi-Fi usage dramatically increased with the introduction of smartphones (Bulchand-Gidumal et al., 2011; Lambert et al., 2018). The risk of using free public Wi-Fi on the chance of identity theft has been documented by many authors

(Noor and Hassan, 2013; Straw, 2013; Watts, 2016). Fraudsters either set up their own fake Internet hotspots, namely rogue access points, on public places (Check Point, 2014; Norton, 2017) or interfere unsecured networks to access poorly protected devices (Hoffman, 2014; Kaspersky, 2017) . Up to date, cybercrime studies neglected the impact of free public Wi-Fi usage on the risk of becoming a victim. This doctoral thesis aimed to discern vulnerabilities posed by free public Wi-Fi usage through victims' and non-victims' accounts.

Interviews indicate that the majority of young Internet user-participants preferred accessing free Wi-Fi offered at public places. While 8 out of 10 young victims (under 30 years old) accessed free Wi-Fi, 3 out of 4 non-victim young participants accessed freely offered public Wi-Fi. There appeared to be a balanced distribution between free Wi-Fi users and non-users for both victims and control group participants for other age groups (Table 7.8).

Table 7.8
*Free Public Wi-Fi Usage*

| Usage | Victim | | | | Non-victim | | | |
|---|---|---|---|---|---|---|---|---|
| | Age Categories | | | | Age Categories | | | |
| | Under 30 | 30-60 | Over 60 | Total | Under 30 | 30-60 | Over 60 | Total |
| Yes | 8 | 7 | 5 | 20 | 3 | 2 | 2 | 7 |
| No | 2 | 5 | 5 | 12 | 1 | 2 | 2 | 5 |

These results indicate that young Internet users felt free to use public Wi-Fi. It seems that they did not perceive public Wi-Fi usage as a cause of identity theft when compared to other age groups.

*"Some of them ask for my email address, and some other ask for the mobile number. I provide these details. I do not worry about it."* (Amelia, 29 years old female victim).

*"I sometimes use free Wi-Fi in an airport or in café. I think they do not ask for very important personal information, so I am not very worried about providing them."* (Tilly, 28 years old female victim).

*"I did try to use McDonald's, but my husband was a little bit suspicious about it. So, I did not use it."* (Isabella, 71 years old female victim).

Although public Wi-Fi usage was common among Internet users, only two participants reported free Wi-Fi usage as a possible explanation of experiencing economic cybercrime victimisation. This outcome may be attributed to the fact that those who steal personal information and those who use stolen information are different individuals, and financial loss may occur long after personal or financial information loss (Ablon et al., 2014; Wueest, 2015).

*"...However, I accessed my online banking account to transfer money to my father. I used the hotel's Wi-Fi for these transactions. I also used the airport's Wi-Fi, but I do not remember doing any online banking at the airport."* (Harrison, 32 years old male victim).

*"If they hacked my email, they could get my details. So, I think it is because I was using public Wi-Fi that they could hack my email."* (Kian, 33 years old male victim).

Participants were also asked whether they were concerned about submitting their personal information like email address, name or mobile number to be eligible to access free Wi-Fi. Although the majority of free Wi-Fi users were not happy to submit their personal information, it is acknowledged that they yielded the required information as they wanted to access the Internet.

*"They asked me my phone number, my email, my postcode, my full name and it made me very uncomfortable. But I still do it anyway."* (Joshua, 25 years old male victim).

"*I am concerned about providing my information. But if I want to use an application, I have to agree to share some privileges."* (Kyle, 30 years old male control group).

Some participants of them devised survival strategies such as submitting fake details or only using trusted public Wi-Fi's. The majority of Wi-Fi users said that they did not engage with serious things while connected to free hotspots. They tend to limit their online usage to social networking, checking emails and reading newspapers.

*"I provide a fake email address and a fake name to access free Wi-Fi."* (Arthur, 28 years old male, control group).

*"I check my emails, read notifications in my social networking sites."* (Alice, 29 years old female victim).

*"I try not to access my online banking while connected to a public Wi-Fi. I generally do social networking."* (Amelia, 29 years old female victim).

**Mobile Applications**

Mobile applications may be considered as the most significant novelties of smartphones. There can be found a mobile application for nearly any purpose. Online stores like Google Play and Apple Store thrive with many different sorts of mobile applications. It is argued that fraudsters provide freely distributed mobile applications (Gold, 2012) or exploit security breaches of popular applications (Kirk, 2015; Sullivan, 2015) to access Internet users' personal credentials. The impact of mobile application usage on the risk of experiencing cybercrime has not been researched yet. This section of the chapter provides findings pertaining to the risk of victimisation caused by mobile application usage.

The majority of both victim and control group participants used mobile application with their mobile phones or smartphones. Only three victim participants and two control group participants did not use mobile applications as their mobile phones were not smartphones. Although the majority of participants used mobile applications, the source of applications and type of information that applications want to access was the main concerns of smartphone users. Respondents acknowledged that they tended to refuse installation of applications when applications wanted to access information that is not required for their intended use; for instance, a compass application trying to access photos or contact lists.

Interviews appear to suggest that mobile applications impact the risk of victimisation in two ways. It appears that mobile applications can be used to gain money directly from individuals' credit card or bank accounts.

*"I installed a mobile application called "Boss Revolution". It is used to make cheap calls to Egypt. A friend of mine recommended it to me. I installed it, and it asked me to top up money, so I used the application to top up money, which means that I entered my card details into the application... When I checked the application, I saw that I had downloaded another program, which imitates the real one".* (Sophie, 32 years old female victim).

"*I had installed an application called OAS to buy some shoes and clothes. I think this application is not secure; it is a new application. I made the payment through these applications with my PayPal account. So, they could get my PayPal name through this application. Why I am suspicious about this one is that I received an email saying that there is such an application which can be used to buy things for low prices. I installed that application and the incident happened after I created an account through this application."* (Kai, 32 years old male victim).

Moreover, mobile applications may also be used to steal personal information (Ghouzali et al., 2016; Laka and Mazurczyk, 2018). Literature suggests that perpetrators intercept mobile phone users' credentials through mobile applications that have privileges to access the content of mobile phones. These contents can be stored data such as address book or data capturing devices such as a camera or microphone (Balduzzi et al., 2016; Vashisht et al., 2016). Interviews with victims appear to support these studies as most of the victim participants provided privileges to random or non-reputable applications to access their personal information. Only one participant related his victimisation experience to identity theft caused by mobile application usage.

*I was using a mobile app, and I believe that was the reason I might have been hacked.* (Kai, 32 years old male victim).

It appears that victim participants were not really concerned about the security issues of mobile application.

*"I do not read anything. I just accept and install the app."* (Jenna, 37 years old female victim).

*"I do not worry about what type of information these apps want to access. I just install."* (Joy, 45 years old female victim).

Whereas some respondents did not check the type of privileges, mobile applications ask other participants faced a threat to download an application they are after.

*"I never really think about how these apply to me. If it is gonna be a problem. I sometimes do not want to share this information, but I want that app. So, it is like a trade-off."* (Joshua, 25 years old male victim).

"*However, I do not check which type of information they try to access in my mobile phone.*" (Thomas, 26 years old male victim).

**Refund Policy**

The most surprising macro vulnerability that may have increased the odds of victimisation was the banks' refund policy. Interviews indicate that the sense of security provided refund system may affect the security considerations of Internet users.

*"I used some peer to peer sharing programs such as eMule, but I recently use BitTorrent to download French movies as it is difficult to find free French movies. … if I am hacked my bank has to pay it. … I know that the bank is responsible, so I feel quite safe*." (Ruby, 24 years old female victim).

*"I don't go for a specific website. Wherever I find a cheap product, I buy there. … I know that banks cover financial losses caused by online fraud. So, I try to use my credit card rather than a debit card. So, I am pretty more relaxed about using my card to buy things from websites that offer the lowest price."* (Yasmin, 46 years old female, multiple victimisations).

*"It was so easy to have the problem resolved. I was not that careful. I thought that was fine because they refunded me."* (Samuel, 28 years old male, multiple victimisations)

It appears that the perceptions about banks' reimbursement policies decreased perceived severity of economic cybercrime victimisation, which in turn alleviated protection motivation. Those who did not perceive any severe threat were encouraged to engage with risky deviant online behaviours or decreased their vigilance about the credibility of websites. Two participants who felt quite relaxed about their online actions were victimised multiple times. These multiple victimisations may also stem from a sense of security caused by banks' reimbursement policies.

**Security Breaches of Online Traders**

Security breaches of shopping websites appeared to another macro vulnerability that may facilitate victimisation. It seems that fraudsters targeted online traders to acquire personal financial information of their customers.

*"I did order grocery for Tesco. It was about four or five days after grocery had been delivered, my credit card hacked."* (Scarlett, 32 years old female victim).

*"When I talked to somebody from Oxfam. They said it was such a popular thing that Oxfam had to recruit very quickly a lot of people who can access your details. So, my details could have been sold on the third party."* (Isaac, 57 years old male victim).

This section examined the effects of contextual vulnerabilities on the risk of experiencing economic cybercrime victimisation. A contextual vulnerability approach was proposed to increase the explanatory power of LRAT. Findings presented here appear to suggest that contextual vulnerabilities, namely technological, social, personal and macro vulnerabilities increase the odds of becoming a victim of economic cybercrime. Security breaches of electronic devices such as tablets, free Wi-Fi usage and mobile applications appeared to be emerging technological vulnerabilities that may facilitate victimisation. Social and personal vulnerabilities such as sudden and dramatic changes in individuals' lives, desire to buy extraordinary presents seemed to enhance the risk of victimisation. Macro vulnerabilities like data breaches of big companies, banks' reimbursement policies or security deficiencies of online traders appeared to increase the risk of victimisation.

## 7.3 Summary

The primary aim of this was to investigate why and how individuals became victims of economic cybercrime. While the first section of the chapter endeavoured to examine

victimisation process, the second section of the chapter tried to distinguish the effect of Internet users' online activities and the contextual on the risk of experiencing economic cybercrime victimisation.

Phishing victimisation cases were selected to be analysed as phishing victims were more aware of their victimisation process when compared to hacking victims. Email phishing and website phishing victimisation processes were examined separately. While personal involvement, believability cues and fear appeals emerged to be the main reasons for falling victim of phishing attacks, problems with differentiating bogus websites from the legitimate ones appeared to be a risk factor for website phishing.

The aim of the second section of the chapter was to discern the correlates of economic cybercrime victimisation. Normal routine online activities like online shopping, or online banking appeared to have no impact on the risk of victimisation. The data reveals that technological vulnerabilities like free public Wi-Fi usage and mobile applications were risk factors for economic cybercrime victimisation. Social and personal vulnerabilities in individuals' lives also emerged to be risk factors for victimisation. Macro vulnerabilities (i.e. data breaches of big companies), which are beyond Internet users' control, also appeared to be risk factors.

# Chapter 8 Consequences of Economic Cybercrime Victimisation

## 8.1 Introduction

The previous chapter examined the determinants of economic cybercrime victimisation through script analysis of victims' accounts. Personal involvement, fear appeals, naivety and self-efficacy emerged to be the main drives behind disclosing personal information through email or website phishing. Contextual vulnerabilities encompassing social, personal, psychological and technological variables appeared to be other reasons for losing money through the Internet. As was referred to previously, becoming aware of victimisation and dealing with post victimisation effects is the last phase of the victimisation process. Findings pertaining to the impact of victimisation experiences on victims' online lifestyles and protection motivation will be presented. This chapter aims to address the forth of the key research questions: *What are the emotional responses to economic cybercrime victimisation and how these emotional responses impact victims' behavioural and security intentions?*

The post-victimisation phase of phishing victimisation will be evaluated together with hacking victimisation in order to examine the impact of economic cybercrime victimisation on individuals holistically. The Cyber Victimisation Coping Model (Figure 8.1) will be utilised to analyse and understand changes in victims' online life-styles after experiencing economic cybercrime victimisation. This unique model was generated during the Pilot Study phase specifically created for this research. The model is the combination of Protection Motivation Theory (Rogers, 1975; Maddux and Rogers, 1983; Prentice-Dunn and Rogers, 1986) and Coping Adoption Approach Paradigm (Lazarus, 1980; Lazarus and Folkman, 1984).

This thesis evaluates cybercrime victims' survival strategies through lenses of Protection Motivation Theory and Approach-Avoidance Coping Paradigm. PMT proposes that when individuals face a threat, they assess the situation through threat and coping appraisals (Rogers, 1975, 1983). While perceived severity and perceived vulnerability elements are the subsets of threat appraisal, where individuals assess the extent of damage to be experienced; perceived self-efficacy and response efficacy are a subset of coping appraisal. Later reward or benefit concepts were included in the theory to account for motivations behind protection decisions (Shillair et al., 2015; Thompson et al., 2017).

The coping approach paradigm posits that individuals either implement an approach or avoidance strategy after threat and coping appraisals (Lazarus and Folkman, 1984, Roth and Cohen, 1986). Whereas individuals adopting approach strategies implement actions or security measures to overcome the negative impact of the situation, those who adopt avoidance behaviour either do not carry out any protective measures and prefer facing the outcomes of the threat or stop carrying out the task (Arachchilage and Love, 2014; Wang et al., 2017).

Lazarus and Folkman (1984) conceptualise approach coping and avoidance coping strategies as problem-oriented and emotion-oriented coping strategies respectively. While problem-oriented coping strategies cover active solutions to the problems faced, emotion-oriented coping strategies entails passive actions like distancing from the problem (Herman-Stabl et al., 1995). As these terms denote similar concepts and approach-avoidance divide is more common in literature, this thesis follows approach coping and avoidance coping terminology to refer to coping strategies of cybercrime victims. Another concept that will be scrutinised is the active-passive divide in avoidance coping strategies. Whereas passive avoidance denotes ignoring or escaping from the problem, active avoidance refers to stop doing the action to overcome the problem (Piko, 2001).

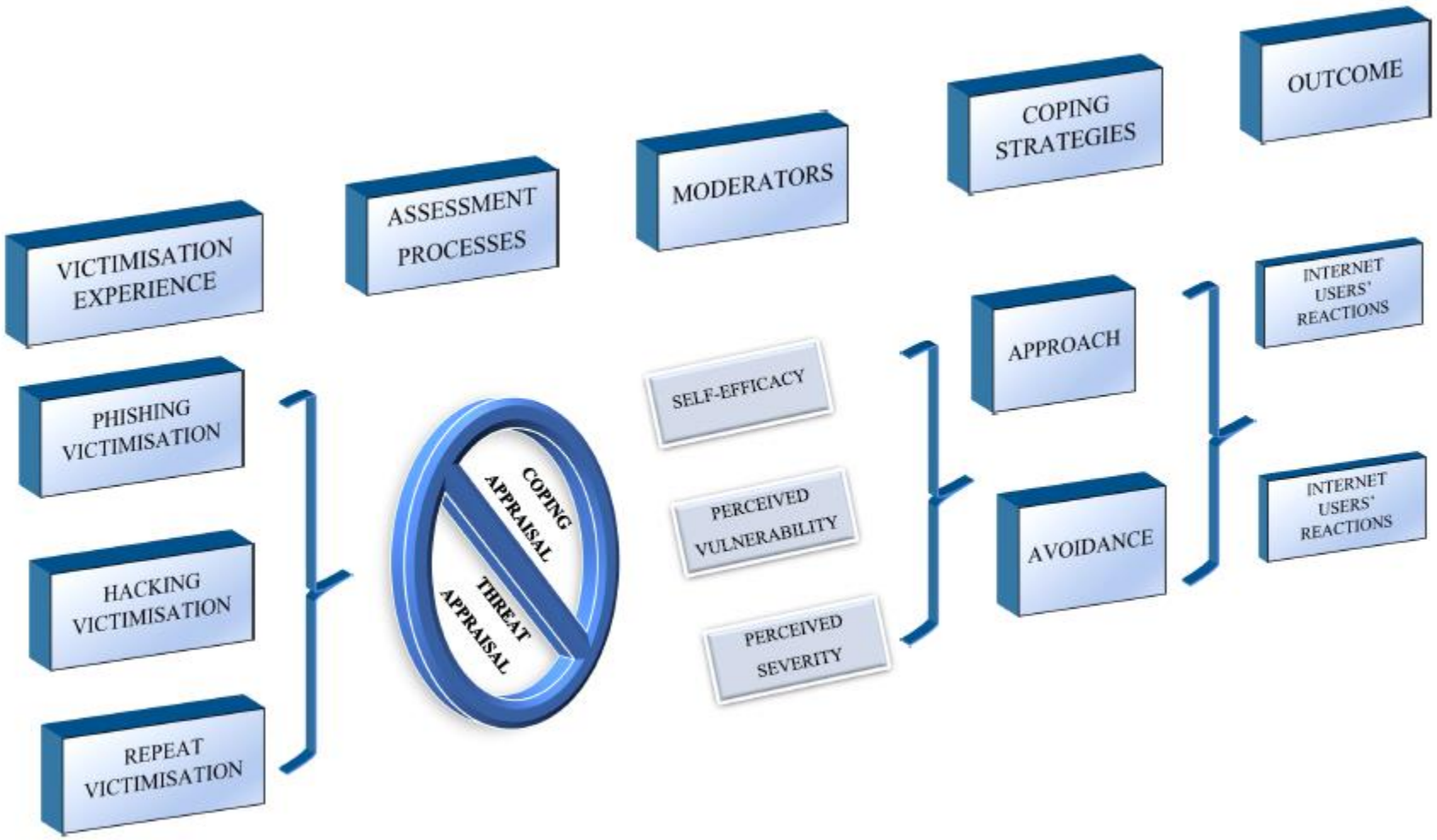



Figure 8.1: *Cyber Victimisation Coping Model*

## 8.2 Psychological Effects of Victimisation Experience

Past research has found that white-collar crime or fraud victimisation experiences may have similar long-lasting effects such as anxiety and depressive disorder on individuals when compared to violent or property crimes (Ganzini et al., 1990; Titus et al., 1995; Piquero et al., 2007). The findings of this research indicated that anger, stress, annoyance, self-blaming, embarrassment, worry and feeling vulnerable were the common themes that participants initially experienced. Victims' accounts are presented here to exemplify their feelings while providing a flow of reading.

### 8.2.1 Emotional Responses

It appears that shock was the primary feelings that victims experienced just after becoming aware of victimisation. Most victims were shocked as victimisation was something unexpected and they were usually informed about the situation while they were carrying out ordinary things such as shopping, reading emails or checking bank statements.

*"... but it left me very shocked because you try to work out how this could have happened."* (Poppy, 66 years old female victim).

*"... I was a little bit shocked for a couple of minutes."* (Chole, 62 years old female victim).

Primary feelings of shock were replaced with panic as most respondents did not know what to do or how to resolve the problem. Banks' customer services appeared to be the first place to contact to deal with the situation.

*"So, I was pretty panicked about it."* (Joshua, 25 years old male victim).

*"I was very angry. Somebody is making a lot of money because of our ignorance."* (Florence, 75 years old female victim).

Most respondents found the victimisation experiences stressful and annoying as they had faced some financial and social hardship following the victimisation since banks immediately cancelled their bank cards or victims lost a great deal of their savings. This finding is in line with past empirical studies researching the impact of physical world crimes such as burglary (Farrall et al., 2006), identity fraud (Dinisman and Moroz, 2017), stalking victimisation (Korkodeilou, 2017), cyberbullying (Li, 2005; DeHue et al., 2008; Dredge et al., 2014). While some respondents tried to survive with what was left behind, others tried to borrow some money from their family members, which they found to be embarrassing and annoying. Loss of time while engaging with some activities such as restoring accounts, changing passwords and contacting consumer services, banks or police emerged to be another source of frustration.

*"I was really stressed at that time since they took a great deal of money from my account. My bank also cancelled my debit card, so it caused me unease since it happened just before my daughter's birthday. I wanted to buy something for her. It was nearly all of my saving."* (Alice, 29 years old female victim).

*"So, it was a case of how I am going to get food. … I could not go out since I did not have money and it was very boring staying at home all the time as they stole all my spare money. It was a little bit depressing."* (Joshua, 25 years old male victim).

*"I had to borrow money from my relatives, which was really annoying."* (Harrison, 32 years old male victim).

*"I think email hacking was the most stressing one since the hacker contacted my friends, my teachers etc. So, it was really embarrassing. It was also very time consuming as I had to restore my account and I need to contact all people to explain the situation."* (Sophie, 32 years old female, multiple victimisations).

*"Obviously I lost a lot of time. It just worsened my situation."* (Parker, 63 years old male victim).

It appeared that victims' psychological moods were affected by the type of victimisation experiences. Whereas phishing victims blamed themselves as they provided information to fraudsters, hacking victims worried about repeat victimisation.

*"It was really embarrassing as it happened to me twice. ... I know that it was my mistake. I should not believe them."* (Alastair, 28 years old male victim).

*"...feel guilty believing that it must be something that you have done that caused it. ... I thought it must have been something that I did or didn't do; it's a very uncomfortable feeling."* (Poppy, 66 years old female victim).

*"...When you are online, you think everything is safe; everything is under control. But when you are hacked you see that you are always vulnerable. You do not know; you will be targeted again."* (Matthew, 33 years old male victim).

Hacking victims' worries about repeat victimisation appeared to stem from the uncertainty of victims' victimisation process. Most hacking victims were concerned about being pursued online.

*"I am pretty much concerned about being a victim again. I am not sure whether all these incidents were connected, or they happened on separate occasions. So, it is a strange feeling whether somebody pursues me in the online environment."* (Sophie, 32 years old).

"*I was quite depressed after the first one. It was really upsetting as they got all my personal details such as date of birth. I felt quite violated. I become a little bit paranoiac. I began to think what else are they trying to do now? They commit other crimes. I do not know who they are?*" (Yasmin, 46 years old female victim).

Worries related to possible outcomes of victimisation experiences seemed to vary according to financial condition and status of victims. Victims with low income were mainly concerned about receiving reimbursement for their loss.

*"I was really stressed at that time since they took a great deal of money from my account."* (Alice, 27 years old female victim).

*"I was very concerned. I did not have a huge amount of money. It was quite disturbing, you feel in a way like vulnerable, you feel like somebody has invaded your privacy and taken your money. You feel personally vulnerable and upset."* (Samuel, 28 years old male victim).

Victim participants who had a well-paid job or prosperous career worried about possible misuse of their personal and financial details.

*"But it was a little bit creepy that somebody could have had my details, my number and could have used that to purchase something bad. Because it could damage your reputation depending on what they bought."* (Mia, 29 years old female victim).

*"I am also concerned that they may sell my details to other offenders who may use it create new identities."* (Yasmin, 46 years old female victim).

*"I think it is very scary because people always concern about privacy. But if it was something more, such as people accessing private pictures, private emails or my work, it would be quite serious. It might jeopardise my career. I think it made aware of danger so, I stopped doing stupid things online."* (Alisa, 28 years old female).

### 8.2.2 Fear of Crime

This next section of the chapter will examine the impact of victimisation experience on victims' fear of repeat victimisation and fear of crime among non-victim participants. Garofalo (1981, p. 840) defines fear of crime as a *"sense of danger and anxiety produced by the threat of physical harm"*. However, results of previous fear of traditional crime research indicate that not only threat of physical harm but also the threat of financial harm do produce negative emotional responses (Ferraro, 1995; Hale, 1996). Analysis of semi-structured interviews with victim participants appears to support these results.

Interviews with victims suggested the existence of a slight gender and age difference with regards to fear of repeat victimisation (Table 8.1). While nine out of seventeen female participants acknowledged that they were worried to be victimised again, less than half of male participants (eight out of fifteen) worried about repeat victimisation. Empirical studies examining fear of crime also suggest that females are more worried about being subject of a crime when compared to males (May et al., 2010; Snedker, 2015; Ryder et al., 2016). Age emerged to be another difference among victims with regards to fear of repeat victimisation. Interviews indicated that whereas seven out of ten elderly victim participants were worried about repeat victimisation, figures for young and middle age groups emerged to be very close. This finding is in line with past empirical studies indicating that elderly people are more worried about becoming a victim of a crime (Abdullah et al., 2014; Serfaty et al., 2016; Greve et al., 2017). This age difference appeared to stem from a lack of knowledge about online

threats. Most elderly victims admitted that their Internet skills were very poor, and they got help from their relatives or friends. Hence, such negative experiences combined with lack of knowledge appeared to trigger fear of repeat victimisation.

Table 8.1:
*Fear of Economic Cybercrime*

| | **Worried** | |
|---|---|---|
| | **No** | **Yes** |
| **Type of Victimisation** | | |
| Hacking | 3 | 5 |
| Phishing | 10 | 6 |
| Multiple | 2 | 6 |
| **Control Group** | 5 | 7 |
| **Gender** | | |
| Male | 8 | 7 |
| Female | 8 | 9 |
| **Age** | | |
| Under 30 | 6 | 4 |
| Between 30-60 | 5 | 7 |
| Over 60 | 3 | 7 |

*"I am worried about it. It is because I am computer ignorant. … I did not know about Internet-related crimes but since I moved here, the manager, Barbara, gives us advice about these things."* (Jenson, 73 years old male victim).

*"What I did afterwards, the chap living next door was good with computers. He took it back to a time before the contact with them. I was lucky that he was there."* (Jamie, 76 years old male victim).

The type of victimisation experience also appeared to influence victims' fear of repeat victimisation. Hacking victims and those who were victimised multiple times appeared to be more concerned about repeat victimisation.

*"You feel vulnerable and guilty, stupid. … When you are online, you think everything is safe; everything is under control. But when you are hacked you see that you are always vulnerable. You do not know; you may be targeted again."* (Matthew, 33 years old male victim).

*I am feeling really paranoid. I could not sleep well these days.* (Yasmin, 46 years old female victim).

*Yes, I am very worried about being a victim again as I feel vulnerable. It seems like quite bad luck, so I am expecting to happen again.* (Joshua, 25 years old male victim).

The possibility of being targeted personally emerged to be a factor affecting the level of worry among victims. It appears that when the victims felt that they were intentionally targeted personally, they got worried about repeat victimisation. Those who consider their situation as a coincidence such as being at the wrong website at the wrong time appeared to be less concerned about repeat victimisation.

*"I do not feel it as a personal attack. It was not just worrying. (Isaac, 57 years old male victim).*

*"I do not think they personally targeted me. It was my card. I think it was bad luck. (Ruby, 24 years old female victim).*

This first section of the chapter examined the psychological effects of economic cybercrime victimisation. Annoyance and stress were experienced after the feelings of shock

and anger since victims began to deal with the post-effects of victimisation such as cancelling bank cards or restoring accounts. Victims' psychological conditions seem to be mainly affected by the type of economic cybercrime victimisation faced. While phishing victims mainly felt embarrassed and guilty as they themselves somehow provided their financial details to fraudsters, victims of hacking were more concerned about future repeat victimisation. Worries also seemed to be varied according to the financial conditions of victims. Whereas those with low income were worried about getting refunds, those who had a well-paid job or promising career were worried about possible misuse of their personal and financial information. This next section of the chapter aims to address the question of whether past victimisation experiences had an impact on victims' Internet usage as well as online security behaviours.

## 8.3 Impact of Victimisation on Internet Users' Online Lifestyles

Studies researching the effects of cybercrime victimisation on individuals suggest that cyber victimisation experiences affected Internet users' security behaviour as well as Internet usage habits (Henson, 2011; Henson et al., 2013; Roberts et al., 2013; Riek et al., 2014; Riek et al., 2016). While cybercrime studies conducted by Henson (2011) and Henson et al. (2013) researched the impact of cyber interpersonal victimisation experiences, namely cyberstalking, on individuals' online lifestyles, Roberts et al. (2013) examined the effect of online identity theft on the Internet users' online behaviours. Riek et al. (2014) and Riek et al. (2016) did not focus on a specific type of cybercrime. They researched the impact of cybercrime victimisation on Internet users' online shopping and online banking usage. These mentioned cybercrime studies did not utilise coping approach paradigm (Lazarus and Folkman, 1984; Roth and Cohen, 1986) as a theoretical framework. Generally cyberbullying studies (Price and Dalgleish, 2010; Šléglová and Cerna, 2011; Machmutow et al., 2012; Parris et al., 2012; Machackova et al., 2013) used coping approach paradigm to evaluate the impact of cyberbullying victimisation

on youngsters' behavioural adaptations. Although limiting the sampling universe to college students was the main pitfall of these studies, they introduced a coping approach paradigm to cyber victimisation literature.

Only a handful of studies have researched how privacy concerns as well as negative online experiences such as being a spam victim (Chen et al., 2016), a scam victim (Tsai et al., 2016; Chen et al., 2017) and online identity theft victim (Chen et al., 2016) shapes Internet users' coping strategies. Those studies utilised quantitative analysis methods to investigate the impact of prior victimisation on coping strategy adoption. These studies also did not examine the effects of different victimisation experiences on protection motivation and coping strategy adoption. To address this important gap in the data available, the Protection Motivation Theory and coping approach paradigms (Lazarus and Folkman, 1984; Roth and Cohen, 1986) were utilised as a theoretical framework to evaluate the impact of economic cybercrime victimisation on Internet users' behavioural adaptation and security measures, namely coping strategies. Hence, this research will be one of the first attempts to critically investigate the impact of previous victimisation experiences on protection motivation and coping strategy adoption through qualitative analysis of semi-structured interviews.

Lazarus and Folkman (1984) argue that individuals conduct two types of cognitive appraisals when they face an undesired situation: threat and coping appraisals. Initially, the impact of initial threat assessment on Internet users' online lifestyles and protection motivation, which takes places just after realising victimisation, will be examined and after that, the effects of consecutive coping appraisals will be evaluated.

### 8.3.1 Initial Threat Appraisal

As it was documented in the previous section of this chapter, individuals became aware of their victimisation while they were engaging with ordinary daily activities. Sudden

unexpected news about the loss of money caused a feeling of panic and need to search for help or clarify the situation. Hence, the initial threat appraisals were centred around survival strategies like contacting the bank or financial institution and minimising financial damage.

*"I called my bank and told them about the situation, and then I sent an email to PayPal about it."* (Tilly, 28 years old female).

*"I panicked. I directly went to the bank."* (Harrison, 32 years old male).

*"I immediately called my bank to cancel it. They cancelled my debit card.* (Alastair, 28 years old male).

*"I think after that immediately happens, you are much more aware. But then quite quickly you relax again."* (Samuel, 28 years old male).

Interviews with victim participants suggested that decisions based on initial assessment process did not have any long-lasting impact on victims' online life-styles or protection motivation as they mostly implemented precautions taken to alleviate the initial shock of victimisation experience. Interviews illustrated that all participants devised approach coping strategies like contacting consumer services of credit card providers or e-wallet operators to cancel their bank cards. Changing online account passwords was another approach coping strategy adopted. These approach coping strategies were implemented as short term precautions. Data collected suggest that it is the consecutive assessment process that impacted victims' online lifestyles mostly.

### 8.3.2 Consecutive Coping Appraisals

Interviews suggested that victims conducted consecutive coping appraisals to thwart the imminent threat of financial loss after initial threat assessments. The type of victimisation

appeared to impact victims' consecutive coping assessment processes. For that reason, findings pertaining to phishing, hacking and repeat victims' coping appraisals will be introduced separately.

**Phishing Victims**

Participants were asked about their perceptions with regards to their victimisation experiences and whether their victimisation experiences had an impact on their security intentions as well as their online lifestyles, to understand the behavioural impacts of victimisation experiences. Analysis of the interviews suggested that there was an age difference in phishing victims' perception of their victimisation. Hence, an analysis of interviews conducted with young and middle age participants will be presented, before introducing the analysis of interviews with elderly participants.

It appears that young and middle age phishing victims neither perceived any serious threat nor felt vulnerable to repeat victimisation (Table 8.1). This finding may be attributed two facts: being aware of their mistakes that facilitated victimisation (perceived vulnerability) and the relatively small amounts of money that were lost as a consequence of their victimisation (perceived severity). Only one victim who was coerced to yield financial information through a pop-up message accusing the victim with accessing illegal adult content perceived his situation as severe. The study conducted by Downs et al. (2007) also indicated that phishing victims perceived their victimisation experiences less severe. Their studies suggested that perceived severity of consequences of victimisation did not impact victims' behavioural adaptations. Findings of this thesis, however, indicate that young phishing victims' security intentions were affected by their victimisation experiences.

Young and middle age phishing victims mostly adopted approach coping strategies to avoid repeat victimisation. While website phishing victims changed their shopping website

preferences, email phishing victims increased their guardianship measures. *Reading emails more carefully, using anti-virus programs, using complex passwords* or *checking transactions more frequently* were the most cited approach coping strategies. A study conducted by Arachchilage and Love (2014) found that skilled Internet users adopted problem-focused (approach) coping strategies to prevent phishing victimisation.

Table 8.1:
*Coping Strategy Adaption for Email Phishing Victims*

| Victim | Victimisation Experience | Consecutive Assessment (Coping Appraisal) | Coping Strategy | Action |
|---|---|---|---|---|
| Amelia<br>29 years old female | Email Phishing | **Perceived Vulnerability**<br><br>I am not very worried about being victim again. So it happens many people who are more Internet conscious<br><br>**Perceived Severity**<br><br>I do not consider my situation as something big when compared to other colleagues who had similar issues. | Approach | I would say I am more conscious. I read emails more carefully |
| Alice<br>29 years old femal | Email Phishing | **Perceived Vulnerability**<br><br>I think it happened to me because of my own fault. I did not have an anti-virus program before victimisation. I did not think about security issues before becoming victim.<br>It was all my fault. | Approach | I shop online as before the victimisation but I am more cautious about security issues and I installed an anti-virus program. I check my bank transactions more frequently than before. I use more complex passwords for my accounts. |
| Thomas<br>26 years old male | Website Phishing | **Perceived Severity**<br><br>It was really shocking. Because they showed me many hidden files containing child pornography. I was fairly scared.<br><br>**Perceived Vulnerability**<br><br>I know that it was my mistake to believe them. | Approach | I am very security conscious these days. I only use well-known legitimate websites. I avoid shopping from random websites. |
| Isaac<br>57 years old male | Website Phishing | **Perceived Vulnerability**<br><br>I do not feel it as a personal attack. It was not just worrying. What I have learned is that we do not have an Internet security. I realised that nothing is secure. | Approach | I am more careful about website and more careful about details that I give.<br><br>We did not shop for a while on the Internet then we were back again |

Interviews with elderly participants suggest that elderly Internet users who perceived low Internet self-efficacy tended to adopt active avoidance coping strategies for online activities like online shopping to prevent further victimisation. Yet, they adopted approach coping strategies for Internet banking. This means that while those elderly Internet users stopped shopping online, they increased vigilance for their online banking accounts (Table 8.2 Florence, 75 and Rosie, 78). This finding is significant in differentiating different impacts of self-efficacy on individuals' Internet usage. Past research focusing on the effect of self-efficacy on security behaviour indicated that self-efficacy was associated with approach coping strategies like anti-spyware usage Liang and Xue (2010) and applying computer security measures (Mwagwabi et al., 2014; Thompson et al., 2017). Other studies (Lai et al., 2012; Vance et al., 2013) found that self-efficacy enhanced security intentions, however, Tsai et al. (2016) found that high self-efficacy decreased security intentions.

The straighfoward interface of Internet banking websites may be an explanation for the findings of this thesis with regards to online behaviour adoption. Accessing a legitimate online shopping website and shopping over there would be more challenging for the elderly Internet users since interfaces of online shopping websites greatly vary. There are also many different steps that need to be implemented to shop online. Hawthorn (2007) argues that elderly people limit the number of technology-based tasks to minimise risks. Similarly, Rousseau and Rogers (1998) researching computer usage patterns of elderly people found that elderly people intentionally used a limited number and easy to use programs to diminish errors.

Availability of physical shops and banking branches may be another explanation for elderly participants' application of active avoidance and approach coping strategies. Elderly individuals may not have difficulties in shopping in the physical world as there are many local shops, whereas accessing a branch of a bank would be a more daunting job for them due to the

scarcity of bank branches. This may indicate that it would be easier to change online habits if there are physical world substitutes for them.

Elderly participants who perceived low vulnerability adopted passive avoidance strategies for online services like playing online games or contacting friends and family members over social media. This means that victimisation experience did not impact their online social usage. This might be attributed to the fact that they experienced financial loss and the aforementioned online activities may not pose a risk for personal financial information.

Elderly participants who perceived themselves as vulnerable and perceived their victimisation experiences as severe appeared to adopt approach coping strategies such as increasing online guardianship measures, changing online passwords or using trusted online merchants (Table 8.2, Poppy,66 and Jamie,76). This finding suggests that more computer savvy elderly Internet users who perceived themselves vulnerable and perceived possible consequences of victimisation as severe tended to implement guardianship measures rather than changing their online lifestyles to diminish their risk of victimisation. Moreover, it appears that elderly Internet users made a threat assessment according to the type of online activities. While they continued accessing non-financial online activities, which they did not perceive as a threat, they increased safeguarding measures for financially risk online activities (Table 8.2, Florence).

Table 8.2:
*Coping Strategy Adaption for Elderly Phishing Victims*

| Victim | Victimisation Experience | Consecutive Assessment (Coping Appraisal) | Coping Strategy | Action |
|---|---|---|---|---|
| Florence<br>75 years old female | Website Phishing | **Self Efficacy**<br><br>I am not very good at using the Internet.<br><br>My daughter told me that I should look at the end of address line and it should end with gov. But I did not know that. | Approach | I try to use it as least as possible. I just check the bank account to make sure that everything is paid and nobody touched money. |
| | | | Active Avoidance | I am now very aware of these issues so I never buy anything online. |
| | | | Passive Avoidance | I look at my email and I talk to my friends in America and I look at the bank statements. |
| Rosie<br>78 years old female | Website Phishing | **Self Efficacy**<br><br>I wanted to check my online banking statement and I opened Barclay's website. Then a pop up appeared on the screen. It was an online survey. I filled it and put my bank details on it. But obviously it was another thing. | Passive Avoidance | I still use Internet for online banking and playing online games. |
| | | | Active Avoidance | I do not shop online. |
| Poppy<br>66 years old female | Website Phishing | **Perceived Vulnerability**<br><br>It's an odd feeling not knowing who, or how they got the information.<br><br>I feel the sense of mistrust never quite leaves you. | Approach | I only shop on sites that I trust (even then I feel as if I'm taking a chance),<br><br>I never give genuine information about myself when asked,<br><br>I regularly change my date of birth (unless it's an official site – or this questionnaire),<br><br>If I've made a purchase on line I check my bank statements more regularly.<br><br>I change my passwords so many times that I lose track! |
| Jamie<br>76 years old male | Website Phishing | **Perceived Severity**<br>Because it was a court case against me, they have been knocking on my door. It was an awful experience actually.<br><br>I did not report it to police. I just felt that if I did not pay they would continue to harass me, until they got it. | Approach | I am fairly careful. When I go online I make sure that I am on the right site these days. |

**Hacking Victims**

It appears that hacking victimisation experiences impacted victims' perceived vulnerability and perceived severity when compared to phishing victims. Interviews indicated that hacking victims were more concerned about privacy issues and the risk of repeat victimisation when compared to phishing victims. Having very little information about their victimisation process when compared to phishing victims may be an explanation for increased perceived severity among hacking victims.

Hacking victims who did not consider the financial loss as a matter since their banks refunded their money did not perceive their situation as severe. Hence they adopted passive avoidance coping strategies, which means that they neither changed their online behaviours nor adopted security measures to prevent further victimisation (Table, 8.3, Alisa, 28; Ruby, 24). Female participant (Mia, 29) with a high level of perceived severity adopted active avoidance coping like stopping checking Internet banking.

Those who perceived themselves vulnerable to online threats adopted approach coping strategies (Table, 8.3, Mia, 29; Tilly, 28). *Using complex passwords*, *installing anti-virus programs, limiting shared information through social media*, and *checking bank statements regularly* were examples of approach coping strategies. This result is in line with Mwagwabi et al. (2014) who found that password related hacking experiences were linked to perceived vulnerability. Their findings, however, suggested that it was perceived severity that triggered security intentions rather than perceived vulnerability. Similarly, a study conducted by Thompson et al. (2017) demonstrated that previous security breach experiences increased the feeling of vulnerability among computer users.

As can also be seen from the Table 8.3, hacking victims who were mainly young Internet users either neglected their situation (passive avoidance strategy) or implemented security measures (approach strategy) to prevent future victimisation. However, it appears that they did not stop using the Internet, but they limited the scope of their online lifestyles. From the data collected it is evident that the Internet has become an integral part of young or middle-aged individuals; hence, regardless of their severity and vulnerability perceptions, they keep accessing the Internet for less risky services. Yet, when it comes to access riskier services, it appears that those with high perceived severity refrained themselves using online financial services.

Table 8.3:
*Coping Strategy Adaption for Hacking Victims*

| Victim | Victimisation Experience | Consecutive Assessment (Coping Appraisal) | Coping Strategy | Action |
|---|---|---|---|---|
| Alisa<br>28 years old female | Hacking | **Low Perceived Severity**<br>Actually I did not lose too much money but it could be something more serious, which made me more cautious.<br>To be sincere, I did not lose anything. I received my money back. But if it was something more, such as people accessing private pictures, private emails or my work, it would be quite serious. It might jeopardise my career. | **Passive Avoidance** | I am more conscious but it did not change my online behaviours or security measures. |
| Ruby<br>24 years old female | Hacking | **Low Perceived Severity**<br>I am not worried because I know that if I am hacked my bank has to pay it.<br>I know that bank is responsible so I feel quite safe. | **Passive Avoidance** | So nothing has changed.<br>I have not changed my security measures as well. |
| Mia<br>29 years old female | Hacking | **High Perceived Severity**<br>But it was a little bit creepy that somebody could have had my details my number and could have used that to purchase something bad. Because it could damage your reputation depending on what they bought. | **Active Avoidance** | My Internet usage decreased but it decreased in a sense that I did not stop using the Internet but I certainly stopped checking my Internet banking. |
| | | **High Perceived Vulnerability**<br>You know, you feel a little bit insecure as somebody managed to break through all these security measures you put to safeguard yourself. And still managed to steal money off you and got away with it. | **Approach** | I use different passwords, and I try to make them as complex as possible. I have also anti-virus program McAfee. I scan my computer regularly. I don't put private stuff on Facebook. |
| Tilly<br>28 years old female | Hacking | **High Perceived Vulnerability**<br>I feel very vulnerable. The feeling of being cheated by someone was also another issue. | **Approach** | I check my credit card statement frequently.<br>I still use Internet and online shopping. |

**Repeat Victimisation**

It appears that the type of victimisation experienced repeatedly impacted upon victims' perceived vulnerability and severity assessment. While a participant who faced phishing victimisation more than once did not perceive himself as vulnerable (Table 8.4 Alastair, 28), participants who were hacked multiple times felt vulnerable to threats and perceived their cases as severe due to privacy concerns and likelihood of personal information misuse (Table 8.4, Joshua, 25; Samuel, 28; Yasmin, 46). Interestingly, both groups of participants adopted passive avoidance strategies, which means that they neither changed their online habits nor implemented any safeguarding measure. This might be one of the reasons for their repeat victimisation. They might have faced repeat victimisation as they kept making the same mistakes. It could be a sense of inability to repel online threats, which made them adopt passive avoidance coping strategies.

Female participant (Yasmin, 46) who experienced website phishing and hacking victimisation perceived a low level of severity due to a refund policy, perceived a high level of vulnerability due to possible misuse of personal details. Hence, while she adopted the passive coping strategy, which literally means she did not change her online shopping preferences to prevent victimisation, she adopted approach coping strategy (registering with a credit agency) to prevent loss of financial details.

Table 8.4:
*Coping Strategy Adaption for Repeat Victims*

| Victim | Victimisation Experience | Consecutive Assessment (Coping Appraisal) | Coping Strategy | Action |
|---|---|---|---|---|
| Alastair<br>28 years old male | Repeat Victimisation<br>Phishing and Phishing | **Low Perceived Vulnerability**<br>There is always back doors so I am not so concerned.<br>I know that it was my mistake. I should not believe them. | **Passive Avoidance** | I am more security cautious but my Internet usage has not changed. |
| Joshua<br>25 years old | Repeat Victimisation<br>Hacking and Hacking | **High Perceived Vulnerability**<br>It was quiet distressing if you do not know if it will gonna happen again.<br>After the second incident, I was worried if it was the same person or do they know all thing I am doing.<br>I am very worried about being victim again as I feel vulnerable.<br>**Perceived Severity**<br>It was not really about money since they took small amount of money, it was like if somebody got the information, they could use it for something bigger.<br>**Self Efficacy**<br>I have no idea how to be safer. Do I need change all my passwords? I feel like there is a lack of common knowledge about it. | **Passive Avoidance** | I did not change any of passwords. I know I should but I think I am a little bit lazy about it.<br>In terms of changing online habits, no I don't think that I have change my online habits. |
| Samuel<br>28 years old male | Repeat Victimisation<br>Hacking and Hacking | **Perceived Severity**<br>So it was quite stressful in both times. You do feel the invasion of your privacy and that combined with loss of money. You know, you are not that sure. Especially, the first time, you do not have any idea, whether you can get your money back. It was quiet worrying. | **Passive Avoidance** | Honestly it has not changed that much. But I become a bit more aware and a bit more careful.<br>In truth, I am not as careful as I should be. Even I have experienced the fraud.<br>I felt like I have not done enough to prevent. I felt like I could have done more and more secure. |
| Yasmin<br>46 years old female | Repeat Victimisation<br>Website Phishing and Hacking | **Perceived Severity**<br>I sometimes worry about it but I know that banks cover financial loses caused by online fraud.<br>So I am pretty more relaxed about using my card to buy things from websites that offer cheapest price. | **Passive Avoidance** | As I mostly use my work computer for online shopping and online banking I do not have any security programme such as anti-virus etc. |
| | | **Perceived Severity**<br>It was really upsetting as they got all my personal details such as date of birth. I felt quite violated. I become a little bit paranoiac. I began to think what else are they trying to do now? They commit other crimes. I do not know who they are? I am also concerned that they may sell my details to other offenders who may use it create new identities. | **Approach** | I have registered with one of these credit agencies. So I thought I could track my financial history. |

This section of the chapter has investigated the extent to which prior economic cybercrime victimisation experience impacted victims' coping strategy adoption. After an initial analysis of the pilot study, The Cyber Victimisation Coping Model was created. This unique model which is the integration of Protection Motivation Theory and Approach-Avoidance Paradigm was designed to assess or predict the impact of victimisation on individuals' threat and coping appraisals procedures, which leads individual either apply an approach or avoidance strategy. Figure 8.2 illustrates the coping strategy adoption of cybercrime victims.

Analysis of interviews with victims indicated that the type of victimisation experienced impacted victims' appraisal processes. This finding is significant in that no previous research has distinguished the impact of difference cybercrime victimisation on behavioural and security adaptations. The model has shown that Protection Motivation Theory elements like perceived vulnerability, perceived severity and self-efficacy had a moderating effect on coping appraisal process, which in turn affects coping strategy adoption to prevent future victimisation. Based on the findings of this section, the Integrated model of Cyber Victimisation Coping Model has been finalised (Figure, 8.2).

Firstly, it appears that victims conducted initial threat appraisal to understand the extent of the problem faced. Victims usually contacted the bank or financial institutions to diminish financial loss and possible repeat victimisation. It seems that this phase of assessment does not have any long-lasting impact on victims' behavioural adaptation or security intention.

After the initial threat assessment, victims appeared to conduct coping appraisal process, which is mainly affected by PMT constructs like perceived vulnerability, perceived severity and self-efficacy. With regards to phishing victimisation experience, there appears to be an age difference in victims' behavioural adaptation and security intention. Young and

middle-aged Internet users who neither perceived themselves vulnerable nor perceived their situation as severe adopted approach coping strategies like increasing online safeguarding measures and changing website preferences. Elderly cybercrime victims with low self-efficacy either implemented active avoidance strategies like stopping using the Internet or adopted approach coping strategies like enhancing online security measures. Moreover, while elderly individuals with low perceived vulnerability adopted passive avoidance strategy such as to keep using the Internet as before the victimisation, those with high perceived vulnerability implemented approach coping strategies like enhanced online safeguarding.

With regards to hacking victims, there appeared to be no age difference in their behavioural response to victimisation experiences. Uncertainty about the extent of personal information lost and victimisation processes appeared to increase the perceived vulnerability of hacking victims. It seems that victims were concerned whether loss of personal information was limited to financial, personal information loss or it was extended to private personal information, which may be used to jeopardize their careers. Hacking victims were not aware of factors leading them to victimisation they were concerned about repeat victimisation. The feeling of being pursued appeared to increase perceived vulnerability.

It seems that hacking victims who felt vulnerable to future attacks applied approach coping strategies. Using complex passwords, installing anti-virus programs and checking bank statements were the most cited approach coping strategies adopted. This finding is in line with Kim and Kim (2016) who found that Internet users feeling vulnerable to identity theft were more likely to use identity theft prevention services. Similarly, Youn (2005) find that college students with high perceived vulnerability were less likely to disclose personal information. the results of Jansen and van Schaik (2016) indicate that Dutch online banking users who felt

vulnerable to victimisation did not apply any approach strategy to be secure. Phishing victims who did not consider themselves vulnerable also adopted approach strategies.

Some hacking victims who did not perceive their situation as severe adopted passive avoidance strategies, which means that they did not change either their security measures or Internet habits. This finding complies with Kim and Kim (2016) who found that Internet users who perceived the consequences of online identity victimisation as severe did not use any protection services. Correspondingly, Claar and Johnson (2012) investigating home computer users' behavioural adaptations to use computer security software found a negative relationship between perceived severity and computer security software usage. Those who perceived possible outcomes of victimisation as severe were less likely to install computer security software. Yet, Tsai et al. (2016) who researched predictors of online safety intentions found that perceived severity was positively correlated with security intentions.

Lastly, repeat victims displayed similar characteristics with phishing and hacking victims. Whereas repeat phishing victims did not feel vulnerable to online threats, repeat hacking victims felt vulnerable and perceived their case as severe. The feeling of being pursued appeared to be the main drive behind this high perceived vulnerability for repeat hacking victims. Those with low and high levels of perceived vulnerability as well those perceived their situation as severe adopted passive avoidance strategies, which means that they neither changed their online lifestyles nor implemented any security measures. Correspondingly, a study conducted by (Parris et al. (2012)) indicated that victims of cyberbullying who felt that cyberbullying might not be prevented preferred to adopt avoidance strategies like deleting bullying messages. Only one, a female participant who had concerns about private financial information adopted approach coping strategy.

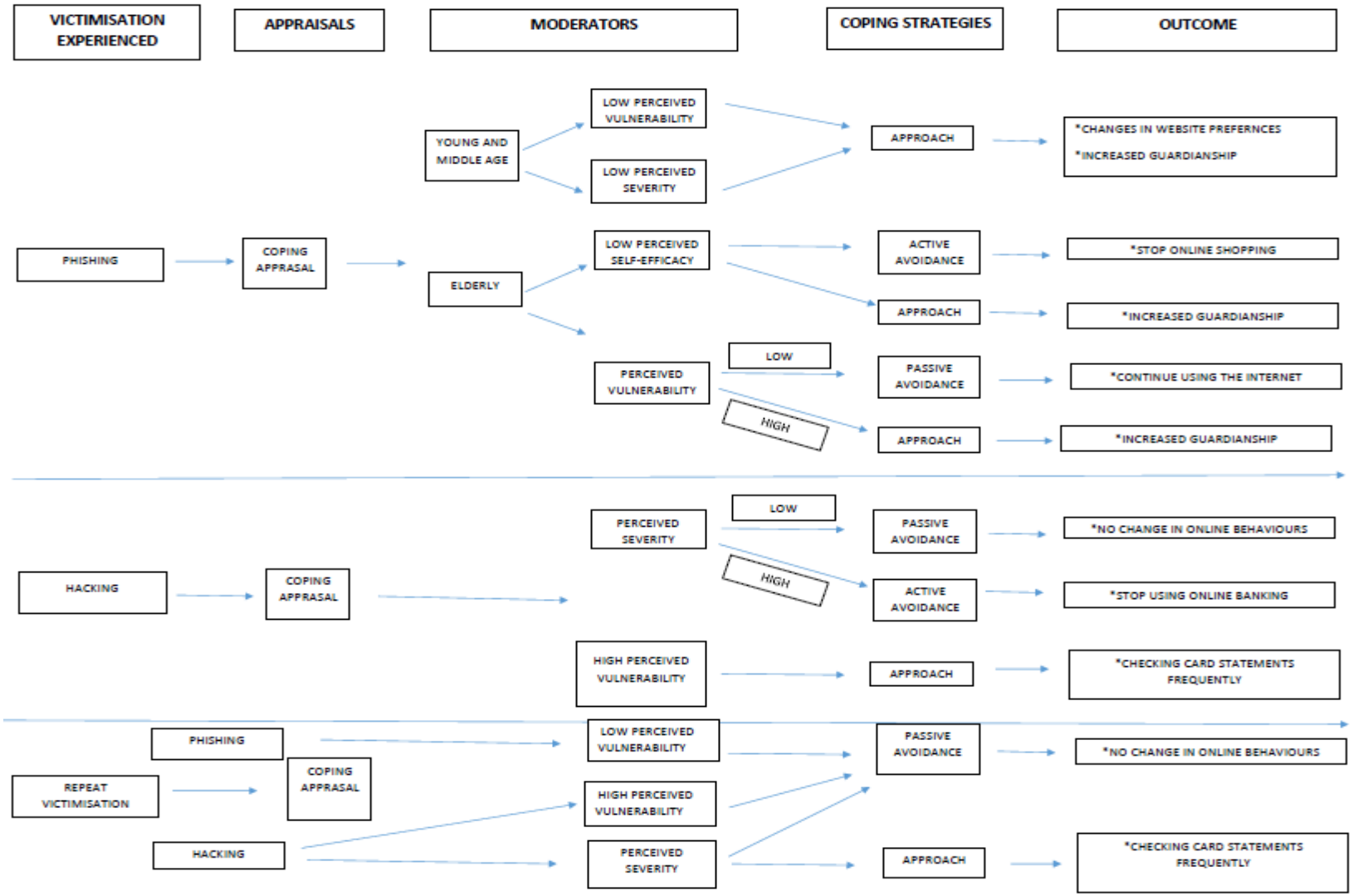



Figure 8.2: *Cyber Victimisation Coping Model*

## 8.4 Summary

This chapter examined the last phase of economic cybercrime victimisation: getting to know the victimisation and coping with consequences of negative experiences. Initially, the psychological impacts of victimisation were examined. It appeared that shock, panic and anger are the primary feelings that victims experienced. While phishing victims felt embarrassed due to their role in yielding personal information, hacking victims perceived themselves as vulnerable since their knowledge related to the victimisation process was limited. Secondly, whether victimisation experiences caused fear of crime was examined. It appeared that fear of crime was more prevalent among the participants who were hacked and experienced repeat victimisation. Lastly, the impact of prior experiences on victims' protection motivation and coping strategy adoption was examined. The Cyber Victimisation Coping Model, which was built after the Pilot Study, was tested. Findings of this chapter will be evaluated together with other quantitative and qualitative chapters in the next Discussion Chapter (Chapter Nine).

# Chapter 9 Discussion

## 9.1 Introduction

This thesis utilised a mixed method approach to examine economic cybercrime victimisation process and understand its impacts on individuals in the UK. The statistical analysis results of CSEW 2014/2015 presented in Chapter Five and qualitative analysis findings of semi-structured interviews presented in Chapters Six, Seven and Eight will be discussed here.

## 9.2 Economic Cybercrime Victimisation Process

Semi-structured interviews were conducted with victims of economic cybercrime and non-victim control group participants. Police reports pertaining to economic cybercrime cases occurring in the Northeast region of the UK in 2015 were also utilised to discern the process of economic cybercrime victimisation. Crime script analysis was used to frame the analysis process while examining the occurrence of economic cybercrime victimisation at each stage of victimisation. Sacco and Kennedy (2010) argue that the three-staged crime template, namely precursors, transactions and aftermath, can be applied to any crime. Following their crime occurrence template, this thesis applied the content analysis method, which aims to discern antecedents of economic cybercrime victimisation as well as occurrence and post victimisation effects of victimisation experiences on the victims' protection motivation and behavioural adaptations. Figure 9.1 illustrates the three-staged economic cybercrime victimisation.


Figure 9.1: *Process of Economic Cybercrime Victimisation*

## 9.3 Being Targeted Online

The findings of the qualitative analysis results suggested that exposure to phishers and proximity to hackers' tools increased the risk of being a target of an online attack.

### 9.3.1 Exposure to Phishers

Phishing is a method utilised to trick Internet users into providing their personal and financial information through socially engineered messages (Wall, 2007; Smith, 2010). Recent Internet security reports indicate that phishing attacks have become more sophisticated and increasingly more Internet users are targeted with phishing attempts (Symantec, 2017, 2018). Past empirical research on phishing mainly focused on Internet users' susceptibility to phishing emails and their behavioural responses to the phishing attempts (Parrish Jr et al., 2009; Sumner et al., 2011; Halevi et al., 2013a; Halevi et al., 2013b; Uebelacker and Quiel, 2014; Halevi et al., 2015). Discerning demographics of Internet users who received phishing emails was another aim of past phishing research (Kumaraguru et al., 2009; Sheng et al., 2010; Khonji et al., 2013; Oliveira et al., 2017). Only a handful of studies (Hutchings and Hayes, 2008; Leukfeldt, 2014; Jansen and Leukfeldt, 2016) researched determinants of being a target of a

phishing attack. This doctoral thesis expands cybercrime literature by examining the antecedents of receiving phishing emails.

Hindelang et al. (1978, p. 507) define exposure as "the physical visibility and accessibility of persons or objects to potential offenders at any given time or place". They posit that increased exposure to motivated offenders and risky situations elevate the odds of experiencing victimisation. Vocational and leisure activities are hypothesised to increase exposure to motivated offenders by rendering individuals visible and accessible to perpetrators (Miethe and Meier, 1990). Qualitative analysis of semi-structured interviews conducted with victims of economic cybercrime suggested visibility and accessibility, which are the function of exposure to motivated offenders, as the leading cause of receiving phishing emails.

Analysis of semi-structured interviews suggested personal information disclosure as the primary reason for increased exposure to phishers. Two types of personal information disclosure were identified: voluntary and involuntary personal information disclosure. Posting personal information like email addresses on Social Networking Sites (SNS) (i.e. LinkedIn, Facebook) and selling goods online emerged as two online activities associated with the risk of receiving phishing emails. Interviews suggested that participants did not perceive sharing email addresses on social media platforms as risky since this kind of information is not considered as something personal. Participants reported a significant increase in phishing emails and SMS messages (SMiShing) received after posting advertisements on websites like Gumtree. Likewise, the results of Williams (2015) suggested selling goods on online auction sites as one of the correlates of online identity theft. The increased amount of phishing attack experienced in the aftermath of posting advertisement online may be associated with the modus operandi of online advertisement websites. An examination of advertisement websites revealed that some online advertisement websites allow others to view personal information of sellers.

For example, as Figure 9.2 illustrates, online sellers' mobile number is available to the public. Once clicking on the reveal button, the whole number can be seen.

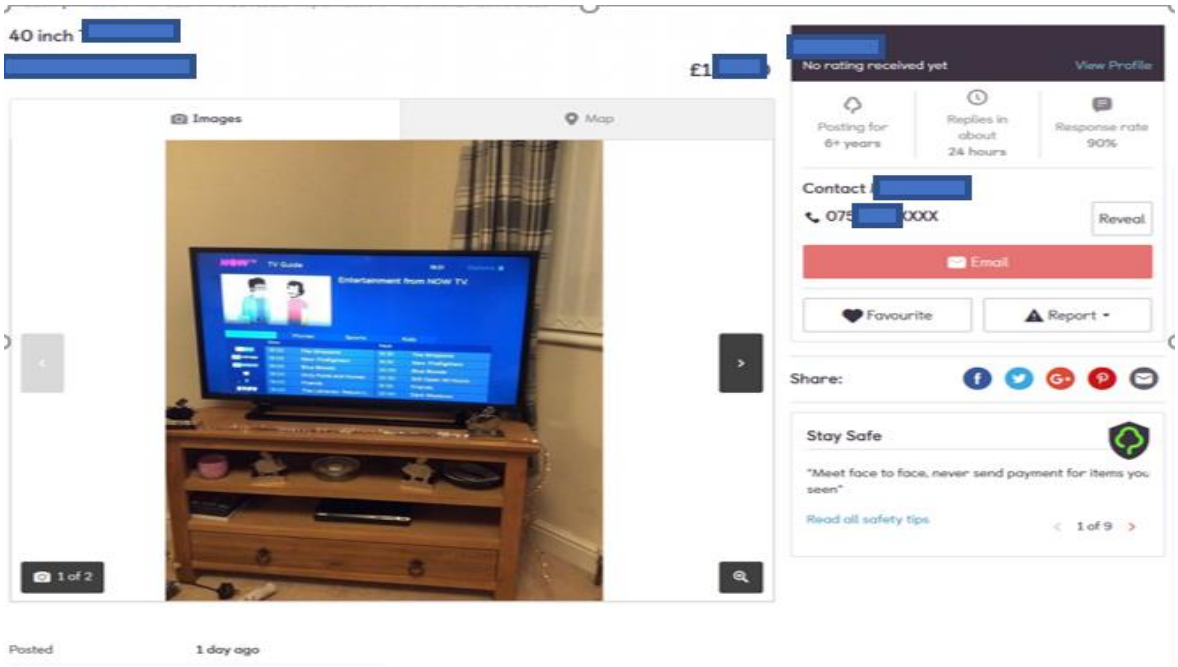



Figure 9.2: *Online Advertisement Sample*

Interviews indicated that sharing personal information on SNS platforms may facilitate being a target of phishing attempts due to data harvesting, a method utilised to collect data from the Internet. SNS (i.e. LinkedIn, Twitter, Facebook and Instagram) have not only been utilised for leisure activities, but these platforms have increasingly been used as an opportunity to construct professional networking (Ferraro, 1996; Fisher and Sloan, 2003). Most of these platforms require their users to create a profile including their brief background information. Posting personal information not only renders Internet users visible to perpetrators but also accessible because of sharing email addresses. Although it is possible to harvest data manually, programs enabling automated data harvesting may also be utilised (Huber et al., 2010). Even though the use of these programs on major Internet platforms like Facebook, Google or eBay is prohibited (Soghoian, 2008; Guo and Zhang, 2015), the results of some studies demonstrate

that there are always back doors for such programs (Huber et al., 2010; Al-Saggaf and Islam, 2015). Spear phishing attacks that target specific individuals bear some relevant information about their targets to increase their believability (Benenson et al., 2017). Harvested data from SNS and online advertisement sites may also be utilised to profile potential targets (Stanko, 1995).

Free Wi-Fi usage emerged as another factor facilitating phishing targeting. Interviews with participants illustrated that participants yield their personal information such as email addresses to be eligible for a free Internet connection in public places. Although Internet service providers holding Internet users' personal information may be considered as trusted agencies, recent news indicates that data sets of these companies are vulnerable to external threats due to security breaches and insider threats (Nurse et al., 2014; Jayapratha and Gnanasekar, 2018). Bogus Internet hotspots mimicking genuine Internet connections may also be a possible explanation of facing the risk of being an online target. Although interviews with participants did not reveal any clue about the role of bogus Internet hotspots, the results of Internet security studies propose bogus Internet hotspots as a potential threat for identity theft (Ortega and Myles, 1987; Rader and Haynes, 2011).

Data breaches of big companies that store Internet users' personal information in their databases emerged as a reason for involuntary personal information disclosure. Some of the participants reported increased email phishing attempts in the aftermath of high-profile data breaches involving companies such as Talk Talk or Vodafone. Participants who were clients of these companies suggested that their personal information stored by these companies may be used to conduct phishing attempts through emails and telephones.

### 9.3.2 Proximity to Hackers' Tools

**Online Deviance**

Cyber deviance or online deviance may be defined as online illicit behaviour that violates the rules, norms and values of a particular society (Holt and Bossler, 2016; Rijnetu, 2018). Labelling some particular actions or behaviours as deviant is a controversial issue since deviance is a socially constructed subjective concept affected by cultural and temporal diversities (Vazsonyi et al., 2002; Thompson and Gibbs, 2016). Nonetheless, cybercrime studies tend to label some online activities that are perceived to be violating moral standards of contemporary society as deviant. Viewing or downloading online pornography (Demetriou and Silke, 2003; Buzzell et al., 2006; Bossler and Holt, 2010; Ngo and Paternoster, 2011), pirating and sharing pirated media (Bossler and Holt, 2010; Ngo and Paternoster, 2011; Donner et al., 2014), hacking (Bossler and Holt, 2010; Ngo and Paternoster, 2011; Donner et al., 2014) and downloading software illegally (Donner et al., 2014; Paek and Nalla, 2015) were conceptualised as deviant online behaviours in cybercrime studies.

Macro-level adverse financial impacts of free livestreaming on football industry and broadcasting companies are well documented (David et al., 2014; South, 2015; Rafique et al., 2016). This thesis illustrated negative effects of accessing free streaming or sharing pirated content at individual level. Interviews with both victim and control group participants suggested that engaging with deviant online activities like free streaming, sharing pirated media through Torrent websites or Peer-to-peer sharing programs and watching free pornography were more prevalent among young Internet users who also mostly experienced economic cybercrime through hacking of their online accounts. Participants mostly reported experiencing pop-up windows while trying to access these free online services. A possible explanation between experiencing economic cybercrime victimisation and the risk posed by unwanted pop-

up windows and illegal downloading which is generally offered for malware dissemination will be evaluated in the following section of this chapter where the hacking victimisation is discussed.

It may be proposed that engaging with risk-bearing deviant online activities increases the chance of converging with the tools of hackers, which are malware or malicious codes written to steal personal and financial information of Internet users. Participants who acknowledged accessing these deviant online services reported feeling financially secure as they did not provide any personal or financial information. This aspect of free deviant online services appears to decrease the perceived severity of engaging with online deviance. The presence of security software was another source of relief among Internet users who engaged with online deviant activities. Most of the participants reported the success of anti-virus software in thwarting virus infection attempts. Though security software is capable of blocking online attacks, it is still vulnerable to zero-day attacks, which are recently designed malicious codes that are not known by security companies (Sheng et al., 2009; Bulakh and Gupta, 2016). Ngo and Paternoster (2011) argue that relying heavily on security software as a way of deterring online attacks may create a false sense of trust that increases the propensity to engage with risky online activities. The findings of this thesis appear to suggest the proposition of a false sense of security among Internet users.

## 9.4 Occurrence of Victimisation

The previous section of this chapter discussed the possible reasons for being a target of a phishing attempt. This section of the chapter examines the causes of economic cybercrime victimisation. This section aims to address *why* and *how* some Internet users experience economic cybercrime victimisation.

### 9.4.1 Phishing

Although previous cybercrime studies did not make a distinction between website phishing and email phishing, this thesis examines the process of victimisation for these two types of phishing separately. The modus operandi of perpetrators is the rationale behind this separation. While online perpetrators target email users directly through unsolicited emails, phishing websites attract targets to them.

#### 9.4.1.1 Email Phishing

Research on human decision-making processes has identified two types: heuristic or system one decision-making processes, and systematic or system two decision-making processes (Maheswaran and Chaiken, 1991; Schwarz, 2000). This latter process of reasoning is known as "dual process model of reasoning" (Croskerry, 2009, p. 28). System one decision-making process, which is based on patterns that are products of past experiences, produces quick and spurious results (Jefford et al., 2011). The systematic decision-making process, however, is a more conscious and deliberate process where data is analysed to reach a sound decision (Acquaviva et al., 2013). The systematic decision-making process is slower than heuristic since it requires a careful analysis of received information (Schutten et al., 2017). The heuristic decision-making process is utilised more often as it necessitates less effort when compared to Systematic decision-making system (Bate et al., 2012). Interviews with phishing victims suggested that online perpetrators coerced Internet users to use heuristic decision-making process through socially engineered messages.

Social engineering is regarded as one of the most effective methods utilised to gain information from potential targets (Wall, 2013c; Conteh and Schmick, 2016) since phishers send socially engineered email messages to exploit a weakness in the human decision-making process (Nirmal et al., 2010; Lakshmi and Vijaya, 2012). Internet security literature has

suggested two groups of factors that are utilised to manipulate Internet users to divulge their personal information: external and individual factors. External factors are the techniques utilised to force Internet users to make decisions based on heuristic or system one decision making. Influence techniques, urgency cues, visceral cues and fear appeals are considered as external factors impacting email users' decision-making process (Vishwanath et al., 2011; Ferreira and Lenzini, 2015; Naidoo, 2015). Individual factors are the cognitive or emotional and socio-psychological vulnerabilities that are inherent to human nature (Macwan, 2004; Yuill et al., 2007; Panwar, 2014). Interviews with both victim and control group participants suggested personal involvement, fear appeals and believability cues as the external factors facilitating phishing victimisation. Low Internet self-efficacy emerged as the only individual factor leading economic cybercrime victimisation through phishing. This thesis also identified contextual vulnerabilities such as the presence of distractors, accessing the Internet while being alone and being tired as factors facilitating victimisation. This third category of factors affecting decision-making system is a novel contribution of this thesis.

**External Factors**

Email usage has many diverse applications in our lives. It can be utilised for many purposes ranging from communicating with colleagues to receiving information from financial institutions or news about recent sales from online retailers. Thus, Internet users receive many emails every day from various sources. While some of these emails grab receivers' attention some of them remain unnoticed. Grabbing Internet users' attention through perceived relevance appears to be the initial aim of phishers. The state of increased attention caused by perceived relevance is named as felt involvement (Celsi and Olson, 1988). The analysis of interviews suggests that participants experienced two types of felt involvement: direct involvement and indirect involvement. Whereas messages which encompass personal information like Internet users' names, or last four digits of credit card information arouse direct felt involvement,

messages indicating some actions about banks, online accounts like PayPal caused indirect involvement.

The findings of this thesis suggested that messages conveying indirect felt involvement were placed in the title of the phishing emails. Participants acknowledged that the contents of the titles provide helpful cues in weighing the importance of email messages. It is reported that general information about something related to participants' lives at the time of receiving email messages influences the propensity to open the emails. For instance, one postgraduate student participant responded to a phishing email containing an alert message in the title of email about refunding. As the participant was awaiting a refund from her university, the title of the message indicating the last chance to get a refund grabbed her attention. As she states, her increased focus on getting a refund prevents her from evaluating the content of the message. This finding is in accordance with previous phishing susceptibility research demonstrating that titles like "Upgrade Your Email Account Now" (Wang et al., 2012, p. 351), "Dear PayPal User" (Downs et al., 2007, p. 38) or "Verify Your University Email Account Now" (Vishwanath et al., 2011, p. 51) were successful in getting attention.

Indirect felt involvement occurred in cases where random phishing messages are received. However, directly felt involvement mostly occurred when victims were targeted with spear-phishing emails that contain some personal information like names or credit card numbers. These kinds of messages were mostly found in the body of the emails to increase the believability of the phishing emails. The utilisation of believability cues was another external factor appeared to increase Internet users' susceptibility to phishing emails.

Interviews with participants suggested that inclusion of believability cues like the name of big brands and relevant personal information into phishing emails increased the odds of responding phishing attacks. Victim participants reported the name of brands like Apple or

PayPal made them believe that the emails were genuine. Phishing emails bearing some relevant personal information about the target is named as spear phishing (Caldwell, 2013). The findings of this thesis are in line with literature suggesting that spear phishing attacks have high success rates due to increased believability (Wall, 2013b; Halevi et al., 2015).

Fear appeals, which are intimidating messages to cause a sense of anxiety (Witte, 1992), emerged as another external vulnerability that facilitated susceptibility to phishing messages. It is proposed that fear appeals have two components. The first component points out the imminent threat to be faced and the second part offers suggestions to thwart mentioned threat (Vance et al., 2013). The threat of paying for unpurchased items from Apple stores, suspicious activities related to PayPal accounts emerged as fear appeals participants acknowledged. Clicking on the link provided in the emails were offered as suggestions to solve the fabricated problem. The results of previous phishing studies highlighting the effectiveness of fear-provoking messages in persuading Internet users to yield their personal information support the findings of this thesis (Sheng et al., 2010; Blythe et al., 2011; El-Din et al., 2014; Panwar, 2014).

#### 9.4.1.2 Website Phishing

Bivariate analysis results presented in Chapter Five indicated a statistically significant association between accessing the Internet for buying goods or services online and using online government services and experiencing economic cybercrime victimisation. Multivariate analysis results demonstrated that buying goods or services online increased the risk of economic cybercrime victimisation 40%. Likewise, Internet users who accessed the Internet for online government service usage appeared to run the risk of victimisation 1.3 times when compared to others who did not use these online services. These results were of significance in depicting the extent of the threat. Why and how these online activities were a risk factor for

economic cybercrime victimisation was not clear. Semi-structured interviews and police reports were utilised to investigate this issue further.

### Accessing the Internet for Online Shopping or Online Services

Participants were asked about website preferences while shopping online. Internet users' website preferences emerged as a risk factor increasing the odds of experiencing economic cybercrime victimisation through website phishing. Most of the participants cited reputable online traders as their most preferred online shopping websites mostly due to trusting their brand name. Some other participants who also lost money because of shopping with unreliable merchants reported shopping from online merchants emerging from web search results. When these participants were further asked about the rationale for their website preferences, the desire to buy something extraordinary, peak sale periods and the opportunity to get a refund for financial loss emerged as the common themes to account for shopping from unknown websites.

Participants who wanted to buy extraordinary presents like Elvis cards, online gaming characters or charity gifts did their shopping via unknown websites. However, these websites are sometimes established to defraud Internet users (McKown, 2017; Vynck and Barr, 2018) or they lack essential security measures to protect their customers (Barrett, 2016; Zurkus, 2016). Peak sale periods also emerged as another reason for shopping from unknown websites rather than reputable traders. Traders generally apply discounts for peak sales periods like Christmas or Black Friday to attract more customers. Internet users may conduct online searches for the lowest prices. The findings of this thesis suggest that peak sales periods appear to create opportunities for some bogus websites that offer alluring prices to defraud online shoppers.

Refund protection provided by law emerged as another factor boosting the intention of shopping with unknown online traders. The regulation is known as *Section 75 of the Consumer Credit Act, 1974* provides financial protection for credit card users when they purchase with between £100 and £30,000. Banks also provide a refund for unauthorised payments. Interviews with victims indicate that for fear of losing reputation, most of the banks in the UK make this refund very quickly and silently. Thus, some of the participants who even faced repeat economic cybercrime victimisation perceived no adverse financial outcome of shopping with unknown websites due to these regulations. The finding related to Internet users' perception about refund policies indicates that Internet users conduct a calculus of behaviour, which refers to assessing the cost and the benefit of an action (Laufer and Wolfe, 1977), before engaging with online activity.

### 9.4.2 Unauthorised Access to Online Financial Accounts and Credit Card Information

Hacking, which is the unauthorised access to networked computer systems with the aim of altering, damaging or gaining information without owner's consent (Floyd et al., 2000), is considered to be one of the significant threats to both social and economic life (Wall, 2008b; Levi, 2017). Hackers not only target financial institutions or governmental bodies, they increasingly target individuals' electronic devices like smartphones as well as financial and social media accounts (Blythe et al., 2011; Chavez, 2018). The hacking of famous people's social media or cloud storage accounts has become an everyday event. Many people including politicians and celebrities suffered reputational damage as a result of leakage of sensitive information. Due to the adverse impacts of hacking, a considerable body of empirical and theoretical research has focused on the determinants of hacking behaviour (Xu et al., 2013; Mohammad et al., 2015; Zhang et al., 2015) and deterrence of hacking attacks (Hjortdal, 2011; Tejay and Zadig, 2012; Cui et al., 2017a). The relationship between hacking, malware infection

(Bossler and Holt, 2009; Moquin and Wakefield, 2016), online identity theft (Reyns and Henson, 2016) and online harassment (van Wilsem, 2013b) has been researched. However, the relationship between hacking and economic cybercrime victimisation has not been documented yet. This thesis examines the causes of becoming a victim of economic cybercrime through hacking.

Bivariate analysis results presented in Chapter Five indicated a statistically significant association between accessing the Internet for online banking or managing finances and risk of victimisation. However, the statistical strength of these relationships was weak. Weak strength of associations can be interpreted as the presence of other factors moderating the relationship between two variables (Field, 2009). Qualitative analyses of semi-structured interviews and police reports suggested that hacking of Internet users' bank account may be related to technological vulnerabilities posed by electronic devices, mobile applications and Wi-Fi connections as well as engaging with online deviancy.

#### 9.4.2.1 Technological Vulnerabilities

This part of the section discusses the impact of technological vulnerabilities on the risk of experiencing economic cybercrime victimisation. The findings discussed in this section contribute to cybercrime victimisation literature by highlighting technological risks. This thesis is one of the first cybercrime studies examining the impact of technological vulnerabilities on the risk of facing cybercrime victimisation.

**The Type of Electronic Device Utilised to Access Online Financial Services**

The impact of electronic devices on the risk of economic cybercrime is firstly examined through statistical analysis of CSEW 2014/2105. The results of the quantitative analysis suggested that Internet users who accessed the Internet via mobile phones or smartphones were

approximately 3.3 times more likely to face online banking fraud when compared to others who did not use mobile phones or smartphones to access the Internet. Handheld computers (i.e. iPad or tablets) and laptops used away from home and work or school emerged as risk factors for card-not-present fraud victimisation.

Interviewees were asked about their electronic device preferences while connecting to the Internet for financial activities like online banking in Qualitative Phase of the research. Types of victimisation experienced and electronic device preferences were cross-tabulated with the help of NVivo QSR software to examine the relationship between electronic device preferences and experiencing economic cybercrime victimisation. Cross-tabulation analysis results illustrated that while hacking victims mostly utilised a laptop and mobile phones to access online financial activities, phishing victims used laptop and tablets. Participants who experienced economic cybercrime victimisation multiple times preferred the mobile phone to access online financial services.

Interviews with participants suggested Internet users' perceptions about the security capability of electronic devices and free Wi-Fi usage as a possible explanation of the association between the type of device utilised to access the risk of victimisation.

Participants were asked about the rationale of choosing electronic devices to access the Internet. Large screens which enable examining online products while shopping was most frequently cited a reason for using laptops and desktop computers for financial activities. Mobility, convenience and presence of mobile applications were mostly reported reasons for mobile or handheld devices like iPad usage for online financial activities. These findings are in line with recent marketing studies researching Internet users' electronic device preferences (Penny et al., 2016; Huang et al., 2017; Bröhl et al., 2018). It is interesting that security

considerations were not reported as a reason for devices preferences to conduct online financial activities.

Moreover, some participants reported that they preferred Apple products to do financial transactions since these products are safe from malware infection. Although Apple products have some extra security applications such as Gatekeeper, an application that blocks the installation of digitally unknown programs, they still bear similar risks when compared to Windows-based products (Hill, 2015; Haslam, 2017; Price, 2017). Adware, Trojan horse, Microsoft Word micro viruses and ransomware attacks are common threats to Apple products as well as Microsoft products (Covington and Taylor, 1991). Since the majority of Internet users rely on Microsoft Windows, most of the malicious codes are written to target Microsoft Windows (Boateng, 2016). Virus writers familiarity with Microsoft platform is another reason for the greater vulnerability of Microsoft products. However, a good deal of malicious codes and scripts are designed for Apple products (Moore and Shepherd, 2006).

Free Wi-Fi usage emerged as another explanation for the vulnerabilities presented by electronic device preferences. As it was stated above, statistical analysis of CSEW 2014/2015 indicated that while mobile phone or smartphone usage emerged as a risk factor for online banking fraud victimisation, the laptop used away from home or work/school settings appeared to be risk enhancing factor for card-not-present fraud victimisation. These results explicitly implied the presence of insecure Internet connections while accessing the Internet. Semi-structured interviews with participants supported this proposition. Some participants acknowledged accessing free Wi-Fi offered at airports, hotels or public places like restaurants. Although most of the participants reported being careful about accessing financial services while utilising free Wi-Fi, two of the victim participants whose online banking accounts were

compromised perceived free Wi-Fi usage as a possible reason of losing online banking account credentials.

### Mobile Application Usage

Mobile applications may be considered as the most significant aspect of smartphones. Mobile applications can be utilised for many purposes ranging from communication to health-tracking. Due to the increased popularity of mobile applications banks and online traders offer their commercial applications to decrease their costs while increasing their visibility (Fajczak-Kowalska and Kowalska, 2017; Lu and Thabtah, 2017). A growing body of mobile technology literature suggests that free mobile applications or security breaches of popular applications may pose a risk of personal information loss (Gold, 2012; Kirk, 2015; Sullivan, 2015). The risk of mobile application usage for cybercrime victimisation has not been researched yet. This thesis aims to address this gap through an analysis of semi-structured interviews with both victims and control group participants.

Interviews illustrated that mobile application usage is widespread among Internet participants. Only three victim and two control group participants did not use mobile applications since their mobile phones were not suitable for application installation. Interviews suggested bogus application usage as a possible explanation of facing economic cybercrime victimisation. Two participants directly lost money due to using a bogus application allegedly providing some commercial services. Recent news appears to support this finding. It is reported that Google removed a fake WhatsApp application after being downloaded more than one million times (BBC, 2017). Internet security companies warn about these cloned applications and recommend utilising security software on mobile phones (Norton, 2018). Interviews with participants suggested that only a few participants use mobile security software. Those who reported using mobile security software acknowledged using it because of being provided as a

complimentary service for their network provider. This finding indicates that network providers should be encouraged to provide free security services to increase the safeguarding of mobile devices.

**Password Fatigue**

Most web services like SNS, shopping sites or online banking sites require Internet users to create digital accounts and passwords to secure these accounts. However, due to a large number of online accounts, it may sometimes become difficult to memorise all these passwords. Password fatigue is defined as the state of being overwhelmed with a load of digital identities or identity-related online passwords (Jøsang et al., 2007). The results of previous studies suggested that password fatigue leads to the application of same passwords to different online accounts (Corre et al., 2017; Dasgupta et al., 2017), the impacts of this behavioural adaptation on the risk of facing cybercrime victimisation have not been empirically researched yet.

Qualitative analysis results of interviews suggested a relationship between password fatigue and financial information loss. Most participants of semi-structured interviews reported using the same password for the different online accounts due to difficulties remembering passwords. Cross-tabulation of password behaviour and type of victimisation displayed that three of these participants who reported password fatigue faced economic cybercrime victimisation due to the hacking of their online financial accounts like PayPal or banking account. This finding supports the findings of Button et al. (2014b) who conducted a qualitative study based on semi-structured interviews with victims of online fraud. Their findings also suggest utilising the same password for different online accounts as an explanation of the loss of money through hacking victimisation.

In sum, technological vulnerabilities and password fatigue appear to account for the statistical analysis results indicating online banking and online shopping as a risk factor for economic cybercrime victimisation. Previous cybercrime studies (Ngo and Paternoster, 2011; Reyns et al., 2011; van Wilsem, 2011; Leukfeldt and Yar, 2016) also suggested online banking and online shopping as a risk factor for cybercrime victimisation; however, this research contributes to the literature by providing a possible explanation of these results.

#### 9.4.2.2 Online Deviance

The impact of deviant online activities on the risk of experiencing cybercrime victimisation has received considerable attention in cybercrime literature over the last decade. The relationship between online deviant activities and malware infection, online harassment and different forms of cybercrime victimisation have been empirically researched (Choi, 2008; Holt and Bossler, 2008; Bossler and Holt, 2009; Bossler and Holt, 2010; Ngo and Paternoster, 2011; Reyns et al., 2011; Donner et al., 2014). This thesis expands the literature by examining the relationship between online deviancy and economic cybercrime victimisation.

Qualitative analysis of semi-structured interviews and police reports suggested deviant online activities like *free streaming*, *illegal downloading*, *accessing free adult content* as a risk fact for economic cybercrime victimisation through hacking. Although the results of previous research suggested engaging with online offending behaviours like hacking others' computers or online accounts and pirating media as the deviant online activities (Bossler and Holt, 2010; Ngo and Paternoster, 2011; Donner et al., 2014), these online behaviours were not reported by participants. The absence of these behaviours may be attributed to the rarity of these deviant behaviours among target population or participants' unwillingness to disclose sensitive information. Participants' unwillingness to share sensitive information is well documented in the literature (Biernacki and Waldorf, 1981; Milne et al., 2004). An instance that I encountered

while conducting interviews also appears to support the literature. One of my participants reported accessing free streaming websites to view free movies online after finishing the recorded session of interview. The participant acknowledged the presence of tape recording as a factor that prevented her from talking about deviant behaviour during the interview.

Cross-tabulation of interviews suggested that deviant online activities are more prevalent among young Internet users who are under thirty years old. Nine participants acknowledge engaging with deviant online activities, and six of them were under thirty years old. Moreover, most of these participants who reported engaging with online deviant activities were hacking victims. This finding is in line with previous studies indicating a statistical relationship between deviant online activities and malware infection (Bossler and Holt, 2009) and identity theft victimisation (Holt and Turner, 2012; Reyns, 2013).

Participants who accessed free streaming and free adult websites reported experiencing pop-up windows. Drive-by-download causing malware infection may be a possible explanation of the association between experiencing economic cybercrime victimisation through hacking of online financial accounts and engaging with deviant online activities. Cybercrime literature suggests that fraudsters utilise pop-up windows where malicious codes are embedded to infect targeted computers (Cluley, 2010; He et al., 2015; Rijnetu, 2018). Malicious software installs itself automatically to target computers once the pop-up windows are opened (Narvaez et al., 2010; Soltani et al., 2014). The results of Choi (2011) suggest clicking on pop-up windows as a risky online behaviour that increases the chance of computer virus infection. Although findings of this thesis illustrate that Internet users were targeted with malicious code containing pop-up windows due to cyber-deviance, Jansen and Leukfeldt (2015) who studied causes of online banking fraud victimisation in the Netherlands found that responding to pop-up

windows messages displayed while visiting legitimate online banking websites also caused malware infection.

Malware infection risk caused by illegal download from Torrent websites or Peer-to-Peer (P2P) programs may be another explanation of the association between online deviance and economic cybercrime victimisation through hacking. It is proposed that virus writers conceal malicious codes within attachments bearing pirated media to steal personal information (Wade, 2004; Holt and Copes, 2010; McCorkle et al., 2012). This means that illegal downloading of pirated digital files facilitates malware dissemination. The results of previous empirical research documented the risk of illegal downloading and opening unknown attachments on the risk of facing malware infection (Choi, 2008; Bossler and Holt, 2009) and identity theft (Holt and Turner, 2012; Reyns, 2013). For example, binary logistic regression analysis of Reyns (2013) demonstrated that Internet users who downloaded music or movie files from the Internet were 27% more likely to experience online identity theft when compared to those who did not download any music or movie file.

Although previous research documented the relationship between online deviant activities and risk of victimisation, they failed to account for the rationale of online deviancy. Perceived benefits of accessing some online services for free emerged as the main reason for cyber-deviance. Participants who accessed free streaming websites or downloaded free software through Torrent websites or Peer-to-peer (P2P) programs, suggested unreasonably high prices of these services as the primary reason for utilising these services. Apart from this neutralisation technique, contextual vulnerabilities such as personal problems and financial hardship also emerged as the reasons for engaging with online deviant behaviours. While one young participant who recently ended her long-term relationship suggested depression as a reason for watching free pornography, the other three older participants acknowledged

loneliness as a rationale for accessing adult content. This finding indicates that contextual vulnerabilities emerged from inadequate or failed socialisation may lead to online deviance which facilitates economic cybercrime victimisation. Although it is argued that increased Internet use may lead to social isolation (Shapira et al., 2003; Asudani, 2018; Mariel et al., 2018), the findings of this thesis suggest that social isolation among Internet users may lead to online deviance.

The desire to earn money online at times of financial difficulties appears to be another reason for engaging with online deviancy. For instance, one of the victim participants acknowledged that he faced both hacking victimisations when he was experiencing financial hardship. A control group participants' account suggesting engaging with online deviant activities like amateur pornography to earn money as a possible reason for the presence of victimisation among his friends may be another example of the relationship between financial hardship and victimisation. Recent empirical studies illustrate an increased propensity to work in the digital sex work industry among university students and adolescents (Sinacore et al., 2015; Koops et al., 2018; Sanders et al., 2018; van Doorn and Velthuis, 2018). The results of these studies suggest that earning money for college fees or living expenses as the primary reason for webcam modelling among students. For instance, the results of Roberts et al. (2010) who studied student involvement in the online sex industry through a sample of undergraduate students at a London university illustrated that 16.5% of participants displayed a willingness to work as a sex worker to help finance their studies.

#### 9.4.2.3 Virtual Hot Spots of Crime

Tempo-spatially disproportionate distribution of crime events is one of the premises of opportunity theories of victimisation (Cohen and Felson, 1979; Cohen and Cantor, 1981). This premise underscores the presence of places where crime events mostly occur. Distinguishing

these crime-centric places which are coined as “hot spots of crime” (Sherman et al., 1989, p. 37), attracted significant criminological attention (Eck et al., 2000; Farrell and Sousa, 2001; Townsley and Pease, 2002). Bars, nightclubs, parks are found to be hot spots of crime because of the lack of social control and high concentration of potential offenders (Meier and Miethe, 1993; Chainey et al., 2008; Johnson and Bowers, 2008). However, up to date, no empirical research examined the virtual hotspots of crime where cybercrime opportunities arise. The findings of this thesis suggest that websites offering free streaming, free pornography and file sharing websites like Torrent websites emerge as virtual hot spots of cybercrime where malware is disseminated to steal personal and financial information. This finding has some significant policy implications for the governance of the Internet. These implications will be discussed in the policy implications section of the Conclusion Chapter (Chapter Ten).

## 9.5 Dealing with Consequences of Economic Cybercrime Victimisation

Previous research has found that white-collar crime or fraud victimisation experiences may have similar long-lasting effects such as anxiety and depressive disorder on individuals when compared to violent or property crimes (Ganzini et al., 1990; Titus et al., 1995; Piquero et al., 2007). This section of the chapter discusses economic cybercrime victims’ both emotional and behavioural responses to their victimisation experiences.

### 9.5.1 Emotional Responses

Semi-structured interviews with victims of economic cybercrime suggested that shock, panic, annoyance and anger were the primary feelings that victims experienced. Most of the respondents become aware of their victimisation through an alert email or a phone call coming from their banks’ customer services. Some others learned about their victimisation while shopping since their banking cards were refused. Unexpected news about their bank accounts caused a feeling of shock and panic. While getting worried about the financial loss they also

rushed to find a solution to prevent future victimisation. Cancelling banking cards and suspending bank accounts were the initial measures to prevent future victimisation.

Primary feelings of shock and panic were later replaced with annoyance. Time lost while contacting police and banks' customer services and restoring account information emerged as a source of annoyance among participants. The attitude of help desk staff while reporting and explaining the occurrence of victimisation was another reason for annoyance. Respondents mostly complained about being questioned about the possible misuse of their financial information. Short term financial hardship due to cancellation of banking card also created a sense of annoyance among participants. This security precaution made them ask for money from their friends or relatives, which also caused annoyance.

Self-blaming is another feeling experienced by especially phishing victims. Phishing victims reported that they felt embarrassed due to their unwariness while responding to phishing emails. Feelings of self-blaming and feeling embarrassed are found to be common among fraud victims. The results of empirical studies yielded that most victims blamed themselves because of believing the fraudsters' fabricated scenarios (Ganzini et al., 1990; Button et al., 2009, 2014a). The feeling of embarrassment was coupled when they had to ask money from their friends or relatives since they had to explain how they were deceived.

Anger emerged as the strongest emotional response participants reported. It appears that anger is the cumulative outcome of all adverse events experienced the aftermath of victimisation. Most participants were angry due to inconvenience experienced. As it was explained earlier, a great deal of time and effort were spent to settle down all formalities. This feeling of inconvenience was stronger than financial worries. Some other participants found their victimisation experience unfair. For instance, an older participant complained: *"I asked my son, why they rob an old lady?"* (Rosie, 78 years old female victim participant). The results

of fear of traditional crime studies suggest that anger is more prevalent than fear of crime among victims (Silverman and Kennedy, 1985; Smith and Hill, 1991).

### 9.5.2 Fear of Crime

Fear of crime has generally been considered as a significant problem for decades due to its numerous psychological and social consequences as well as detrimental effects on the quality of life (Liska et al., 1982; Box et al., 1988; LaGrange et al., 1992; Amerio and Roccato, 2005; Vieno et al., 2013). Although Garofalo (1981) limits fear of crime to emotional reactions arouse due to physical harm threat, fear of crime literature accepts a more general definition of it. While Ferraro (1995, p. 23) defines it as "an emotional response of dread or anxiety to crime or symbols that a person associates with crime", Henson and Reyns (2015, p. 92) define fear of crime as "an emotional response to a danger or threat of an actual or potential criminal incident". As can be seen, Henson and Reyns (2015) included emotional reactions to potential threats into their definition. This expansion of the scope of fear of crime may be aimed to encompass the feeling of anxiety since some scholars (Binder, 1999; Warr, 2000) argue that anxiety and fear of crime are conceptually different. It is argued that while anxiety is the anticipation of potential dangers, fear is the emotional reactions to immediate threats (Warr, 2000). Thus, the definition of Henson and Reyns (2015) includes a broader range of feelings towards the threat of victimisation.

Fear of traditional crime studies categorised antecedents of fear of crime into three groups: social determinants, demographic characteristics and psychological determinants (Yin, 1980; Skogan, 1986). Findings related to fear of economic cybercrime will be discussed under these headings.

#### 9.5.2.1 Social Determinants of Fear of Cybercrime

Fear of traditional crime literature suggested previous victimisation experience (direct victimisation experience) and interactions about crime (indirect victimisation experience) as two significant determinants of fear of crime (Yin, 1980). The results of the empirical studies indicated that both direct and indirect victimisation experiences intensify the fear of crime (Smith and Hill, 1991; Russo and Roccato, 2010; Grubb and Bouffard, 2015). Fear of cybercrime studies yielded somewhat contradictory results about the influence of prior experience on fear of cybercrime. Fear of online interpersonal victimisation studies suggested that prior victimisation experience increased the fear of online interpersonal victimisation (Alshalan, 2006; Henson et al., 2013; Yu, 2014). Yu (2014) found no relationship between fear of cybercrime and previous experiences of digital piracy and online scams.

Quantitative analysis results presented in Chapter Five suggested that fear of identity theft was more prevalent than fear of cybercrime among the British population. Whereas approximately 66% of participants reported a degree of fear of identity theft, nearly 48% and 44% of Internet users acknowledged a worry about the fear of credit card fraud and cybercrime respectively. Bivariate analyses were also conducted to observe the impact of prior economic cybercrime victimisation on fear of crime. The results of these bivariate analyses indicated that fear of identity theft, credit card fraud and cybercrime was more prevalent among participants who experienced economic cybercrime victimisation. These results suggested the impact of previous victimisation experience on fear of cybercrime.

To explore the fear of economic cybercrime, both victim and non-victim control group participants were asked about whether they felt worried about being a victim of economic cybercrime. Previous victimisation experience and indirect victimisation experience emerged to increase the fear of economic cybercrime among participants. Most of the participants who

had been victimised more than once reported a concern about facing economic cybercrime victimisation again (six out of seven participants). Control group participants acknowledged slightly higher figures of fear of economic cybercrime. Seven out of twelve control group participants reported being fearful of experiencing victimisation. Media news was the most cited source of the fear of economic cybercrime among non-victim control group participants. The findings of this thesis appear to support the fear of traditional crime literature suggesting the impact of direct and indirect victimisation experiences on fear of crime.

#### 9.5.2.2 Demographic Characteristics

Fear of traditional crime studies suggested the prevalence of fear of crime among females (Schafer et al., 2006; May et al., 2010) and older people (Covington and Taylor, 1991; Moore and Shepherd, 2006). Fear of cybercrime studies yielded contradictory results about gender differences. Whereas fear of cybercrime studies found no gender difference for fear of online identity theft and malware infection, the results of fear of online interpersonal crime studies suggested that females are significantly more fearful than males. Since female Internet users are mostly targeted by online interpersonal crime (Finn, 2004; Franks, 2011), the prevalence of fear of online interpersonal crime may be considered to be rational.

To explore the extent of gender differences in fear of cybercrime and economic cybercrime statistical analysis of CSEW 2014/2015 and qualitative analysis of semi-structured interviews were conducted. Bivariate analysis results of CSEW 2014/2015 displayed in Chapter Five suggested a slight gender difference in fear of cybercrime. When the relationship between fear of cybercrime and gender was examined with the introduction of age as the third variable, the multivariate analysis suggested that middle-aged and older female participants were more fearful than those who were under thirty years old. The qualitative analysis of interviews suggested a slightly higher fear of economic cybercrime among female participants.

Nine out of seventeen female participants acknowledged being fearful of economic cybercrime, and five of those were over sixty years old. When these results are evaluated together, the evidence suggests that fear of economic cybercrime is more prevalent among older female Internet users than young female Internet users.

#### 9.5.2.3 Psychological Factors

Psychological factors, perceived risk of victimisation and perceived seriousness of the crime, were also proposed to be determinants of fear of crime (Yin, 1980). It is assumed that fear of crime and perceived risk of victimisation are conceptually different (Rachman, 1976; LaGrange and Ferraro, 1989; Warr, 1993; Ferraro, 1995). Perceived risk of victimisation is conceptualised as the cognitive assessment of the likelihood of experiencing victimisation. However, fear of crime is regarded as emotional reactions towards the threat of victimisation (Rengifo and Bolton, 2012). Fear of traditional crime studies found a reciprocal relationship between these two constructs (Wyant, 2008; Cook and Fox, 2011). Fear of cybercrime studies has also found that perceived risk is associated with fear of identity theft and online crime (Higgins et al., 2008; Yu, 2014), fear of online interpersonal crime victimisation (Henson et al., 2013; Randa, 2013).

Interviews with victims of economic cybercrime suggested that there is a relationship between the type of victimisation experienced, perceived risk of victimisation and fear of economic cybercrime. Interviews indicated that whereas hacking victims were more worried about repeat victimisation, phishing victims were less worried about the chance of being a victim again. This difference may be attributed to the fact that phishing victims were more informed about their victimisation process. Unfortunately, nearly all hacking victims had little or no information about how they were hacked. Participants mostly complained about receiving insufficient feedback about the causes of their victimisation.

Uncertainty about the reasons of victimisation appeared to boost the risk perception among victims who experienced financial loss through hacking. The literature on perceived risk appears to support the finding of this thesis suggesting an association between the lack of information about the victimisation process and heightened perceived risk of victimisation. It is argued that uncertainty is a dimension of perceived risk and it has a multiplier effect on perceived risk (Dowling, 1986; Mitchell, 1999). The results of empirical studies indicate that consumers whose perceived risk is affected by uncertainties around the brand name or product quality decreased their purchase intention (Mitchell and Greatorex, 1993; Kim et al., 2008).

The perceived severity of consequences also appeared to modify the intensity of fear of economic cybercrime. Interviews with victim participants suggested an association between socio-economic factors, perceived severity of consequences and fear of economic cybercrime. Interviews with victim participants indicated that financial loss appeared to have varying impacts on victims' psychological well-being. Participants who perceived the amount of money lost as significant reported fear of repeat victimisation, those who found financial loss as insignificant were psychologically more relaxed. Wall (2005, p. 310) coins the modus operandi of online perpetrators utilising financially low impact cybercrime as *"de minimis"*. He maintains that this method, which entails stealing a small amount of money from multiple targets rather than stealing a huge amount of money from a single target, is an effective way of evading from being detected as well as decreasing reporting rate of incidents (Wall, 2008a, 2010c). The findings of this thesis suggest that de minimis aspect of economic cybercrime incidents also affect victims' threat perceptions which in turn impact fear of economic cybercrime.

Participants with well-paid jobs or those who are planning a prosperous career were more fearful of reputational damage caused by possible misuse of their personal information

acquired by online perpetrators. Fear of identity theft studies, as well as consumer purchase intention studies, also indicate that fear of reputational damage is one of the significant determinants of fear of crime (Sproule and Archer, 2007; Mukherjee and Dubé, 2012; Hille et al., 2015). The results of fear of cybercrime studies suggested a relationship between fear of cybercrime and low social status (Roberts et al., 2013).

#### 9.5.2.4 Behavioural Responses

Individuals' reactions to victimisation experiences are not limited to emotional responses such as anger or fear of crime, but negative experiences may also cause some behavioural responses (Henson, 2011; Riek et al., 2014). Coping perspectives are generally utilised to examine individuals' behavioural and emotional responses to incidents that act as stressors (Nyamathi, 1989; Verhaeghe et al., 2005) Coping is defined as the behavioural and emotional reactions to master the demands that are perceived as exceeding the capabilities of a person (Lazarus and Folkman, 1984). Emotional and behavioural responses performed to overcome the distress faced are generally classified under two groups: approach (problem-oriented) and avoidance (emotion-oriented) (Lazarus and Folkman, 1984; Roth and Cohen, 1986). Approach coping strategies encompass actions implemented to confront the problem faced and aimed to actively deal with the aversive consequences of negative life events (Compas et al., 1993). Avoidance coping strategies are more passive and entail running away from the problem or ignoring the threat (DeLongis and Holtzman, 2005). Empirical research suggests that individuals adopting avoidance strategies tend to internalise the problem, strive to hide their feelings or blame themselves (Holahan and Moos, 1987; Finset et al., 2002).

Prior victimisation experience is considered to be one of the most significant negative life experiences that may have an impact on coping strategies. (Frieze and Bookwala, 1996; Salston and Figley, 2003). The results of traditional crime studies suggested that individuals

adapted approach coping strategies (Scarpa et al., 2006; Benight, 2012) avoidance coping strategies (Leitenberg et al., 1992; May et al., 2010) or both of them at the same time (Green and Pomeroy, 2007) to master negative consequences of prior victimisation experiences. Coping literature indicates that adaption of coping strategies is highly contextual (Stahl and Caligiuri, 2005). Contextual factors such as personality of individuals involved, type of victimisation (i.e. either being a violent victimisation or not), personal and social circumstances or availability of counselling in the aftermath of criminal victimisation shaped the coping strategies adapted (Holahan and Moos, 1987; DeLongis and Holtzman, 2005; Tenenbaum et al., 2011).

As it was noted in the Literature Review Chapter (Chapter) the 'Coping' perspectives have been utilised as conceptual frameworks in online privacy, internet security and cyberbullying studies. The results of these studies suggested that prior negative online experiences like receiving unwanted communication, losing personal information over SNS or experiencing an online scam boosted protective behaviours (Parris et al., 2012; Chen et al., 2016; Thompson et al., 2017). The findings of this thesis suggest that behavioural responses to economic cybercrime victimisation may be summarised under two subcategories: changes in online lifestyle and security intentions. As it was noted in fear of crime section of this chapter, the type of victimisation impacted Internet users' threat and coping appraisals. Thus, the impact of victimisation experiences on individuals' behavioural responses and security intentions will be examined for each victimisation type.

### 9.5.3 Behavioural Responses

#### 9.5.3.1 Impact of Phishing Victimisation Experience on Behavioural Responses

Interviews with victims suggested age differences in behavioural responses to victimisation experiences. Interviews indicated a prevalence of low perceived vulnerability and

low perceived severity among young and middle-aged phishing victims. Being aware of the victimisation process and a small amount of money lost as a result of victimisation experiences emerged as the possible reasons for low perceived vulnerability and perceived severity among phishing victims. 'Approach' coping strategies were mostly adopted by young and middle-aged phishing victims. Reported approach coping strategies encompassed both behavioural changes like changing online shopping preferences as well as security intentions such as reading emails more carefully, checking transactions more frequently, using complex passwords and installing anti-virus programs.

It appears that low perceived vulnerability strengthened with low perceived severity lead to adaptation of approach coping strategies. Website phishing victims who perceived economic cybercrime as preventable seemed to change their online shopping habits rather than stopping online purchasing. Increasing guardianship measures to prevent future victimisation is another outcome of low perceived severity and low perceived vulnerability. It appears that phishing victim participants evaluated the risk of repeat victimisation with the perceived benefits of Internet purchasing. This trade-off between risk and perceived benefits, which is named as the calculus of behaviour (Wall, 2004), seemed to boost approach coping strategies.

Interviews with victim participants suggested that high perceived vulnerability and low-self efficacy emerged to be more prevalent among older participants. It seems that perceived vulnerability was mediated by low-self efficacy for older victim interviewees. Participants who reported low Internet self-efficacy also acknowledged concerns about experiencing cybercrime victimisation again. Victimisation experiences appeared to have varying impacts on older participants' behavioural adaptations. Older phishing victim participants adapted both approach coping and avoidance coping strategies to prevent future economic cybercrime victimisation. Older participants applied approach coping strategies like increasing their

guardianship measures to continue using online banking; however, they tended to implement passive avoidance behaviour like stopping shopping online.

The finding suggesting quitting online shopping as an avoidance behaviour to master perceived vulnerability and low self-efficacy was echoed in consumer shopping intention literature. Numerous research on customers' purchase intention illustrated that perceived risk, which is the combination of perceived vulnerability and perceived severity of consequences, influences Internet users' online purchase intention (Pappas, 2016; Kamalul Ariffin et al., 2018). Results of empirical studies indicate that the higher the perceived risk, the less likely individuals' shop online (Kim and Lennon, 2013; Zhao et al., 2017). The negative influence of perceived risk on shopping intention is found to be more prevalent among mature Internet users. The results of Chakraborty et al. (2016) suggests that senior citizens who experienced a data breach reported higher perceived risk which in turn lead to decreased online shopping intention.

However, the finding suggesting applying approach strategies like increased guardianship to continue online banking was unexpected. It is argued that older Internet users are more likely to stop using online banking when they feel vulnerable to financial loss or personal information breaches when compared to younger Internet users (Durkin et al., 2008; Kesharwani and Singh Bisht, 2012; Arenas Gaitán et al., 2015).

Ease of use which is affected by the design of the web pages may be one explanation of the tendency to stop online shopping while increasing guardianship to continue online banking among older participants. Web design is considered to be the utmost importance in accepting an online service (Ho and Lin, 2010; Chiu and Yang, 2016). It is argued that the design and interface of websites put a significant cognitive burden on older Internet users (Sato et al., 2011; Hussain et al., 2018). Older participants, who were mostly website phishing

victims, reported low Internet self-efficacy. Those older participants who perceived their Internet skills insufficient to carry out the difficult task required in online shopping sites may have preferred to stop using online purchasing. The interface of many Internet banking websites is more user-friendly and less complicated actions required to carry out intended online operations.

The relationship between low self-efficacy and application of safeguarding measure may be another explanation for the above mentioned unexpected result. Chen et al. (2016) argue that implementation of avoidance and approach coping strategies necessitates different levels of Internet skills. They maintain that Internet users with high Internet self-efficacy may easily apply security measures required to ensure a safer online environment whereas those who lack Internet skills may prefer applying avoidance strategies which are more passive. While installing anti-virus software and careful password management may be effective measures to ensure secure online banking usage, evading website phishing which may require differentiating between bogus and real websites may be a more daunting task for older Internet users.

#### 9.5.3.2 Impact of Hacking Victimisation Experience on Behavioural Response

Interviews with victims indicated that it is mostly younger Internet users who experienced economic cybercrime victimisation through hacking of online financial accounts. Hacking victims adopted both approach and avoidance strategies based on their perceived severity and vulnerability. Frijda (1988, p. 349) argues that “emotions arise in response to the meaning structures of given situations; different emotions arise in response to different meaning structures”. Similar events may cause different emotions depending on how individuals interpret the incidents they faced. It appears that the criteria that hacking victims utilised to evaluate their victimisation experiences had an impact on their coping appraisals.

While some participants evaluated their victimisation experiences with financial outcomes, others assessed their negative experiences with social outcomes such as reputational damage.

Hacking victims who evaluated their experiences with financial outcomes reported low perceived severity which in turn boosted passive avoidance strategies. Participants who were more relaxed about receiving a refund for their financial losses did not perceive the outcome of their victimisation as severe. Thus, they neither changed their online lifestyles nor applied any security measures to prevent future victimisation. Victim participants who were worried about reputational damage or possible misuse of their personal information perceived the outcomes of their victimisation more severe. For instance, one of the participants acknowledged worries about the possible use of her personal financial information to purchase illegal substances like drugs or explosives. Another male participant reported fear of future risks of possible misuse of credit card information since his credit card information was used to access online pornographic content. They also noted feeling vulnerable to future online attacks due to the loss of personal and financial information. These participants acknowledged applying approach coping strategies like installing anti-virus programs, limiting shared information through social media, checking bank statements regularly and using complex passwords.

Low perceived severity stemming from the feeling financially secure due to refund protection policies of financial institutions like banks is significant for both psychological well-being of Internet users and continuance of online service usage. Empirical studies researching the dynamics of e-commerce suggest trust as the most significant aspect of the business to customer (B2C) e-commerce due to financial uncertainties between consumers and online traders (Vatanasombut et al., 2008; Chen and Chou, 2012). Several measures such as the display of trust seals, professional web designs, clear return policies are proposed to overcome

trust barriers between online customers and merchants (Chang et al., 2013; Kim et al., 2016; Etzioni, 2017). The findings of this thesis suggest that apart from these trust-building strategies refund protection also fosters the sense of trust among Internet users. Nevertheless, findings also suggest that the sense of financial trust may also prevent Internet users from applying security measures to prevent further economic cybercrime victimisation.

The application of approach coping strategies to decrease the risk of personal information theft for fear of facing aversive social consequences indicates that theft of personal identifying information may have a more significant impact on individuals' online behavioural adaptation than financial loss. However, Hille et al. (2015) who examined the impact of fear of online identity theft on online purchase intention through a qualitative analysis of interviews found that fear of financial losses had a greater effect on Internet users' online purchasing intention when compared to the fear of reputational damage. The impact of direct victimisation experiences and indirect victimisation experiences may be an explanation for the discrepancy between the findings of this thesis suggesting fear of reputational damage as a major determinant of behavioural change and those of Hille et al. (2015) proposing fear of financial loss as a significant predictor of decreased purchasing intention. Whereas this thesis assessed victim participants' behavioural reactions to their victimisation experiences, Hille et al. (2015) evaluated the impact of non-victim participants' fear of online identity theft on online purchasing intention.

## 9.6 Evaluating the Applicability of LRAT to Economic Cybercrime Victimisation

As it was extensively discussed in Literature Review Chapter, Lifestyle Routine Activities Theory, which is the latest version of Opportunity Theories of Victimisation has been applied as a theoretical framework in cybercrime studies over the last decade. Whereas

some scholars (i.e. Bossler and Holt, 2009; van Wilsem, 2011; Holt and Bossler, 2013) preferred to utilise an original version of RAT or LRAT, some other scholars (Choi, 2008; Reyns et al., 2011) suggested adapted cyber versions of opportunity theories. These versions were examined in the First Literature Review Chapter extensively. This section of this chapter discusses the applicability of LRAT's concepts to economic cybercrime context.

### 9.6.1 Proximity to Motivated Offender

Hindelang et al. (1978) conceptualise proximity in terms of geographical closeness to the areas where potential offenders are mostly present. Proximity assumed to be a risk-enhancing factor since potential offenders would have more chance to observe potential targets' routine activities and security measures applied to protect homes. There is a reciprocal relationship between proximity and exposure. The more individuals reside near would be offenders, the more they are exposed to the risk of victimisation (Miethe and Meier, 1990). As it was extensively discussed in the Literature Review Chapter (Chapter Two), transposition of the proximity concept to cyberspace presents some difficulties since proximity in cyberspace is constant (Yar, 2005). Every Internet user virtually resides at the same distance to potential online offenders.

The significant overlap between two concepts, exposure and proximity, renders it difficult to operationalise proximity in cybercrime studies (Vakhitova et al., 2015). Scholars researching cybercrime victimisation operationalised these two concepts either as one concept (Bossler and Holt, 2009; Holt and Bossler, 2013) or they did not operationalise proximity concept in their studies (Leukfeldt, 2014; Leukfeldt, 2015; Leukfeldt and Yar, 2016). Only a few scholars operationalised proximity in their cybercrime research (Reyns et al., 2011; van Wilsem, 2013b; Reyns and Henson, 2016).

Proxy variables utilised to measure proximity element of the theory have varied. Reyns et al. (2011) utilised the number of strangers and friends allowed to access online social networks as the proxy measure of proximity concept. van Wilsem (2013b) used offending behaviour as proximity to a motivated offender. Harassing someone online and sending computer viruses were used as proxy measures. Lastly, Reyns and Henson (2016) assumed experiencing malware infection (virus, spyware or adware), phishing and hacking incidents as the proxy of proximity to the motivated offender for online identity theft victimisation. As can be seen, all of these measures fail to reflect the original concept of proximity, which denotes residing or being at a close distance to the places where offenders are mostly found.

To overcome this shortcoming of previous cybercrime studies, this thesis utilises *information disclosure* as a criterion to make a distinction between proximity and exposure to motivated offenders. Online activities that require personal information disclosure were proposed to be proxy measures of exposure concept. For instance, online shopping and online banking were used as a proxy of exposure in analyses since these activities require disclosure of personal or financial information. On the other hand, online activities such as reading newspaper, watching movies online or searching for information are assumed to be proxy measures of proximity to the motivated offender.

Bivariate analysis results presented in Chapter Five yielded proxy variables of proximity to the motivated offender, accessing the Internet for social networking, e-mail, instant messaging and chat rooms and browsing for news or information as statistically significant associates of economic cybercrime victimisation. Multivariate binary logistic regression analysis results indicated that accessing the Internet for email/instant messaging/chatrooms increase the risk of victimisation.

Interviews with victim participants suggested that the proximity concept is more applicable to experiencing economic cybercrime through hacking. It appears that Internet users' deviant online activities such as accessing free movies or sharing pirated media increase Internet users' proximity to hackers' tools, which are utilised to infect targeted computers to acquire personal or financial credentials.

The results of quantitative analysis of CSEW 2014/15 and findings of a qualitative analysis of semi-structured interviews suggest that the proximity concept, which denotes mere presence on certain websites, which can be considered as hotspots of the Internet, may facilitate being the target of an online attack. It seems that certain websites are utilised as hotspots of cybercrime to disseminate malware. Internet users who visit these websites may encounter some risks regardless of yielding any information or even taking any action due to the ability of some hidden scripts to load them on target devices through drive-by-download. Thus, the results and findings of this thesis support the applicability of the proximity concept of LRAT to cybercrime victimisation. Thus, it may be alleged that proximity to motivated offenders' tools increases the odds of becoming a victim of economic cybercrime.

### 9.6.2 Exposure to Motivated Offenders

Opportunity theories of victimisation posit that both vocational and leisure activities which require spending time out of the home settings increase the risk of victimisation through converging potential targets and would be offenders (Hindelang et al., 1978; Cohen and Felson, 1979; Cohen and Cantor, 1981). Exposure to risky situations or motivated offenders is presented as the outcome of individuals' lifestyles and routine activities (Cohen and Cantor, 1981). Exposure to motivated offender is operationalised as outdoor activities like going bars at night or the amount of time spent outside home settings and drinking habits, peer involvement in real-world studies (Miethe et al., 1987; Sampson and Wooldredge, 1987;

Miethe and McDowall, 1993; Tillyer et al., 2011; Bellone, 2013). Regarding cybercrime, context exposure is operationalised with both deviant and normal online activities and time spent online (Marcum, 2011; van Wilsem, 2011; Holt and Bossler, 2013; Jansen and Leukfeldt, 2015). This research operationalised online activities that require personal and financial information disclosure and amount of time spent online as the proxy measures of exposure to online perpetrators while conducting a quantitative analysis of CSEW 2014/2015 in Chapter Five.

Bivariate analysis results of CSEW 2014/2015 suggested a statistically significant relationship between accessing the Internet for online banking, buying goods or services online and online governmental services and economic cybercrime victimisation. Multivariate binary logistic regression analysis result indicated that Internet users who accessed the Internet for buying goods or services online, using online governmental services were at higher risk of victimisation when compared to those who did not use these online services.

To triangulate quantitative analysis results, participants were asked about the online activities they mostly engaged while they accessed the Internet. SNS, online leisure activities playing online games or reading newspapers, online financial activities online banking and online shopping, online leisure or vocational activities checking emails and browsing for information emerged as the most frequently accessed online activities. The comparison of the online activity patterns of both victim and non-victim control group indicated no significant differences between these two groups. This finding suggested that the results of quantitative analysis yielded an association between Internet users' online lifestyle and risk of victimisation rather than a causal relationship.

Personal information disclosure emerged as the main antecedent of exposure to the motivated offender. Voluntary personal information disclosure through online advertisement

websites, online networking websites, to be eligible for free Wi-Fi and involuntary personal information disclosure through data breaches of big companies holding personal and financial information of Internet users emerged as a reason for receiving unsolicited emails. It appears that exposed personal information was utilised to send both phishing emails and SMiShing (SMS phishing) messages. Thus, the result of quantitative and qualitative analysis results suggested the applicability of exposure concept to cybercrime victimisation studies.

However, it should be noted that proximity and exposure concepts were found to be associated with the pre-victimisation phase of economic cybercrime victimisation. In other words, engaging with online activities like online shopping, online banking or selling goods online increased the odds of being a target of an online attack. Being a target of an online attack does not necessarily lead to victimisation. Control group participants acknowledged thwarting online attacks successfully.

It is argued that the main postulate of opportunity theories of victimisation, which conceives lifestyle or routine activities as main facilitator victimisation, is an unfalsifiable tautology (Walklate, 1989) since it is a mere description of crime events (Sutton, 2014). (Garofalo, 1986) issued an updated version of LET, where he made a distinction between "absolute and probabilistic exposure to risk". Garofalo (1986) argues that absolute exposure to risks, which is the function of individuals' lifestyles, is a necessary condition for the occurrence of a crime event. He posits that it is the probabilistic exposure risk that is the outcome of the frequency of engaging with risky activities or frequency being at close proximity to would be offenders that increases the chances of victimisation. Garofalo's (1986) distinction between necessary and sufficient conditions of victimisation has been ignored in cybercrime victimisation studies. Previous cybercrime studies perceived online activities like online shopping and online banking as both necessary and sufficient conditions of cybercrime victimisation.

However, this thesis proposes that engaging online activities, either deviant or normal, present necessary conditions of being a victim of cybercrime. Quantitative bivariate analysis conducted to test the strength of the relationship between online activities and the risk of economic cybercrime demonstrated that the mentioned relationship was very weak. This weak relationship may be interpreted as a minor contribution of normal online behaviours like shopping online to the odds of becoming a victim. Thus, these online activities should not be perceived as sufficient conditions of victimisation. Qualitative analysis of semi-structured interviews indicated that it might be the contextual vulnerabilities that distinguish victims from non-victims when individuals encounter with online threats.

### 9.6.3 The absence of Capable Guardianship

Opportunity theories of victimisation conceive the absence of capable guardianship as one of the three components of a victimisation event (Cohen and Felson, 1979). It is proposed that the absence of a guardian capable of deterring a threat increase the chances of being a victim of a crime (Cohen et al., 1981). A capable guardian is not only perceived as a means of impeding an immediate threat but also a factor alleviating target attractiveness of a person or an object (Meier and Miethe, 1993). As was noted in the First Literature Review Chapter (Chapter Two), the results of previous cybercrime studies yielded mixed results about the effectiveness of guardianship measures in preventing cybercrime victimisation. Whereas the results of some studies suggested that guardianship measures decreased the risk of victimisation (Choi, 2008; Williams, 2015), the results of some others indicated that application of online security measures increased the risk of victimisation (Ngo and Paternoster, 2011; Reyns et al., 2016). Some other cybercrime studies found no association between guardianship measures and cybercrime victimisation (Hutchings and Hayes, 2008; Bossler and Holt, 2009; Marcum, 2011; van Wilsem, 2013b; Leukfeldt, 2014).

To examine the effect of guardianship measures on the risk of experiencing economic cybercrime victimisation, quantitative analysis of CSEW 2014/2015 and qualitative analysis of semi-structured interviews utilised. bivariate statistical analysis results presented in Chapter Five suggested a statistically significant association between guardianship measures applied to protect electronic devices and personal account. Multivariate binary logistic regression results, however, suggested anti-virus or other security software usage as a statistically significant predictor of economic cybercrime victimisation. Though, the impact of security software usage was contrary to expectations. The logistic regression analysis result indicated that those who used security software were at increased risk of victimisation. This unexpected result may be explained with the confusion among participants with regard to the temporal order of occasions. Participants who installed security software after experiencing victimisation may have confused the time that they installed the software. Failure of security software to protect electronic devices may be another unexpected result. Qualitative analysis of semi-structured interviews appears to support the second scenario since of the twenty-one victim participants who acknowledged using security software prior to victimisation incidents; eleven participants reported experiencing hacking victimisation. The results and finding of this thesis supported LRAT's proposition underscoring the significance of guardianship in preventing victimisation.

Overall, the results and findings of this thesis suggest that LRAT, which is the latest version of opportunity theories of victimisation is applicable to economic cybercrime context. The hypothesis assuming a relationship between individuals' lifestyles (proximity and exposure to motivated offender), absence of capable guardianship and risk of experiencing economic cybercrime victimisation were supported both via statistical analysis of CSEW 2014/2015 and qualitative analysis of semi-structured interviews and police reports pertaining to economic cybercrime cases occurred in a city in Northeast of the UK in 2015.

Despite its applicability to economic cybercrime victimisation context, still, LRAT presented some shortcomings. Firstly, LRAT focuses on an individual level (micro) correlates of a victimisation event; however, the results of this thesis suggested that aggregate level (macro level) factors also impacted the risk of victimisation. Secondly, LRAT downplays the importance of contextual factors in victims' lives in the occurrence of victimisation. Although individuals' lifestyles are proposed to be the main facilitator of victimisation, factors affecting individuals' lifestyles and decision-making processes when individuals faced a threat are either ignored or assumed as constant for all individuals. Lastly, LRAT does not consider the impact of behavioural and psychological consequences of victimisation experiences on the risk of repeat victimisation. The findings of this thesis suggested that prior victimisation has significant consequences on individuals' security intentions. Thus, this thesis proposes a contextual vulnerability approach and an Integrated Cyber Victimisation model as a remedy for these shortcomings of LRAT.

## 9.7 Summary

This Discussion Chapter aimed to critically evaluate the findings of this doctoral thesis in the light of theoretical and conceptual frameworks that informed the research process. The findings of this thesis illustrate that economic cybercrime victimisation is a multi-faceted complex issue. Contrary to past empirical cybercrime victimisation research, which perceived Internet users' online lifestyles as the main source of cybercrime victimisation, findings of this thesis suggest that contextual factors (individual, macro or socio-cultural) may have influence the likelihood of experiencing economic cybercrime victimisation. Demonstrating applicability of Lifestyle Routine Activities Theory (LRAT), Protection Motivation Theory (PMT) and Approach-Avoidance Coping Paradigm while examining the cognitive process of Internet users when they were exposed to online threats and impacts of victimisation experiences on

Internet users' lifestyles is another significant contribution of this thesis. Implications of unique contributions of this doctoral research, the Contextual Vulnerabilities Approach and The Integrated Cyber Victimisation Model, which incorporates these three theories into one single model, will be explained in the next Conclusion Chapter (Chapter Ten).

# Chapter 10 Conclusion

## 10.1 Introduction

This concluding chapter recapitulates the central arguments of this doctoral research. The first section of the chapter provides a summary of research findings. The second section of the chapter presents the novel contributions of this thesis (The Contextual Vulnerabilities Approach and Integrated Cyber Victimisation Model) to cybercrime victimisation knowledge. The penultimate section of the chapter discusses the limitations of this doctoral research and the implications of the findings for the governance and policing of the Internet. The final section of the chapter presents the recommendations for future studies.

The Internet has been an integral and inevitable part of our daily routines. It has numerous applications that can make our lives easier and more enjoyable. However, this widespread use of the Internet has also created new opportunities for perpetrators to commit traditional crimes in increasingly large volumes while remaining relatively anonymous. Additionally, the cyberspace environment has given rise to new forms of online crimes like malware distribution, which would not exist in the absence of networked Internet technologies. These threats are coupled with the commercial use of the Internet. Online shopping and Internet banking are the most vivid examples of commercialisation of the Internet. Online perpetrators strive to acquire financial gain from both online retailers and individual Internet users. Extant research illustrates that economic cybercrime poses a significant threat to individuals, businesses and governments (Levi et al., 2015; Munjal, 2016; Pathak, 2016a; Levi et al., 2017). Despite growing interest in cybercrime victimisation, there is a dearth of theoretically informed empirical research on economic cybercrime victimisation. This thesis aimed to address this gap in the cybercrime victimisation literature. This thesis also strived to examine the antecedents

of being a target of an online attack, conditions that facilitated victimisation and impact of victimisation experiences on individuals' behavioural adaptation and security intention. Up to date, cybercrime victimisation studies examined mentioned dimensions of victimisation in separate studies. This doctoral thesis is one of the first pieces of research that examines cybercrime victimisation holistically. The aims of this doctoral research were:

g) To explore factors that render some Internet users a target of an online attack;

h) To examine the decision-making process of Internet users when they face an online threat;

i) To explore factors increasing the risk of being a victim of economic cybercrime;

j) To explore the impact of technological vulnerabilities on the risk of becoming a victim of economic cybercrime;

k) To identify and understand the emotional and behavioural impacts of economic cybercrime victimisation on individuals' online lifestyles;

l) To test the applicability of LRAT as a theoretical framework to economic cybercrime victimisation and address the theoretical shortcomings of LRAT in economic cybercrime victimisation context.

A mixed-methods approach was adapted to achieve these aims. A significant body of cybercrime victimisation literature utilised quantitative research methods to examine the correlates of cybercrime victimisation. Being descriptive was the main shortcoming of these studies. Though these studies illustrated statistically significant associations between online lifestyle variables such as online shopping or online banking and risk of experiencing cybercrime victimisation, they failed to account for the underlying reasons for the mentioned statistical relationships. Thus, the voices of cybercrime victims were not echoed in extant research. Only a handful of studies (Li, 2005; Burgard and Schlembach, 2013; Jansen and

Leukfeldt, 2016) conducted qualitatively driven research to examine cybercrime victimisation. However, a lack of generalisable results are the main limitations of qualitatively informed studies (Patton, 2002; Bryman, 2008). To address these methodological shortcomings of the extant research, a mixed methods research methodology was applied. Mixed-methods research methodology provided a number of benefits for this doctoral thesis.

A sequential mixed-methods methodology was utilised to enable quantitative analysis results to inform the qualitative phase of the thesis. Interviews guides were shaped according to the outcomes of the quantitative phase of the research. Thus, development was the first benefit of the research methodology. Triangulating quantitative analysis results was another advantage of applying a mixed-methods research paradigm. For instance, quantitative analysis results suggested that the type of electronic device utilised to access the Internet was associated with an increased risk of victimisation. This result was triangulated through semi-structured interviews. Findings of qualitative analysis supported the results of quantitative analyses suggesting mobile devices, the laptop used away from home settings and tablets as a risk factor for victimisation.

A mixed-methods research design was also helpful in expanding and explaining the results of the first phase of the research. Though the initial phase of the research indicated that type of electronic device utilised to access the Internet was associated with risk of victimisation, the impact of other technological factors could not be analysed due to limitations of CSEW 2014/2015. The Qualitative phase of the research expanded this issue and illustrated that mobile applications and Wi-Fi usage were other technological factors facilitating victimisation. This Qualitative phase of the research also helped to explain the unexpected results of the quantitative analysis. For instance, quantitative analysis results suggested a relationship between online government service usage and the risk of victimisation. Semi-structured

interviews indicated bogus websites mimicking government websites or websites charging money for some free governmental services as explanations of the mentioned association.

Complementarity, which denotes incorporating the strength of each research paradigm into the research process, was another advantage of utilising a mixed-methods methodology. Semi-structured interviews with the victim and non-victim control group participants illustrated the adverse effects of victimisation experiences through the lenses of victims. For instance, past empirical research on fear of crime and perceived risk of victimisation was mainly based on quantitative analysis of self-report surveys. Hollway and Jefferson (1997) argue that fear of crime can better be understood through biography and experiences of individuals. Semi-structured interviews with victims of economic cybercrime provided an in-depth understanding of the adverse impacts of victimisation experiences on Internet users' psychological well-being and behavioural adaptations.

## 10.2 Summary of Findings

### 10.2.1 Being a Target of an Online Attack

The first research question was: *What are the factors renders Internet users susceptible to be the target of an online attack?* This research question was aimed to understand why some Internet users are being targeted by online perpetrators, while some others access the Internet without being a target of an online attack. Understanding the factors that distinguish these two groups of Internet users was the central concern of this research question. Discerning the factors that distinguish Internet users who are targeted online from those who have not been targeted may be helpful for implementing proactive initiatives to combat economic cybercrime. A review of the literature suggested that there is a dearth of research studying the causes of being a target of an online attack. Only a handful of online fraud victimisation studies (Holtfreter et al., 2008; Pratt et al., 2010; Policastro and Payne, 2014) examined the correlates of being

targeted online. The results of these empirical studies suggest frequent use of the Internet and online purchasing as the antecedents of being targeted online (Holtfreter et al., 2008; Pratt et al., 2010).

Semi-structured interviews and police reports illustrated that email phishing, website phishing, hacking and online scams (scareware, tech support scam and ransomware scam) were the online threats that Internet users experienced. Qualitative analysis of data suggested that the factors that render Internet users an online target varied according to the type of threat. While personal information disclosure increased the chance of being an email phishing attempt, engaging with online deviance like illegal downloading or visiting adult content websites enhanced the odds of being a target of hacking or online scam due to malware infection. Website phishing victims were mostly targeted by websites that they accessed through hitting the most popular search engine results.

Low perceived severity and perceived vulnerability were found to increase the propensity to disclose personal information through SNS. It appeared that participants did not perceive email addresses as something personal. Moreover, the perceived benefits of sharing information while selling goods online or posting personal information to SNS for establishing professional networking also emerged to increase the chance of being a target of an email phishing attempt. In addition to voluntary personal information disclosure, involuntary personal information disclosure stemming from the data breaches of companies holding personal information of Internet users seemed to be associated with being an email phishing target.

Illegal downloading, peer-to-peer sharing, torrent downloading, online streaming and watching free online adult content movies were most cited online deviant activities. It appears that engaging with online deviance increased the odds of malware infection which facilitates

both being a target of hacking or online scams like ransomware scam. Traditional crime studies named some places (i.e. bars, night clubs or parks at night) where criminals mostly present as hotspots of crime (Meier and Miethe, 1993; Johnson and Bowers, 2008). Interviews of this research suggest that websites are offering free streaming, illegal downloading and adult content may be considered as the hotspots of the Internet, where malware is distributed. It appears that Internet users visiting these websites run the risk of malware infection because of drive-by-download attempts.

### 10.2.2 Process of Becoming a Victim

The second and third research questions were: *What factors affect Internet users' decision making-system when they face an online threat? And: How do technological vulnerabilities impact the chance of being a victim of economic cybercrime?* Previous cybercrime victimisation studies heavily focus on discerning online activities and demographic characteristics of individuals that are associated with the risk of victimisation. Although this thesis also researched the relationship between the type of online activities engaged and the risk of economic cybercrime victimisation, the main aim of this thesis was to understand why some online activities are associated with the risk of victimisation and how Internet users lose their personal or financial information. To that end, the victimisation processes of Internet users were examined through quantitative analysis of CSEW 2014/2015 and qualitative analysis of semi-structured interviews and the content of police reports. The results of the quantitative analysis suggested weak relationships between online activities and the risk of victimisation. These weak relationships indicated the existence of other factors that impact the chance of victimisation. Qualitative analysis suggested a number of factors that impact Internet users' decision-making processes when they face an online threat. This thesis names these factors as

contextual vulnerabilities. Factors facilitating the victimisation process will be presented within this framework.

### 10.2.3 Contextual Vulnerabilities Approach

Vulnerability, as a concept, can be traced back to the Ancient Greek Mythology, where invincible Achilles was killed in the Trojan War. Paris was able to kill Achilles due to the weakness in his heel. The word vulnerable is a derived the form of a Latin word *vulnerare* meaning wound (Pereira et al., 2016). *The term vulnerability* can be defined as the state of being open to attacks or damages (Merriam Webster, 2016). The vulnerability can also be defined in terms of the level of risks or harm that certain groups or individuals may face (Green, 2012). For this perspective, vulnerability means facing *"a significant probability of incurring identifiable harm while substantially lacking the ability and/or means to protect oneself"* (Pereira and Matos, 2016, p. 117). From information security perspective vulnerability denotes, "a weakness in information system security design, procedures, implementation or internal controls that could be exploited to gain unauthorized access to information or information system." (Maddison and Jeske, 2014, p. 21).

This thesis considering cyberspace as a socio-technological system, which is the outcome of interactions between human and technology components of virtual space (Virtanen, 2017), conceives vulnerability as any personal, social or technological weakness that increases the probability of being exposed to online attacks aimed to acquire financial gain. Contextual vulnerabilities are the outcomes of criminogenic interactions, which are heavily influenced by social, cultural and personal factors, between Internet users and either online perpetrators or their tools.

Keith (2018) categorises vulnerabilities into three distinct groups as an individual (micro level), neighbourhood (macro level) and context-specific level. Based on his

categorisation and the findings of this thesis, contextual vulnerabilities are divided into three groups: individual, macro and socio-cultural vulnerabilities.

#### 10.2.3.1 Individual and Behavioural (Micro Level) Vulnerabilities

The individual vulnerability is seen as something internal, which is embodied in us. From this perspective, vulnerability is the ontological condition of being a human being (Cornelius, 2016).We inherit this kind of vulnerability from birth and carry out through our lives. Hence, it is perceived as a universal phenomenon, which is embodied in every individual (Hille et al., 2015). In other words, it is a "conditio humana", an inevitable part of our existence (Jennings et al., 2007, p. 282). We are prone to diseases, illnesses and injuries due to embodied vulnerabilities. This inherent vulnerability is beyond the control of humanity (Hille et al., 2015; Cornelius, 2016) and it is the source of dependence on other people (Gutt and Randa, 2016). However, this thesis conceives individual vulnerability in a more general sense. It not only encompasses biologically inherent vulnerabilities, but it also encapsulates acquired attributes like the level of education or Internet skills.

Age emerged as one of the significant individual factors increasing Internet users' vulnerability to online threats. Age did not emerge as an intrinsic attribute of getting older, which hampers cognitive abilities, but as a function of Internet self-efficacy. Prensky (2001, p. 2) uses the terms "digital immigrants" and "digital natives" to differentiate between the Internet skills of Baby Boomers and Generation Y Internet users. He argues that digital immigrants who met networked Internet technologies face difficulties in adapting to the norms and, rules of these new environments. However, it is a way of living for digital natives who were born with these technologies. The findings of this thesis suggest that digital immigrants have difficulties in understanding potential online threats and lack the required skills to deter them. Lack of Internet skills appears to render older Internet users susceptible to website phishing threats.

Gender was another individual vulnerability that appears to impact the risk of victimisation. Both quantitative and qualitative analysis results indicated that female Internet users were more likely to be a victim of economic cybercrime. Moreover, the results of quantitative analysis of CSEW 2014/2015 suggested that Internet users with low household income and lower educational levels were at increased risk of economic cybercrime victimisation due to engaging with online financial activities.

Self-efficacy, perceived vulnerability, perceived severity and perceived rewards emerged as other individual factors impacting the risk of victimisation when individuals' face a threat. Security studies argue that the human is the weakest chain in computer security (Schafer et al., 2006; Franklin and Franklin, 2009) due to human reasoning which can be exploited by external manipulations (Cook and Fox, 2011). The findings of this thesis suggest that human reasoning is subject to make erroneous decisions due to the impacts of these factors. The impacts of these individual factors will be detailed in the next section where the Integrated Cyber Victimisation Model will be explained.

Password fatigue also emerged as an essential behavioural factor affecting the risk of victimisation through hacking. Interviews suggested that participants have many online accounts either financial or non-financial, which require a username and password to log in. It appears that Internet users tend to use the same username and password for different online accounts. Thus, in case of loss of any personal details, this may also facilitate financial or personal information saved on other accounts.

#### 10.2.3.2 Macro Vulnerabilities

Miethe and McDowall (1993, p. 743) argue that contextual variables should be included in crime analysis since "individuals' risks of victimisation are determined to some extent by social forces in their wider environment". This approach aims to incorporate individual level

(micro) and aggregate level (macro) factors in understanding the conditions leading to victimisation (Rader et al., 2007). Several traditional crime studies (e.g. Rountree and Clayton, 1999; Kanan and Pruitt, 2002; Rader, 2004; Wyant, 2008) utilised contextual variables such as neighbourhood characteristics, socioeconomic status in their analysis successfully. The extensive review of the literature suggested that cybercrime studies utilising crime opportunity theories of victimisation have focused solely on individual-level factors such as online activities engaged or demographics of Internet users. It appears that the extant cybercrime research has downplayed the role of contextual factors in the occurrence of cybercrime victimisation. This thesis is one of the first empirical cybercrime victimisation research striving to incorporate micro and macro level causes of economic cybercrime victimisation. Technological vulnerabilities and data breaches of bodies holding personal and financial information of Internet users emerged as two macro-level vulnerabilities that increased the risk of being a target of an online attack and odds of becoming a victim of economic cybercrime.

Pamphlet (2010, p. 8) argues that cyberspace is composed of three layers, i.e. "a physical layer, a logical layer and a social layer." We may also add devices utilised to connect the Internet as the fourth layer of cyberspace. Although new Internet technologies are introduced to increase the ease of accessing the Internet, they may sometimes have secondary-knock-on- effects (Wall, 2001). Devices such as tablets and smartphones are increasingly used to access the Internet. However, these devices have many security problems, which are exploited by perpetrators to obtain personal information (Cobbina et al., 2008; van Eijk, 2017). As mentioned above, the results of the quantitative analysis of CSEW 2014/2105 and qualitative analysis of semi-structured interviews suggested the type of device utilised to access the Internet had an impact on the risk of experiencing economic cybercrime victimisation. Mobile phones or smartphones and hand-held computers (tablets or iPads) emerged as a risk factor for online banking fraud and hacking victimisation.

Mobile applications appeared to be another technological vulnerability that increased the risk of victimisation. Bogus mobile applications mimicking popular applications and administrative privileges given to mobile applications to access the personal data were vulnerabilities identified. Although security literature proposes that mobile application usage poses a threat to mobile device users (Madriz, 1997; Jain and Shanbhag, 2012), this research is one of the first cybercrime victimisation studies documenting the risk of mobile applications for online identity theft and economic cybercrime victimisation.

The type of Internet connection was another technological vulnerability that facilitated economic cybercrime victimisation. Statistical analysis of CSEW 2014/2105 suggest laptops used away from secure Internet connection as a risk factor. Also, victim participants' accounts reporting free Wi-Fi offered at hotels, airports and public places as other possible reasons for losing financial information point out the type of Internet connection a technological vulnerability that enhance the risk of victimisation.

Data breaches of agencies holding Internet users' personal details emerged as a macro level vulnerability that increased the risk of being a target of an online attack. Interviews with both victim and non-victim participants yielded that some participants experienced the increased volume of phishing attempts in the aftermath of notorious hacking incidents of Talk Talk and Vodafone. Although these companies assured their clients that loss of information is limited, there were still individuals targeted because of stolen data.

Online merchants that save personal financial information of their customers and online shopping sites that failed to provide a secure environment emerged as another macro vulnerability that facilitated economic cybercrime victimisation. Participants who shopped through these poorly secured websites reported unauthorised use of their banking card information.

Failure of search engines in detecting websites utilising fake pop-up or scam messages to coerce Internet users into paying a ransom through fear-evoking messages or fraudulent websites mimicking the real government sites emerged as another macro level vulnerability that increases the risk of victimisation through website phishing.

Interestingly, refund protection emerged as also a risk factor increasing risk-taking behaviours of Internet users. Shopping from random online sellers rather than reputable online traders was a reason for losing money through website phishing. Participants acknowledged a sense of relief provided by the possibility of getting a refund due to refund protection as a rationale for preferring a random online seller who offers a competitive price.

#### 10.2.3.3 Socio-cultural (Context Specific) Vulnerabilities

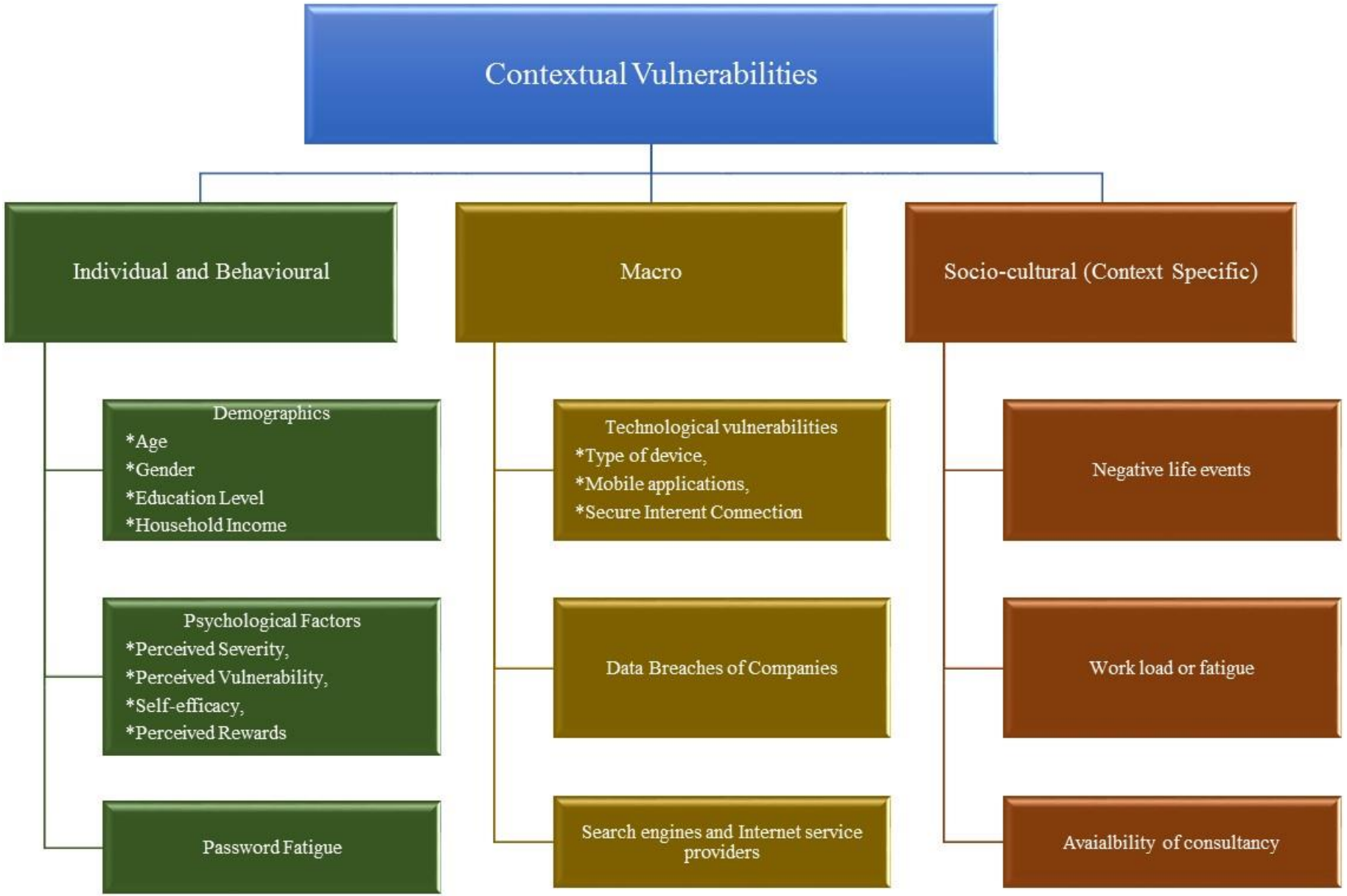
Crime victimisation is the outcome of the individual's interaction with their environment and other people. However, most empirical studies fail to observe the complexities of these settings and social interactions (Hope, 2012). Socio-cultural or context-specific vulnerabilities, which are the outcomes of the interactions between individual and macro vulnerabilities, are the third category of contextual vulnerabilities. Context-specific vulnerabilities that emerged as risk factors underscore the fact that economic cybercrime victimisation is a dynamic, multi-dimensional phenomenon mainly formed by the social, cultural and psychological background of individuals. The decreasing of guardianship of Internet users while facing an online threat was the main aspect of context-specific vulnerabilities. Interviews suggested that participants who experienced context specific vulnerabilities at the time of experiencing an online threat were more likely to make decisions based on heuristic decision-making process rather than a systematic decision-making process.

Negative life events, having financial difficulties, breaking a long-term relationship or family problems such a severe illness of a family member emerged as a context-specific

vulnerability that either lead Internet users to engage with risky online activities or to make decisions with decreased attention. Living alone emerged as another social vulnerability that impacted the risk of victimisation. Older participants who were living alone or in sheltered accommodation emerged to be at increased risk of victimisation due to lack of any personal support when they faced a threat.

The time that Internet users accessed the Internet appeared to be another context specific vulnerability. For instance, while a participant made an erroneous decision because of the presence of a child urging to purchase a popular online game character, another participant yielded financial information to a phishing email due to the absence of anyone to ask help.

Peak sale periods emerged to be a socio-cultural vulnerability that impacted the likelihood of experiencing economic cybercrime victimisation. Interviews conducted with both victim and non-victim participants indicated that Internet users increased their online purchases during special time periods such as Valentine's Day or Christmas. It appears that rushing to find out a rare presents like Elvis Cards rendered Internet users' susceptible to website phishing.


Contextual Vulnerabilities
Individual and Behavioural
Macro
Socio-cultural (Context Specific)
Demographics
*Age
*Gender
*Education Level
*Household Income
Psychological Factors
*Perceived Severity,
*Perceived Vulnerability,
*Self-efficacy,
*Perceived Rewards
Password Fatigue
Technological vulnerabilities
*Type of device,
*Mobile applications,
*Secure Interent Connection
Data Breaches of Companies
Search engines and Internet service providers
Negative life events
Work load or fatigue
Avaialbility of consultancy

### 10.2.4 Impacts of Victimisation

The fourth research question was: *What is the impact of economic cybercrime victimisation on Internet users' behavioural and security adaptations?* It is argued that apart from financial loss, economic crimes may have adverse impacts on victims' psychological well-being and behavioural responses (Box et al., 1988; Button et al., 2009) and these negative impacts of economic crime victimisation may sometimes be as severe as violent crimes (Eaton, 1999; Barnard, 2001). However, extant cybercrime victimisation literature has not examined the influence of victimisation experiences on individuals' behavioural adaptations and security intentions, and this thesis attempts to address that.

Interviews with victims suggested that shock and panic were the initial negative feelings when victims realised their victimisation. These feelings are replaced with the annoyance caused by dealing with formalities such as restoring account details or cancelling credit cards in the aftermath of victimisation. Anger was another strong feeling experienced. It seems that although these feelings were short-term, fear of economic cybercrime victimisation was more persistent among participants.

Although the fear of traditional crime studies suggested the prevalence of fear of crime among females, the findings of this thesis suggested no significant gender differences in fear of economic cybercrime victimisation. Yet, older female participants reported a higher fear of economic cybercrime. These findings indicating the higher levels of fear of crime among older female participants may be attributed to the Internet skills of younger females. Expansion of the Internet seems to nullify the gender difference in accessing the Internet, which in turn boosted female Internet users' confidence and Internet skills.

Semi-structured interviews indicated that the type of victimisation experienced influenced fear of economic cybercrime. While fear of economic cybercrime was more

prevalent among hacking victims, phishing victims were less fearful of economic cybercrime victimisation. Being aware of the victimisation process and the factors that lead to victimisation appeared to be the main reason for this difference.

With regard to impacts of psychological factors, perceived severity of consequences seemed to boost fear of economic cybercrime. Whereas participants with well-paid jobs were more fearful about the possibility of damaging their reputation or misuse of their personal and financial information to commit more serious crimes, those with lower income were more concerned about getting a refund.

Regarding behavioural responses to economic cybercrime victimisation, young and middle-aged phishing victims' adapted approach coping strategies, which means they actively seek solutions to prevent future victimisation while continuing using the Internet. Reading emails carefully, checking transactions frequently, installing ant-virus software and using complex passwords were most cited approach coping strategies. Older phishing victims applied both approach coping and avoidance coping strategies in the aftermath of victimisation. Interviews suggested that older participants who perceived themselves vulnerable to victimisation applied passive avoidance strategies for online financial activities. This means that they stopped online shopping to prevent future victimisation.

It appears that perceived vulnerability and perceived consequences of victimisation influenced hacking victims coping strategies. Hacking victims seemed to apply both approaches and active avoidance strategies to prevent future victimisation. Installing anti-virus software, checking bank statements regularly, limiting shared information online and using complex passwords emerged as approach coping strategies applied.

### 10.2.5 Applicability of LRAT to Economic Cybercrime Victimisation

The fifth research question was: *Can Lifestyle Routine Activities Theory provide a sound theoretical framework to explain the economic cybercrime victimisation in cyberspace?* Scholars (Gale and Coupe, 2005; Holt and Bossler, 2014; Leukfeldt and Yar, 2016) emphasise the need for the theoretical work to explain victimisation in the cyberspace. Up to date Lifestyle, Routine Activities Theory is the most favoured and tested theory to explain victimisation in cyberspace (Bossler and Holt, 2010; Reyns et al., 2011; van Wilsem, 2013a). However, as it was analysed in the literature review section of this report, the applicability of Lifestyle Routine Activities Theory to cyber victimisation is questionable (Ngo and Paternoster, 2011; Holt and Bossler, 2014). It is argued that transposition of some conceptual elements of theory to the cyberspace environment introduces some problems (Yar, 2005).

Previous cybercrime studies testing the applicability of LRAT to cybercrime yielded inconsistent results. Whereas the results of (Choi, 2008; Reyns et al., 2011) yielded support, the results of (Bossler and Holt, 2009; Marcum et al., 2010; Holt and Bossler, 2013; van Wilsem, 2013b; Leukfeldt and Yar, 2016) suggested partial support. Yet, (Ngo and Paternoster, 2011) and (Policastro and Payne, 2014) found no empirical support of the applicability of theory to cybercrime victimisation. The results of this thesis suggest that all conceptual components of theory can successfully be applied to economic cybercrime victimisation. Thus, this thesis illustrates that LRAT is a suitable theoretical framework to examine economic cybercrime victimisation. However, some limitations of the theory are also observed. This section of the chapter aims to address the shortcomings of LRAT.

As it is highlighted previously, LRAT conceives individuals' lifestyles and demographic characteristics as a facilitator of victimisation. The theory, in essence, deals with individual-level factors. Thus, it downplays the impacts of macro variables on the chance of

becoming a victim. Miethe and McDowall (1993) argue that multi-level contextual analyses can act as a bridge between two levels. The contextual vulnerabilities approach, which considers both individual and aggregate level factors as a potential source of victimisation, aims to address this shortcoming of the theory.

LRAT posits that the absence of a capable guardianship is a significant factor for the occurrence of a crime event. However, theory accounts for neither the factors that motivate individuals to implement safeguarding measures nor the decision-making process of applying a safeguarding measure. This thesis suggests Rogers' (1975) Protection Motivation Theory (PMT) as a conceptual framework to examine Internet users' decision-making process when they face an online threat.

LRAT does not account for the impacts of victimisation on individuals' behavioural adaptations and security intentions. The findings of this thesis indicate that behavioural adaptations and changes in security intention may facilitate repeat victimisation. Analysis of semi-structured interviews illustrated that eight out of thirty-two participants experienced repeat victimisation. Some participants experiencing repeat victimisation acknowledged the possibility of making the same mistakes which caused victimisation several times. This thesis illustrated that approach-avoidance paradigm (Lazarus and Folkman, 1984; Roth and Cohen, 1986) might be a sound conceptual framework to examine impacts of victimisation experiences on Internet users' behavioural adaptations and security intentions. Though the approach-avoidance coping paradigm has been increasingly utilised in Internet Technologies related studies, this approach has limited application in cybercrime studies. Only some cyberbullying studies (Price and Dalgleish, 2010; Šléglová and Cerna, 2011; Machmutow et al., 2012; Parris et al., 2012; Machackova et al., 2013) utilised a coping approach to understand college students survival strategies after experiencing cyberbullying. Integrating this approach to LRAT may

be helpful in examining factors leading to cybercrime victimisation holistically. Overall, this thesis proposes an Integrated Cyber Victimisation Model (ICVM) to address the aforementioned shortcomings of LRAT as a theoretical framework.

## 10.3 Integrated Cyber Victimisation Model

This thesis utilised LRAT, PMT and Coping Approach as a theoretical and conceptual framework while examining each dimension of economic cybercrime victimisation. Components of ICVM, which is the fusion of these three theoretical approaches, will be discussed here.

As mentioned earlier, previous cybercrime victimisation studies examined different phases of victimisation in separate studies. For instance, while some studies researched the causes of being a target of online fraud, some others examined the correlates of becoming a victim of cybercrime. This thesis posits that cybercrime victimisation should be examined holistically since each phase of victimisation process informs the other phases and victimisation may be a recurring experience should victims do not realise the factors that render them a victim of economic cybercrime. ICVM proposes a universal framework to be applied while examining any sort of cybercrime victimisation. In effect, it is a systematic approach taking conceptual factors into account while examining the occurrence of cybercrime victimisation holistically.

### 10.3.1 Being Targeted Online

This is the first phase of the victimisation process. The aim of examining this stage of victimisation is to understand individual and macro level conditions that render Internet users a target of an online attack. Visibility and Accessibility are two conceptual elements that should be operationalised while examining this stage of victimisation.

**Visibility and Accessibility**

Routine Activities Theory (RAT), the initial form of opportunity theory of victimisation, assumed that a suitable target has four attributes which are visibility, accessibility, value and inertia (Cohen and Felson, 1979). Later, the Opportunity Model divided suitable target concept into two parts. Visibility and accessibility proposed to be functions of exposure to potential offenders, whereas value and inertia conceived as a function of target attractiveness (Cohen et al., 1981). The results of this thesis indicated that target attractiveness of Internet users has no meaningful analogy in economic cybercrime context since perpetrators have little or no information about the economic well-being of most targets. Most of the respondents were being targeted because of stolen or shared information rather than the assets they owned. Wall (2010b) argues that most of the online fraud cases are micro frauds, which means perpetrators aim to steal a small amount of money from their targets. It appears that it is accessibility that renders Internet users as attractive targets. Internet users whose personal details such as email addresses or telephone numbers are a visible online run higher risk of being a target of an email phishing attempt since they provided a mean to be accessible. Otherwise, phishers would not be able to contact victims via emails or SMS messages. So, the first aspect of online visibility is the visibility of personal information, which renders Internet users accessible.

Another aspect of online visibility is the visibility of electronic devices utilised to access the Internet to perpetrators' tools. Interviews with participants suggested that Internet users who visited websites that may be considered to be hotspots of the Internet were more likely to experience malware infection. Malware is utilised to access or control electronic devices of Internet users.

In sum, Internet users' online activities that required sharing personal or financial information increase the chance of being a phishing attempt; deviant online activities increase the odds of being a target of a hacking attack. Internet users' decisions of sharing personal information and engaging with online deviancy are influenced by the perceived severity of consequences and perceived benefits of engaging with online deviancy.

Thus, the first assumption of the model is: the higher perceived benefits and the lower perceived severity and perceived vulnerability, the more visible Internet users or their electronic devices. The greater visibility of a device or personal information to perpetrators or their tools, the higher the risk of a security compromise. Thus, increased visibility and accessibility enhances the odds of being a victim of economic cybercrime.

### 10.3.2 Threat Assessment

LRAT posits that congruence of the motivated offender (an online threat in cyberspace) and suitable target in the absence of capable guardianship leads to victimisation (Cohen and Felson, 1979); however, it does not account for what happens when a suitable target faces a threat. Qualitative analysis of semi-structured interviews and police reports suggested that Internet users conduct a decision-making process and online perpetrators aim to hamper this process through socially engineered messages, either written or voice-operated. This phase of model utilises PMT to understand how Internet users evaluate socially engineered online attempts.

PMT posits that individuals conduct threat and coping appraisals when they face a threat (Rogers, 1975). Likewise, interviews suggest when Internet users face an online threat (a phishing email, ransomware or scareware), they initiate a cognitive process to assess the nature and extent of the threat. This cognitive process is influenced by the Internet users' perceived vulnerability and the perceived severity. Interviews suggested perceived

vulnerability and perceived severity is moderated by Internet self-efficacy. Users with high Internet skills were able to understand the real extent of the threat better when compared to those with low Internet skills. Context-specific factors like the existence of a distractor also impact this process. For instance, one of the participants was urged by his son to purchase an online game figure from an unknown website. She acknowledged that her son's behaviour impaired her evaluation of the extent of the threat.

A coping appraisal is conducted after understanding the nature and the extent of the threat faced. Self-efficacy emerged to be the most significant factor impacting the outcome. Internet users who are more knowledgeable about online threats and the ways to thwart these threats appear to evade online threats easily. Perceived rewards also seem to affect Internet users' decision-making process. Interviews suggested that although some Internet users were aware of the danger of malware infection when they experienced pop-up windows generated by free streaming websites, they still continued accessing these websites to watch films free of charge. After this coping appraisal, individuals make a decision based on their heuristic decision-making processes or systematic decision-making processes. Internet users either agree with a solution proposed by an email message or pop-up message or refuse to coerce with the proposed solution. Figure 10.1 illustrates the cognitive process when Internet users face an online threat.

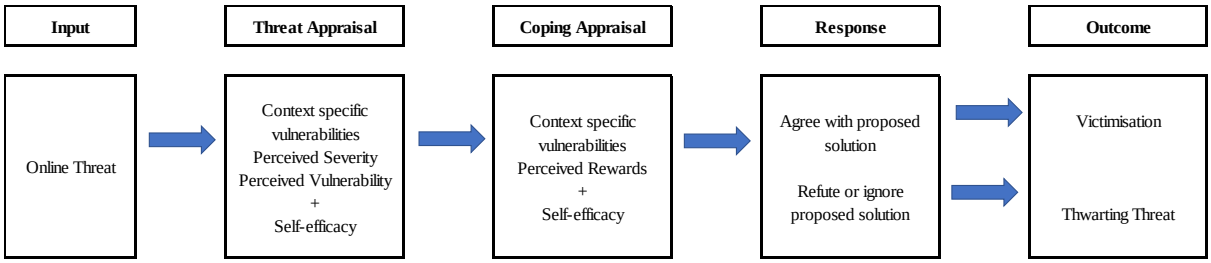



Figure *10.1: Decision-making Process*

The second assumption of the model is: Online perpetrators aim to coerce Internet users into following their proposed solutions to perceived online threats. Internet users either use heuristic or systematic decision-making systems to evaluate the extent of the threat and their responses to thwart the threat. This process of decision-making is influenced by cognitive factors (perceived severity, perceived vulnerability, perceived rewards and self-efficacy) and context-specific vulnerabilities.

### 10.3.3 Consequences of Victimisation

Despite a growing body of literature about fear of cybercrime and perceived risk of cybercrime victimisation, cybercrime victims' behavioural and emotional experiences in the aftermath of victimisation are largely understudied in cybercrime victimisation literature. Semi-structured interviews suggested that economic cybercrime victimisation may have adverse impacts on the psychological well-being of Internet users. A set of emotions ranging from shock to fear of crime are reported. However, understanding how these negative emotional responses impact Internet users' behavioural adaptations and security intentions may have implications for preventing repeat victimisation. Applying the approach-avoidance coping paradigm may enable researchers to understand the causes of repeat victimisation.

A coping perspective posits that individuals display some emotional and behavioural responses to negative life events like victimisation experiences. These responses may encapsulate approach and avoidance coping strategies (Lazarus and Folkman, 1984; Roth and Cohen, 1986). Whereas approach coping strategies entails implementing active measures to confront the negative consequences of victimisation, coping avoidance strategies cover passive actions like ignoring the threat or stopping accessing the Internet for online financial activities. The findings of this thesis suggest that a majority of repeat victims were hacking victims who abstained from applying a safeguarding measure. Interviews with of cybercrime suggested that

psychological factors (fear of economic cybercrime, perceived severity, perceived vulnerability, response efficacy, response cost and perceived rewards) shaped Internet users' online lifestyles and security measures applied. For instance, some participants did not make any changes in their online security measures as they perceived that no safeguarding measure might prevent victimisation. Regarding changes in online lifestyles, participants who perceived rewards of engaging with online deviant activities outweighs the risk of economic cybercrime victimisation did not make any changes in their online lifestyles.

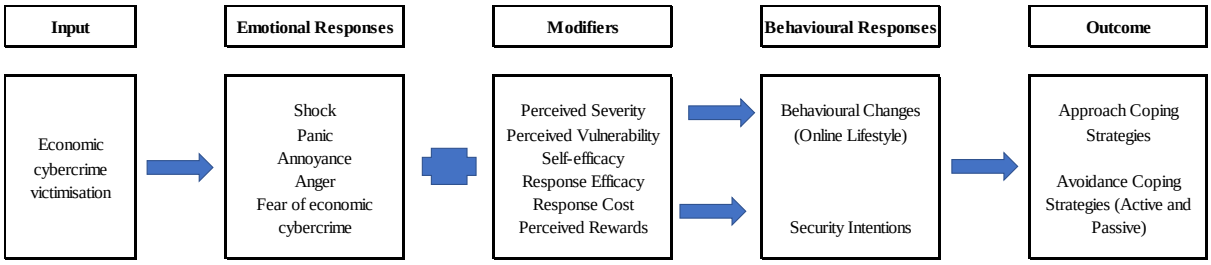



Figure 10.2: Decision-making Process

The third postulate of the ICVM is the cybercrime victimisation experiences causes emotional responses. These emotional responses which are modified by psychological factors (perceived severity, perceived vulnerability, self-efficacy, response efficacy, response cost and perceived rewards) may lead to behavioural adaptations (changes in online lifestyle) and/or security intentions. The influence of victimisation experiences may be shown as the application of approach coping strategies or avoidance coping strategies or both strategies at the same time.

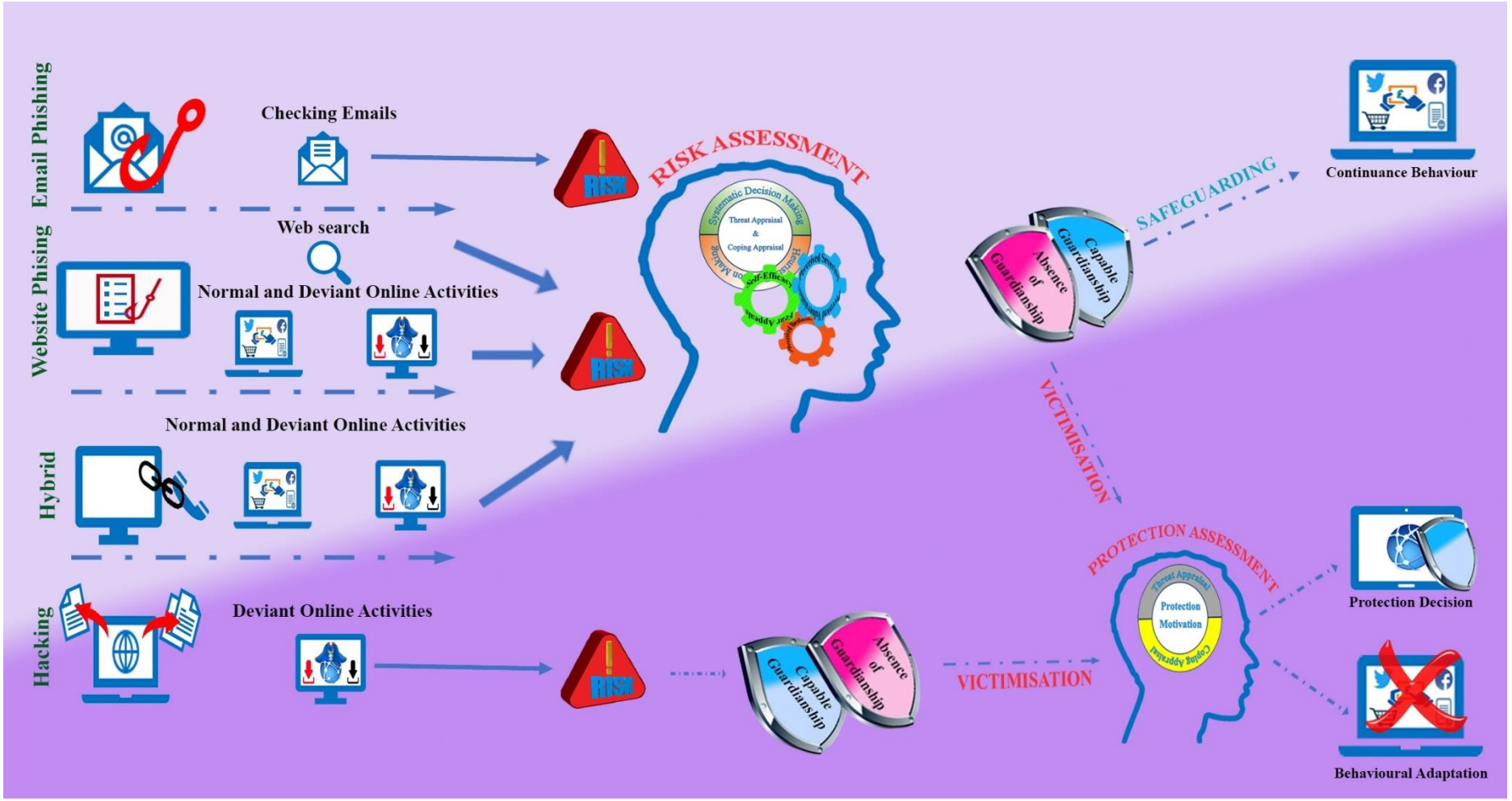



Figure 10.3: Integrated Cyber Victimisation Model

## 10.4 Significance of Research and Original Contributions to Cybercrime Victimisation Literature

This doctoral thesis aimed to contribute to the growing area of cybercrime victimisation literature by examining the economic cybercrime victimisation process to discern factors facilitating victimisation and understand impacts of economic cybercrime victimisation experiences on Internet users' behavioural adaptations and security intentions. A mixed-methods research paradigm was utilised to explore the factors increasing the risk of victimisation. This doctoral thesis is one of the first cybercrime victimisation studies utilising a mixed-methods approach to investigate victimisation in cyberspace in the UK. Each phase of economic cybercrime victimisation was examined through the application of the content analysis method, which enabled one of the first theoretically informed systematic analysis of economic cybercrime victimisation in the UK context. Besides the methodological innovative novelty of the research, this thesis offers some noteworthy insights into our understanding of the causes of economic cybercrime victimisation.

This thesis empirically demonstrated, for the first time, that besides Internet users' online activities or online lifestyles, some other factors which are not under Internet users' control may facilitate cybercrime victimisation. These factors are named as contextual vulnerabilities. Previous cybercrime studies that utilised Lifestyle Routine Activities Theory as a theoretical framework implicitly blamed victims of cybercrime for being a victim since these studies perceived Internet users' online lifestyles and demographic characteristics as the main source of victimisation. The Contextual vulnerabilities approach, however, suggest that macro vulnerabilities such as data breaches of large companies or technological vulnerabilities like mobile applications may also increase the risk of victimisation. Even implicitly, blaming

victims due to their online lifestyles or demographic attributes may hamper the combat against online perpetrators. Implications of this finding will be evaluated in the next section.

This thesis is one of the first empirical studies examining the causes of website phishing. The findings of this thesis suggested that website phishing is the most prevalent form of online attacks that lead to economic cybercrime victimisation. Not only bogus websites mimicking the real online merchants caused victimisation but also tech support websites also defrauded Internet users. The findings of this thesis also illustrated that online perpetrators utilise phishing websites to contact individuals' in the physical world through telephone contacts.

This thesis also contributes to an existing fear of crime and approach-avoidance coping knowledge by providing a new application area of research. The thesis has significantly enhanced our understanding of post-victimisation effects of economic cybercrime victimisation experiences on Internet users' psychological well-being as well as behavioural adaptations and security intentions.

The Integrated Cyber Victimisation Model (ICVM) is another novel and innovative contribution of this thesis. This model, which is the integration of Lifestyle Routine Activities Theory, Protection Motivation Theory and Approach-Avoidance Coping Paradigm, may serve as a base for future cybercrime victimisation studies. This is the first time that these approaches, which account for different phases of the victimisation process, are used together to explore cybercrime victimisation.

## 10.5 Implication of Research Findings for Policy and Policing Economic Cybercrime

As it was stated earlier, this thesis illustrated that macro and micro level factors other than individuals' online lifestyles might facilitate economic cybercrime victimisation. The findings of this thesis illustrated that Internet users' online lifestyles provide necessary conditions of victimisation. It is a congruence of contextual vulnerabilities that pose the real threat. Previous research results explicitly blamed victims for creating suitable conditions for the victimisation. However, this thesis argues that rather than putting the onus of victimisation on Internet users, efforts should be directed to the introduction of solutions to alleviate the influence of macro-level factors. These findings suggesting contextual vulnerabilities as the main drive behind economic cybercrime victimisation have several notable implications for practice.

The findings of this thesis suggest that data breaches of companies or online traders increased the risk of being a target of online attack. Semi-structured interviews indicated that stolen personal information of their customers was utilised to conduct phishing attempts or offline scams. Participants acknowledged that companies experiencing security compromise mostly assure customers that their financial information was not lost. However, the loss of personal information still poses a threat. Hence, bodies holding Internet users' personal information should provide security not only for financial information but also for personal information. Bogus mobile applications and malware containing genuine mobile applications emerged as major risk factors. Internet users download these from online stores like App Store or Google Play Store. These stores run the responsibility to check the security of applications uploaded to their stores. Governments should consider imposing some sanctions to these stores when they fail to provide security checks. Free Wi-Fi usage also emerged as a reason for being a target of online attacks and experiencing victimisation through theft of credentials. Providing

a publicly accessible secure Internet connection by Internet services providers free of charge may be taken into consideration. Although the application of this policy may require a significant budget, it might be less costly in the long term considering financial losses caused by insecure Internet connections.

Interviews with older participants suggested that the interface of websites and their complex designs pose particular difficulties for older citizens. Online merchants and banks should offer a more user-friendly and simplified version of their online services, which helps users with the procedures to be followed. Some functions of these websites may also be voice operated to eliminate the burden of using these websites. Low Internet self-efficacy among older participants provided another significant implication for governments, municipalities and non-governmental organisations. Interviews suggested accessing the Internet may be more important for the social and psychological well-being of older citizens due to mobility restrictions that prevent them from socialising when compared to younger generations. The findings of this thesis suggested that there is a definite need for education programmes for older citizens who are not very familiar with cyberspace. These education programmes may both entail providing technical skills to access the Internet but as importantly how to manage online threats.

Password fatigue, which is the result of memorising many login details for online accounts, was another significant issue that facilitated economic cybercrime victimisation through hacking. Participants acknowledged using the same password for different online accounts due to difficulties in remembering all passwords. Offering new login methods would be a remedy for password fatigue related to victimisation risks. A new application of Yahoo mail can be used as an example of these new methods. When Yahoo mail users want to log in their email accounts system send a confirmation code to users' mobile phones rather than

asking a password. This policy eliminates the risk of unauthorised access to email accounts. Similar adjustments may also be implemented by banks and online merchants.

The findings of this thesis suggesting engaging with deviant online activities like free streaming have also some significant policy implications. Participants who accessed the free streaming websites acknowledged football matches and movies as the primary reasons for using these online websites. For instance, participants who watched football matches through live streaming websites reported the football blackout[13] rule applied in the UK as the main reason for accessing these websites. Fans who do not have a chance to watch football games on TV or legal live streaming, access free live streaming websites that offer broadcasts of the Premier League matches shown in other countries. Respondents who watched movies via free online websites proposed that the high prices of watching movies through legal websites were prohibitive. Changes in broadcasting policies and marketing strategies may alleviate the need to access these websites. Birmingham and David (2011) argue that broadcasting companies should devise an official substitute of broadcasting football matches for affordable prices to decrease the popularity of free live streaming websites. In that vein, this thesis suggests that websites like YouTube or Netflix may be encouraged to offer special plans to decrease the access rates to illegal streaming websites.

A naïve question of an older participant saying, *"I don't understand why they are allowed to do it?"* seems to summarise the problem of governing the Internet. The issue is actually who should be responsible for governing or regulating the Internet? This thesis proposed that previous cybercrime studies explicitly put the responsibility of victimisation on victims' shoulders, likewise Wall (2013d, p. 45) argues that "the corporate sector has unfortunately determined that identity is to be the basis for security systems and has then shifted

[13] Football blackout is a football broadcasting regulation that bans the broadcasting football matches on Saturday between 2:45pm and 5.15 pm in the UK.

the burden of responsibility from themselves (to provide secure systems) to the individual to protect their own identity." The private sectors' evasion from taking responsibility for providing a secure environment creates public expectations from public police to fill this gap (Cross and Blackshaw, 2014). Interviews with police officers working in the cybercrime department of a Northeast city in the UK indicated the demand for cybercrime cases exceed the resources of police forces. Wall (2010c, p. 17) argues that rather one single unit, a group of interest bodies, which he names as a "policing assemblage", should be responsible for regulating the Internet. He outlines this assemblage as Internet users and user groups, virtual environment managers, Internet service providers, corporate security organisations, non-governmental or non-police organisations, governmental non-police organisations and public police organisations[14]. As can be seen, there are many interest groups that need to be working harmoniously to provide a secure environment for Internet users. The role of governmental non-police organisations or public police may be coordinating efforts of policing assemblage to govern cyberspace (Wall, 2007). However, despite the growing adverse impacts of cybercrime it is hard to say that interest groups work harmoniously to control hotspots of the Internet (Levi et al., 2017).

Levi et al. (2015) propose a Four Ps Model, pursue, prevent, protect and prepare, to combat economic cybercrime. Pursue strategy denotes prosecuting online perpetrators. This strategy is mainly falling into the realm of law enforcement agencies. Prevent strategy is about refraining individuals to get involved with criminal acts. This strategy involves coordinated efforts of governments and non-governmental organisations to introduce public awareness campaigns to illustrate that online criminality is no different from physical world criminality. Online perpetrators generally perceive economic cybercrime as a victimless crime since

[14] Please see Wall (2010b) for detailed account of interest groups that may be responsible for regulating cyberspace.

individuals get a refund for their financial loses (Goucher, 2010). The results of this thesis suggested that besides financial losses, economic cybercrime victimisation had adverse impacts on Internet users' psychological well-being and online lifestyles. All adverse effects of victimisation should be explained public to reduce online criminal intention.

Protect strategy puts the responsibility of regulating the Internet on governments, the private sector and non-governmental agencies (Levi et al., 2015). Wall (2008a) proposes a digital realism approach, which assumes that technology which provides an opportunity for online perpetrators may also be used to combat cyber criminality and, to regulate cyberspace. This is a multi-disciplinary approach that blends both law and technology to control cyberspace. Following this line of logic, several initiatives may be implemented to provide a safer online environment.

Firstly, virtual hotspots of the Internet that are utilised to distribute malware and bogus websites tricking Internet users into yielding their information or buying fake products should be controlled. This control may be attained through search engines. Search engines codes may be configured to hide websites that are harmful. Moreover, the design of the Internet may be reconfigured. Levi et al. (2015) argue that encrypted online banking should be a compulsory requirement for online banking. In the same vein, Mark Johnson[15], one of the expert interviewees, proposed that the current Internet structure should be replaced with an encrypted version of it to combat economic cybercrime effectively since the present design of the cyberspace was constructed to provide communication between and this unsafe structure creates numerous opportunities for online criminality. He further suggests that the new version of the Internet should be end to end encryption with secure authentication of trusted domains. Domain registrars should be required to validate the identity of domain owners and Internet

[15] Mark Johnson is an Associate of the City of London Police Economic Crime Academy. He delivers cybercrime training and consultancy to the UK Police, the United Nations, Europol and the Home Office.

users should be able to limit access to unauthenticated domains by default. This would represent an Internet Green Zone in which most users would operate. The Red Zone would be a high-risk area that corporate networks could block and which private users could only access after accepting liability for so doing via a browser prompt.

Lastly, interviews suggested that security breaches of online merchants lead to victimisation. Since security maintenance can be costly, some online traders are unwilling to update their security systems. In order to prevent security breaches of online merchants, getting a security certificate, which maintains that the online merchant complies with security requirements and their security systems are up to date, should be compulsory to be an online merchant. Any online merchant failing to comply with these regulations should be responsible for financial loss caused.

Prepare strategy is related to the post-victimisation phase of the economic cybercrime. As it was stated earlier, economic cybercrime victimisation may have psychological and behavioural adverse impacts on Internet users. Governments, non-government organisations and local governments should offer rehabilitation programs to victims of economic cybercrime to alleviate the adverse impacts of victimisation on the quality of victims' lives.

## 10.6 Limitations of the Thesis and Recommendations for Future Research

This thesis examined the factors influencing email phishing victims' decision-making processes. Past research illustrated those personality traits, which are neuroticism, extroversion, openness, agreeableness and conscientiousness, increase Internet users' susceptibility to email phishing attempts. This thesis did not examine the impacts of personality traits on the risk of economic cybercrime victimisation through phishing. This was mainly due to the lack of a survey measuring personality traits of participants. Future research including a self-report survey measuring the personality traits of respondents may be able to measure the

effect of personality traits on the risk of economic cybercrime victimisation through email and website phishing.

The findings of this thesis suggested that technological vulnerabilities such as the type of electronic devices utilised to access the Internet, Wi-Fi connections and mobile applications increased the risk of economic cybercrime victimisation. However, it needed to examine more closely how mobile applications exploit vulnerabilities. Recent news indicates that new genres of mobile applications are introduced to steal personal information (Koetsier, 2018; Watson, 2018). These applications aim to exploit social media users' curiosity about the individuals who visited their online profiles or their desire to get more likes for their posts. These applications grant access to social networking accounts like Facebook, Twitter and Instagram to work, which means that Internet users willingly yield the control of their account to fraudsters. Examination of the impacts of these technological vulnerabilities on the risk of identity theft and economic cybercrime victimisation in a separate study may enable us to understand better the extent of the threat they pose and modus operandi of perpetrators.

This thesis illustrated that some older Internet users apply passive avoidance strategies like stopping using the Internet. The scope of this thesis was limited to examine how victimisation experiences impacted older Internet users' online lifestyles and security intentions. The findings of this thesis indicated that abstaining from using the Internet contributed to their loneliness. Future work may focus on long-term adverse impacts of cybercrime victimisation on older people's lives.

The contextual vulnerabilities approach, which aims to build the gap between macro and micro level factors, is another area that needs to be examined in future studies. Further research is needed to investigate how macro vulnerabilities (data breaches of companies

holding personal information of Internet users) affect the risk of victimisation in the cyberspace.

The Integrated Cyber Victimisation Model is proposed to account for economic cybercrime victimisation. This model offers a systematic theoretically informed methodology to investigate victimisation events. Further research is needed to test the applicability of this model to other forms of cybercrime victimisation.

**Appendices**

**Appendix 1: Ethical Approval Letter from Durham University**

**TO: Akdemir, Naci**

**FROM: Jackson, Fiona, E.**

**DATE: 03/11/2016**

Dear Naci;

I am pleased to advise that your Ethics Application has been approved by the School Ethics Committee and you are now permitted to begin data collection for your research.

I have attached a signed copy of your application form which you should ensure you have available either in hard copy or electronically should you be asked to show evidence of Ethical Approval.

Please let me know if you need any further details.

Regards

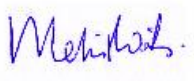
**PART F: OUTCOME OF THE APPLICATION**

| | |
|---|---|
| Reject<br><br>The application is incomplete and/or cannot be assessed in its current format. Please complete the application fully. | |
| Revise and Resubmit<br><br>The application cannot be approved in its current format. Please revise the application as per the comments below. Please complete the application fully. | |
| Approved, with Set Date for Review<br><br>The application is approved and you may begin data collection.<br><br>A date for further review of the project as it develops has been set to take place on: _____<br><br>The anticipated nominated reviewer will be:_____ | |
| Approved<br><br>The application is approved and you may begin data collection. | **X** |

**Comments:**

No major ethical issues raised by the study and suitable consideration has been given to those minor issues which are.

I approve this Ethics and Risk Assessment application and I have no conflict of interest to declare.

First Reviewer's Signature: 

First Reviewer's Name: Martin Roderick

First Reviewer's Role: Director, Postgraduate Research

Date: 01/11/2016

If applicable:

I approve this Ethics and Risk Assessment application and I have no conflict of interest to declare.

Second Reviewer's Signature: 

Second Reviewer's Name: Will Craige

Second Reviewer's Role: Ethics Committee member

Date: 29/10/2016

**Appendix 2: Participant Information Sheets**

Durham University
School of Applied Social Sciences

## PARTICIPANT INFORMATION SHEET – VICTIMS

**Project Title:** Understanding the Individual Level and Macro Level Causes of Economic Cybercrime Victimisation in the UK: A Contextual Vulnerabilities Approach to Examine Cybercrime Victimisation

Thank you for your interest in participating in the above project. I would like to invite you to take part in a research study. Please take time to read the following information carefully as it explains why the research is being done and what it would involve for you. Please feel free to ask questions if anything you read is not clear, or you would like more information.

The project is being undertaken as part of a postgraduate doctorate study, which is being undertaken in the School of Applied Social Sciences at Durham University. The main aim of the project is to understand the nature of economic cybercrime and discern its social, financial and psychological effects on individuals through the lenses of victims.

You are being asked to participate in the interview since you have experienced at least one form of economic cybercrime. You are being asked to participate in a short interview where you will be asked about your opinions and experiences as a victim of economic cybercrime.

I cannot promise the study will help you personally, but the information I get from the study will help to increase the understanding of the nature of economic cybercrime. The results

of the study may be used by policy makers and police forces to prevent or decrease further victimisation. While it is unlikely that this interview will carry any risk for you, revisiting your experience of this crime may be distressing. You are welcome - and encouraged - not to answer questions if you feel they will be distressing, and you may terminate the interview at any time.

The interview will be recorded and later transcribed for analysis. Anything you say during the interview will be anonymised during transcription, and the recordings will be deleted immediately after the transcription. The transcriptions will be analysed to perceive the nature of economic cybercrime victimisation and to find out social, financial and psychological impacts of economic cybercrime on individuals.

The transcripts will only be saved to a secure storage area of my university account. Only my two supervisors will be able to access these transcripts.

You are free to refuse to answer any question during the interview, and you may withdraw your consent to participate at any time before submission of the thesis to Durham University. If you choose to do this, the information collected during the interview will be destroyed and whatever you have told me during the interview will be omitted from the study.

If you need information about the study at any point, please contact me as follows:

Telephone: 07405 958054

Email: naci.akdemir@durham.ac.uk

Durham University
School of Applied Social Sciences

**PARTICIPANT INFORMATION SHEET – CONTROL GROUP**

**Project Title:** Understanding the Individual Level and Macro Level Causes of Economic Cybercrime Victimisation in the UK: A Contextual Vulnerabilities Approach to Examine Cybercrime Victimisation

Thank you for your interest in participating in the above project. I would like to invite you to take part in a research study. Please take time to read the following information carefully as it explains why the research is being done and what it would involve for you. Please feel free to ask questions if anything you read is not clear, or you would like more information.

The project is being undertaken as part of a postgraduate doctorate study, which is being undertaken in the School of Applied Social Sciences at Durham University. The main aim of the project is to understand the nature of economic cybercrime and discern its social, financial and psychological effects on individuals through the lenses of victims.

You are being asked to participate in the interview as a control group respondent since you have avoided being a victim of economic cybercrime. You are being asked to participate in a short interview where you will be asked about your opinions and experiences

I cannot promise the study will help you personally, but the information I get from the study will help to increase the understanding of the nature of economic cybercrime. The results of the study may be used by policy makers and police forces to prevent or decrease further victimisation. While it is unlikely that this interview will carry any risk for you, revisiting your

experience may be distressing. You are welcome - and encouraged - not to answer questions if you feel they will be distressing, and you may terminate the interview at any time.

The interview will be recorded and later transcribed for analysis. Anything you say during the interview will be anonymised during transcriptio, and the recordings will be deleted immediately after the transcription. The transcriptions will be analysed to perceive the nature of economic cybercrime victimisation and to find out social, financial and psychological impacts of economic cybercrime on individuals.

The transcripts will only be saved to a secure storage area of my university account. Only my two supervisors will be able to access these transcripts.

You are free to refuse to answer any question during the interview, and you may withdraw your consent to participate at any time before submission of the thesis to Durham University. If you choose to do this, the information collected during the interview will be destroyed and whatever you have told me during the interview will be omitted from the study.

If you need information about the study at any point, please contact me as follows:

Telephone: 07405 958054

Email: naci.akdemir@durham.ac.uk

Durham University
School of Applied Social Sciences

**PARTICIPANT INFORMATION SHEET – POLICE OFFICERS**

**Project Title:** Understanding the Individual Level and Macro Level Causes of Economic Cybercrime Victimisation in the UK: A Contextual Vulnerabilities Approach to Examine Cybercrime Victimisation

Thank you for your interest in participating in the above project. I would like to invite you to take part in a research study. Please take time to read the following information carefully as it explains why the research is being done and what it would involve for you. Please feel free to ask questions if anything you read is not clear, or you would like more information.

The project is being undertaken as part of a postgraduate doctorate study, which is being undertaken in the School of Applied Social Sciences at Durham University. The main aim of the project is to discern the role of public police in the police assemblage and to find out challenges police officers face while prosecuting cases.

You are being asked to participate in the interview since you have particular expertise and experience in the policing of cybercrime. You are being asked to participate in a short interview where you will be asked about your opinions and experiences as a police officer dealing with economic cybercrimes.

I cannot promise the study will help you personall, but the information I get from the study will help to increase our understanding of policing economic cybercrime. The results of the study may be used by policy makers and police forces to reconsider the current state of policing economic cybercrime. These interviews should not carry any risk for you. However,

if you feel that answering a question may place you or your work in jeopardy, then you are encouraged not to answer. Further, you are welcome to terminate the interview at any point.

The interview will be recorded and later transcribed for analysis. Anything you say during the interview will be anonymised during transcription, and the recordings will be deleted immediately after the transcription. The transcriptions will be analysed to perceive the nature of economic cybercrime victimisation and to find out social, financial and psychological impacts of economic cybercrime on individuals.

The transcripts will only be saved to a secured storage area of my university account. Only my two supervisors will be able to access these transcripts.

You are free to refuse to answer any question during the interview and you may withdraw your consent to participate at any time before submission of the thesis to Durham University. If you choose to do this, the information collected during the interview will be destroyed and whatever you have told me during the interview will be omitted from the study.

If you need information about the study at any point, please contact me as follows:

Telephone: 07405 958054

Email: naci.akdemir@durham.ac.uk

**Appendix 3: Request Letter**


**Name of Company**
**Address**

Naci Akdemir
PhD Candidate
School of Applied Social Sciences
Durham University
32 Old Elvet
Durham DH1 3HN

To whom it may concern;

I would like to let you know about a research study that may be of interest to your customers and ask you to consider displaying fliers of the study in your facilities.

Economic cybercrime is a growing issue, and millions of people are victimized every year. It is estimated that the total cost of economic cybercrime was approximately £217 million in 2014. Despite its huge impact of economic cybercrim, there is a lack of study on this area, and more important voices of victims of economic cybercrime are unheard. This study aims to discern the causes of economic cybercrime on the individual level through lenses of a victim of economic cybercrime.

Thank you for your time and consideration.

Sincerely,

**Enclosed:**
Flier of the study
**Contact Details:**
Email: naci.akdemir@durham.ac.uk
Phone:07405 958054

**Appendix 4: Consent Form**

Durham University
School of Applied Social Sciences

**CONSENT FORM**

**Project Title:** Understanding the Individual Level and Macro Level Causes of Economic Cybercrime Victimisation in the UK: A Contextual Vulnerabilities Approach to Examine Cybercrime Victimisation

☐ I confirm that I have read and understood the Participant Information document for the above study and have been given the opportunity to ask questions.

☐ I understand that my participation is entirely voluntary and that I am free to withdraw at any time without giving a reason.

☐ I understand that I am free to refuse to answer any question during the interview.

☐ I agree to the interview being recorded and later transcribed.

☐ I agree to take part in the above study.

**Participant's Signature:** ……

**Participant's Name:** ……

**Date:** ……

## Appendix 5: Interview Guides

### Interview Guide for Victims of Economic Cybercrime

#### Introduction

Hello, as it is stated in the participant information sheet, you are going to be asked some questions about your Internet usage and economic cybercrime victimisation experiences. You are free to not to answer any question or to stop the interview whenever you want.

#### Demographic information

I would like to ask some questions to capture your demographic information. You are free to not to answer any question.

- Could you please tell me about yourself, especially your gender, age, annual household income and education level?

#### Internet usage and online lifestyle

I am going to ask you some questions about your Internet usage. You are free to not to answer any questions.

- Do you consider yourself a confident or skilled Internet user? Why?
- How often do you access the Internet?
- The Internet can be used for many different purposes such as online shopping, social networking via Facebook or chatrooms and leisure. Why do you access the Internet mostly?
    - Possible Prompts
        - Can you please list me your online activities from the most frequent to less frequent one?
- Do you use the Internet for online shopping?
    - Possible Prompts
        - Do you have any preferences for online shopping websites?
        - Do you shop from random websites or reputable merchants? Why

        - Have you experienced something negative/bad while shopping online?
- Do you use the Internet for online banking?
    - Possible Prompts
        - Do you have any bad experience related to online banking usage?
        - Are you worried when you provide your personal details to the online banking website?
- Have you ever used online government services?
    - Possible Prompts
        - Do you have any bad experience related to online government website usage?
        - Are worried when you provide your personal details to an online website?
- Have you ever posted an advertisement on the Internet to sell something?
    - Possible Prompts
        - What kind of information did you provide while posting the add?
        - Have you experienced anything unusual such contact from a stranger or online communication?
        - Did you experience something negative after posting advertisement online?
- Did you post any personal information online over the last year?
    - Possible Prompts
        - What kind of information did you share?
        - Do you think that posting personal information on social networking websites may have some adverse consequences?
        - Are you worried about misuse of your posted personal information?

Now I would like to ask some questions about your electronic device preferences to access the Internet? Desktop at home, laptop at home or away from home, mobile phone and tablets are the most popular devices to access the Internet.

- Which electronic device did you mostly use to access the Internet before your negative experience?
    - Possible Prompts
        - Why do you prefer that device (mentioned device) to access the Internet?

        - Does the location that you need to access the Internet have an effect on your choice, for instance, using a laptop while at home but using a mobile phone while at work?
        - Do you use different devices to access the Internet for different purposes such as only using the desktop to shop online?
- Do you use mobile applications?
    - Possible Prompts
        - What kind of mobile applications do you use mostly?
        - Do you pay attention to the type of application and the type of information that application asks to access in your mobile phone?
        - Did you experience anything negative while using mobile applications?
- Do you use free Wi-Fi connections to access the Internet?
    - Possible Prompts
        - Have you ever used a free Wi-Fi offered in airport or café to access the Internet before the negative incident you experienced?
        - What would be your reaction to information asked when you want to access free Wi-Fi in public places? For instance, do you think about them carefully or just answer them to access the Internet quickly?
        - Are you worried about providing your email address or any other personal information to be eligible for free Internet?

Now I would like to ask some questions about your security measures taken to prevent victimisation. Firstly, I would like to explain two terms. Digital guardianship includes actions such as using anti-virus software or scanning devices regularly with these devices. Personal guardianship includes actions such as being careful about popularity websites while shopping or checking security signs in web devices or using a separate card for online shopping.

- What kind of digital and personal security measures do you use?
    - Possible Prompts:
        - Do you use any digital security in your mobile devices?
        - How do you secure your personal and financial accounts?
        - Can you please tell me about your password management? For instance, do you use the same password, or do you use complex passwords?

**Occurrence and the process of the victimisation**

I would like to clarify the term "economic cybercrime". Economic cybercrime refers to card-not-present or remote purchase fraud and online banking fraud. Card-not-present fraud occurs when your payment card (i.e. credit card or debit card) is used without your knowledge or consent. Online banking fraud occurs when your online banking account is used to transfer money or buy goods without your knowledge or consent.

- Could you please tell me about your experiences of economic cybercrime in as much detail as possible?
    - Possible Prompts
        - Do you think any reason for being a target of an online attack?
        - How do you think your financial details be compromised by perpetrators?
        - Do you know anybody who responded to fraudulent online communication?
        - What do you think about responding to fraudulent communications such as bogus official-looking emails? Have you any negative experiences with such emails?
        - Could you please describe me your social, psychological and financial condition at the time of victimisation?

**Effects of victimisation**

- Although some people experience economic cybercrime, they do not define themselves as a victim. How do you feel about that?
    - Possible Prompts
        - Did your victimisation experience have any effect on you apart from losing money?
        - What were your primary feelings when you learned about the incident?
        - Does your negative experience hadlong-lasting psychological effects like fear of crime?
        - Do you blame yourself for being a victim?
        - What do you do differently to protect from being a victim again?

- Do you think that your experience had impacted your online behaviours or online security measures you applied?

**Perceptions**

- What are your thoughts about the general state of economic cybercrime?
  - Possible prompts
    - Do you consider economic cybercrime as a significant issue?
    - Do you think that the government or police take enough precautions to prevent economic cybercrime?
    - Are you worried about the victim of economic cybercrime again?

**Online Deviance**

I am now going to ask you some more questions about online activities that you engaged before experiencing negative online experience. These questions will be about online activities that some people in our society may label them as illicit or deviant. You are free to not to answer any of these questions or we may stop when you feel uncomfortable.

- Have you ever engaged with one of these online activities? (Live streaming, adult content, free downloading, peer-to-peer sharing)
  - Possible prompts
    - Have you experienced anything unusual while accessing these websites or after accessing these websites? For instance, your computer may start slowing down, or you may have received some messages on your computer screen after accessing these websites?
      - Why did you access these websites?

## Interview Guide for Control Group Participants

### Introduction

Hello, as it is stated in the participant information sheet, you are going to be asked some questions about your Internet usage, online security measures and perceptions about economic cybercrime in the UK. You are free to not to answer any question or to stop the interview whenever you want.

### Demographic information

I would like to ask some questions to capture your demographic information. You are free to not to answer any question.

- Could you please tell me about yourself, especially your gender, age, annual household income and education level?

### Internet usage and online lifestyle

I am going to ask you some questions about your Internet usage. You are free to not to answer any questions.

- Do you consider yourself a confident or skilled Internet user? Why?
- How often do you access the Internet?
- The Internet can be used for many different purposes such as online shopping, social networking via Facebook or chatrooms and leisure. Why do you access the Internet mostly?
    - Possible Prompts
        - Can you please list me your online activities from the most frequent to less frequent one?
- Do you use the Internet for online shopping?
    - Possible Prompts
        - Do you have any preferences for online shopping websites?
        - Do you shop from random websites or reputable merchants? Why
        - Have you experienced something negative/bad while shopping online?
- Do you use the Internet for online banking?
    - Possible Prompts

        - Do you have any bad experience related to online banking usage?
        - Are you worried when you provide your personal details to the online banking website?
- Have you ever used online government services?
    - Possible Prompts
        - Do you have any bad experience related to online government website usage?
        - Are worried when you provide your personal details to an online website?
- Have you ever posted an advertisement on the Internet to sell something?
    - Possible Prompts
        - What kind of information did you provide while posting the add?
        - Have you experienced anything unusual such contact from a stranger or online communication?
        - Did you experience something negative after posting advertisement online?
- Did you post any personal information online over the last year?
    - Possible Prompts
        - What kind of information did you share?
        - Do you think that posting personal information on social networking websites may have some adverse consequences?
        - Are you worried about misuse of your posted personal information?

Now I would like to ask some questions about your electronic device preferences to access the Internet? Desktop at home, laptop at home or away from home, mobile phone and tablets are the most popular devices to access the Internet.

- Which electronic device did you mostly use to access the Internet before your negative experience?
    - Possible Prompts
        - Why do you prefer that device (mentioned device) to access the Internet?
        - Does the location that you need to access the Internet have an effect on your choice, for instance, using a laptop while at home but using a mobile phone while at work?

        - Do you use different devices to access the Internet for different purposes such as only using the desktop to shop online?
- Do you use mobile applications?
    - Possible Prompts
        - What kind of mobile applications do you use mostly?
        - Do you pay attention to the type of application and the type of information that application asks to access in your mobile phone?
        - Did you experience anything negative while using mobile applications?
- Do you use free Wi-Fi connections to access the Internet?
    - Possible Prompts
        - Have you ever used a free Wi-Fi offered in airport or café to access the Internet before the negative incident you experienced?
        - What would be your reaction to information asked when you want to access free Wi-Fi in public places? For instance, do you think about them carefully or just answer them to access the Internet quickly?
        - Are you worried about providing your email address or any other personal information to be eligible for free Internet?

Now I would like to ask some questions about your security measures taken to prevent victimisation. Firstly, I would like to explain two terms. Digital guardianship includes actions such as using anti-virus software or scanning devices regularly with these devices. Personal guardianship includes actions such as being careful about popularity websites while shopping or checking security signs in web devices or using a separate card for online shopping.

- What kind of digital and personal security measures do you use?
    - Possible Prompts:
        - Do you use any digital security in your mobile devices?
        - How do you secure your personal and financial accounts?
        - Can you please tell me about your password management? For instance, do you use the same password, or do you use complex passwords?

**Perceptions**

- What are your thoughts about the general state of economic cybercrime?
    - Possible prompts

- Do you consider economic cybercrime as a significant issue?
- Do you think that the government or police take enough precautions to prevent economic cybercrime?
- Are you worried about the victim of economic cybercrime?
- Does the news related economic cybercrime cause any worries about being a victim of economic cybercrime?

**Online Deviance**

I am now going to ask you some more questions about online activities that you engaged before experiencing negative online experience. These questions will be about online activities that some people in our society may label them as illicit or deviant. You are free to not to answer any of these questions or we may stop when you feel uncomfortable.

- Have you ever engaged with one of these online activities? (Live streaming, adult content, free downloading, peer-to-peer sharing)
    - Possible prompts
        - Have you experienced anything unusual while accessing these websites or after accessing these websites? For instance, your computer may start slowing down, or you may have received some messages on your computer screen after accessing these websites?
        - Why did you access these websites?

**Appendix 6 : Poster and Flier**

## Appendix 7: Coding Outcome Variables

### Obtaining the Outcome Variables

Crime Survey England and Wales 2014/2015 did not measure the extent of economic cybercrime victimisation with one single question. Interviewees were asked questions about their experiences pertaining to online banking fraud, loss of money through virus infection, online identity fraud and card-not-present fraud at separate sections. In order to obtain economic cybercrime victimisation variable, variables representing different aspects of economic cybercrime were merged. Since different facets of economic cybercrime were measured separately, a different number of respondents answered questions, which means missing values of each variable were different. This variation in missing values made utilisation of in-built merge command impossible. Hence, new codes were written to merge each variable.

### Online Banking Fraud (onln_bnk_frd):

Online Banking Fraud is obtained through a combination of three variables, qbnchk, qfrhwc and qfrhwe. *Qbnchk* refers to the loss of money from a bank or building account while using the Internet, variable *qfrhwc* denotes loss of money due to unauthorised access to online banking information (hacking), and variable *qfrhwe* refers to the loss of money from a bank account due to opening an email link opened into the fake website (phishing). The command written to obtain online banking fraud is as follows:

```
DO IF
(recode_qfrhwc =5  AND recode_qfrhwe=5 AND recode_qbnchk =0) OR
(recode_qfrhwc =5  AND recode_qfrhwe=0 AND recode_qbnchk =5) OR
(recode_qfrhwc =5  AND recode_qfrhwe=0 AND recode_qbnchk =0) OR
(recode_qfrhwc =0  AND recode_qfrhwe=5 AND recode_qbnchk =5) OR
(recode_qfrhwc =0  AND recode_qfrhwe=5 AND recode_qbnchk =0) OR
(recode_qfrhwc =0  AND recode_qfrhwe=0 AND recode_qbnchk =5) OR
```

(recode_qfrhwc =0  AND recode_qfrhwe=0 AND recode_qbnchk =0).
**COMPUTE** onln_bnk_frd =0.
**ELSE IF**
(recode_qfrhwc =5  AND recode_qfrhwe=5 AND recode_qbnchk =5).
**COMPUTE** onln_bnk_frd =5.
**ELSE.**
**COMPUTE** onln_bnk_frd=1.
**END IF.**
**EXECUTE.**

### Loss of money through virus infection (lossevirimp):

This variable was obtained through a combination of two variables, evirimpa and evirimpb. Variable ***evirimb*** refers to the refunded loss of money through virus infection, ***evirimpa*** denotes non-refunded loss of money through virus infection. The command written to obtain online banking fraud is as follows:

**DO IF** (EVIRIMPA =0 AND EVIRIMPB =0).
**COMPUTE** LOSSEVRIMP =0.
**ELSE**.
**COMPUTE** LOSSEVRIMP = 1.
**END IF**.
**EXECUTE**.

### Online Identity Fraud (lossedatimp):

This variable was obtained through a combination of two variables, (edatimpa and edatimpb), which measured whether respondents lost money due to unauthorised access to personal information. Whereas variable ***edatimpa*** refers to the non-refunded loss of money through personal data loss, variable ***edatimpb*** refers to the refunded loss of money through personal data loss.

DO IF (EDATIMPA =0 AND EDATIMPB =0).
COMPUTE LOSSEDATIMP =0.
ELSE IF

```
(EDATIMPA =0 AND EDATIMPB =1) OR
(EDATIMPA =1 AND EDATIMPB =0) OR
(EDATIMPA =1 AND EDATIMPB =1).
COMPUTE LOSSEDATIMP = 1.
END IF.
EXECUTE.
```

**Card-not-present Fraud (cnp_fraud):**

CSEW 2014/2015 did not measure card-not-present fraud directly; however, this variable can be obtained through subtracting cases that represent financial loss due to real-world causes from credit card fraud cases. Firstly, variables measuring the loss of money due to real-world causes, namely **qrecuse, qidhwa, qidhwb, qidhwd, qidhwf, qidhwg** and **qidhwh,** were combined. In that way, variable **qcrdlost** was obtained.

**Qurecuse:** Loss of money following unauthorised access to the use of personal data.

**Qidwha:** Loss of money through theft of credit card or bank card.

**Qidhwb:** Loss of money through theft of personal documents (e.g. cheque book, bank statements, pass book)

**Qidhwd:** Loss of money through card details being stolen/cloned when made a payment (e.g. at a restaurant or petrol station).

**Qidhwf:** Loss of money through a phone call that received asking for personal information.

**Qidhwg:** Loss of money through someone visiting address and asking for information.

**Qidhwh**: Loss of money through insider corruption (e.g. corrupt employee at a bank).

After that, cases of **qcrdlost** were subtracted from the credit card fraud variable **(qcrduse)** to obtain card-not-present fraud cases (cnp_fraud). Variable qcrduse denotes to cases where "banking cards were used without any permission or prior knowledge to take money from a bank or building society accounts or to charge money to bank, debit, credit or store cards." (Office for National Statistics, 2016b).

```
DO IF
(QIDHWA =0 AND QIDHWB =0 AND QIDHWF=0 AND QIDHWG=0 AND QIDHWH=0).
COMPUTE QIDHW =0.
ELSE.
COMPUTE QIDHW = 1.
END IF.
EXECUTE.

DO IF
(recode_qidhw=5 AND recode_qrecuse =0) OR
(recode_qidhw=0 AND recode_qrecuse =5) OR
(recode_qidhw=0 AND recode_qrecuse =0).
COMPUTE qcrdlost=0.
ELSE IF
(recode_qidhw=5 AND recode_qrecuse =5).
COMPUTE qcrdlost=5.
ELSE.
COMPUTE qcrdlost=1.
END IF.
EXECUTE.

DO IF
(QCRDLOST=5 AND QCRDUSE_NEW2=5) OR
(QCRDLOST=1 AND QCRDUSE_NEW2=0) OR
(QCRDLOST=1 AND QCRDUSE_NEW2=1) OR
(QCRDLOST=1 AND QCRDUSE_NEW2=5) OR
(QCRDLOST=0 AND QCRDUSE_NEW2=5).
COMPUTE CARD_NOT_PRESENT_FRAUD =5.
ELSE IF
(QCRDLOST=0 AND QCRDUSE_NEW2=0) OR
(QCRDLOST=5 AND QCRDUSE_NEW2=0).
COMPUTE CARD_NOT_PRESENT_FRAUD =0.
ELSE.
COMPUTE CARD_NOT_PRESENT_FRAUD=1.
```

**END IF**.
**EXECUTE**.

**Economic Cybercrime Victimisation (econ_cyber):**

This variable was obtained through a combination of five forms of economic cybercrime, namely online banking fraud **(onln_bnk_frd)**, loss of money through virus infection **(lossevirimp)**, loss of money through phishing (responding to communication) **(eexpin2b)**, online identity fraud and card-not-present fraud.

Firstly, ***onlineloss*** variable was obtained through a combination of variables lossedatimp, losselosimp and lossevirimp.

**DO IF**
(recode_lossedatimp =5 AND recode_losselosimp=5 AND recode_lossevirimp =0) OR
(recode_lossedatimp =5 AND recode_losselosimp=0 AND recode_lossevirimp =5) OR
(recode_lossedatimp =5 AND recode_losselosimp=0 AND recode_lossevirimp =0) OR
(recode_lossedatimp =0 AND recode_losselosimp=5 AND recode_lossevirimp =5) OR
(recode_lossedatimp =0 AND recode_losselosimp=5 AND recode_lossevirimp =0) OR
(recode_lossedatimp =0 AND recode_losselosimp=0 AND recode_lossevirimp =5) OR
(recode_lossedatimp =0 AND recode_losselosimp=0 AND recode_lossevirimp =0).
**COMPUTE** onlineloss1=0.
**ELSE IF**
(recode_lossedatimp =5 AND recode_losselosimp=5 AND recode_lossevirimp =5).
**COMPUTE** onlineloss1=5.
**ELSE**.
**COMPUTE** onlineloss1=1.
**END IF**.
**EXECUTE**.

After obtaining onlineloss variable, other two variables, online banking fraud and loss of money due to responding online communication, were merged with that variable to obtain **losswhileint.**

**DO IF**
(onln_bnk_frd =5 AND onlineloss1=5 AND recode_eexpin2b =0) OR
(onln_bnk_frd =5 AND onlineloss1=0 AND recode_eexpin2b =5) OR

```
(onln_bnk_frd =5 AND onlineloss1=0 AND recode_eexpin2b =0) OR
(onln_bnk_frd =0 AND onlineloss1=5 AND recode_eexpin2b =5) OR
(onln_bnk_frd =0 AND onlineloss1=5 AND recode_eexpin2b =0) OR
(onln_bnk_frd =0 AND onlineloss1=0 AND recode_eexpin2b =5) OR
(onln_bnk_frd =0 AND onlineloss1=0 AND recode_eexpin2b =0).
COMPUTE losswhileint=0.
ELSE IF
(onln_bnk_frd =5 AND onlineloss1=5 AND recode_eexpin2b =5).
COMPUTE losswhileint=5.
ELSE.
COMPUTE losswhileint=1.
END IF.
EXECUTE.
```

Finally, card-not-present fraud variable and losswhileint variable were merged to get outcome variable economic cybercrime victimisation (econ-cyber).

```
DO IF
(CARD_NOT_PRESENT_FRAUD =0 AND LOSSWHILEINT =0) OR
(CARD_NOT_PRESENT_FRAUD =5 AND LOSSWHILEINT =0) OR
(CARD_NOT_PRESENT_FRAUD =0 AND LOSSWHILEINT =5).
COMPUTE ECON_CYBER =0.
ELSE IF
(CARD_NOT_PRESENT_FRAUD =5 AND LOSSWHILEINT =5).
COMPUTE ECON_CYBER =5.
ELSE.
COMPUTE ECON_CYBER=1.
END IF.
EXECUTE
```

## Appendix 8: Glossary

**Adult Content:** Adult content includes pornography or images depicting sexual intercourse and images or videos displaying violence, which are generally accepted to be inappropriate for the individuals who are under 18 years old.

**Baby Boomers:** Baby boomers refer to age group preceding Generation X. Individuals who were born between 1946 and 1964 are generally considered to be a member of Baby Boomers.

**Black Friday:** Although Black Friday has a religious reference, the Friday following Thanksgiving Day, the fourth Thursday of November, it is increasingly referred to a special shopping day that discounts are offered.

**Computer-assisted crimes:** Computer-assisted crimes are online crimes that can be committed in the real-world, but networked technologies facilitated the commission of the offences

**Computer content crimes:** Computer content crimes are related to the content of the computer such as the distribution of pornography and hate crime. Offensive communications like cyberbullying and cyberstalking are also considered as computer content crimes

**Computer integrity crimes:** Computer integrity crimes are those that involve a crime against networked computer systems. Hacking is the most vivid example of computer integrity crimes.

**Crypotomarkets:** Cryptomarkets are online black markets that serve as an environment for offences such as illegal drug trading, selling of counterfeit products.

**Digital immigrants:** Digital immigrant is a term used to define people who were born prior to the widespread use of networked Internet technologies. Baby boomers and Generation X Internet users are considered to be digital immigrants.

**Drive-by-download:** Drive-by download refers to the unintended download of a malware (i.e. computer virus or spyware). Drive-by-download may initiate by visiting a website or clicking a link.

**Dumpster diving:** Dumpster diving is an identity theft method aimed to collect information through disposed of documents such as bills or invoices.

**Fear appeal:** Fear appeals are intimidating messages aimed to cause fear and anxiety. A fear appeal mostly contains two parts. The first part, which presents a problem, and the second part, which suggests a proposed solution to thwart the imminent threat described in the first part.

**Generation X:** Generation X is a marketing term used to define individuals born between 1967 and 1976.

**Generation Y:** Generation Y refers to people who were born between 1977 and 1988.

**Illegal downloading:** Illegal downloading is accessing copyrighted materials without the consent of the copyright holder. Illegal downloads are mostly provided by websites designed for distribution of copyrighted digital materials.

**Keylogger:** Keylogger is software or hardware that is utilised to capture keystrokes to retrieve Internet users' personal information.

**Live streaming:** Live streaming denotes accessing live broadcasts such as football matches online in real time.

**Malware:** Malware is a short form of malicious software, which is designed to produce harm on target computers or computer systems. Computer viruses, trojan horses, keyloggers are examples of malware.

**Peer to Peer Sharing (P2P):** Peer-to-peer file sharing enables Internet users to access or obtain digital media files (i.e. films, music or games), which are located in other Internet users' shared file folders, via P2P software.

**Pharming:** Pharming is a cyber attack utilised to exploit DNS server vulnerabilities to direct website traffic to bogus websites. DNS servers are responsible for regulating Internet traffic by communicating with each other. DNS serves holds IP (Internet Protocol) addresses and matches it with hostnames.

**Phone phreaking:** Phreaking is one of the earliest means of stealing personal information via telephone lines.

**SmiShing:** SmiShing is a short form of the term, SMS phishing. It is a method utilised by fraudsters to obtain personal information via socially engineered SMS messages.

**Spamming:** Spamming is the distribution of unsolicited messages via computer systems. Spam messages are mostly advertisements sent repeatedly.

**Torrent downloading:** Torrent downloading is another form of peer-to-peer sharing. Digital materials are distributed through torrent servers and peers. A software program and torrent file, which is downloaded via torrent websites, are required to download digital materials.

**Zero-day attack:** Zero-day attacks are online malicious attacks that Internet security software companies are not aware of it. Networked computer systems are vulnerable to such treats since a countermeasure has not been devised.

## Bibliography


A. Harris, M. and P. Patten, K. 2014, "Mobile Device Security Considerations for Small-and Medium-Sized Enterprise Business Mobility", *Information Management & Computer Security*, Vol. 22 No. 1**,** pp. 97-114.

Abbas, T. and Charles, T. 2003, Handbook of Mixed Methods in Social and Behavioral Research. Thousand Oaks: Sage.

Abdallah, A., Maarof, M. A. and Zainal, A. 2016, "Fraud Detection System: A Survey", *Journal of Network and Computer Applications*, Vol. 68 No. 90-113.

Abdullah, A., Marzbali, M. H., Woolley, H., Bahauddin, A. and Maliki, N. Z. 2014, "Testing for Individual Factors for the Fear of Crime Using a Multiple Indicator-Multiple Cause Model", *European Journal on Criminal Policy and Research*, Vol. 20 No. 1**,** pp. 1-22.

Ablon, L., Libicki, M. C. and Golay, A. A. 2014, *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, Rand Corporation.

Abraham, S. and Chengalur-Smith, I. 2010, "An Overview of Social Engineering Malware: Trends, Tactics, and Implications", *Technology in Society*, Vol. 32 No. 3**,** pp. 183-196.

Acquaviva, K., Haskell, H. and Johnson, J. 2013, "Human Cognition and the Dynamics of Failure to Rescue: The Lewis Blackman Case", *Journal of Professional Nursing*, Vol. 29 No. 2**,** pp. 95-101.

Action Fraud. 2017, "As Identity Fraud Hits Record Levels Survey Reveals That People Are Still Not Protecting Themselves. available at: https://www.actionfraud.police.uk/news/as-identity-fraud-hits-record-levels-survey-reveals-that-people-are-still-not-protecting-themselves-jun17 (accessed 01/09/2017).

Afi. 2017, "Identifying the Cost of Fraud to the Uk Economy", available at: https://brand.crowe.co.uk/wp-content/uploads/sites/2/2017/11/Annual-fraud-indicator-2017.pdf (accessed 01/09/2018).

Afifi, W. A. and Weiner, J. L. 2004, "Toward a Theory of Motivated Information Management", *Communication Theory*, Vol. 14 No. 2**,** pp. 167-190.

Afseer, K. 2017, "Active Social Networking Site Usage and Its Effects on the Quality of Marital Lifeand Family Relationships among It Professionals", *International Research Journal of Multidisciplinary Studies*, Vol. 3 No. 8**,** pp.

Agresti, A. 1996, *An Introduction to Categorical Data Analysis*, Wiley New York.

Aguiar, L. 2017, "Let the Music Play? Free Streaming and Its Effects on Digital Music Consumption", *Information Economics and Policy*, Vol. 41 No. 1-14.

Ahmad, Z., Zeki, A. M. and Olowolayemo, A. (2016), "Security Failures in Emv Smart Card Payment Systems", paper presented at the *Information and Communication Technology for The Muslim World (ICT4M), 2016 6th International Conference on*,2016, avaialable at.

Akers, R. L. 1999, "Criminological Theories", Vol. No.

Akhgar, B. and Arabnia, H. R. 2013, *Emerging Trends in Ict Security*, Newnes.

Akhgar, B., Choras, M., Brewster, B., Bosco, F., Veermeersch, E., Luda, V., Puchalski, D. and Wells, D. 2016, "Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism", in: Akhgar, B. and Brewster, B. (eds.), *Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities*, Springer. pp. 295-322.

Al-Saggaf, Y. and Islam, M. Z. 2015, "Data Mining and Privacy of Social Network Sites' Users: Implications of the Data Mining Problem", *Science and engineering ethics*, Vol. 21 No. 4**,** pp. 941-966.

Albuquerque, U. P., Ramos, M. A., De Lucena, R. F. P. and Alencar, N. L. 2014, "Methods and Techniques Used to Collect Ethnobiological Data", *Methods and Techniques in Ethnobiology and Ethnoecology*, Springer. pp. 15-37.

Aldridge, J. 2019, "Does Online Anonymity Boost Illegal Market Trading?", *Media, Culture & Society*, Vol. No. 0163443719842075.

Algarni, A., Xu, Y. and Chan, T. 2017, "An Empirical Study on the Susceptibility to Social Engineering in Social Networking Sites: The Case of Facebook", *European Journal of Information Systems*, Vol. 26 No. 6**,** pp. 661-687.

Almomani, A., Gupta, B., Atawneh, S., Meulenberg, A. and Almomani, E. 2013, "A Survey of Phishing Email Filtering Techniques", *IEEE communications surveys & tutorials*, Vol. 15 No. 4**,** pp. 2070-2090.

Alshalan, A. 2006, *Cybercrime Fear and Victimization: An Analysis of a National Survey*, ProQuest.

Alsharnouby, M., Alaca, F. and Chiasson, S. 2015, "Why Phishing Still Works: User Strategies for Combating Phishing Attacks", *International Journal of Human-Computer Studies*, Vol. 82 No. 69-82.

Alwagait, E., Shahzad, B. and Alim, S. 2015, "Impact of Social Media Usage on Students' Academic Performance in Saudi Arabia", *Computers in Human Behavior*, Vol. 51 No. 1092-1097.

Amerio, P. and Roccato, M. 2005, "A Predictive Model for Psychological Reactions to Crime in Italy: An Analysis of Fear of Crime and Concern About Crime as a Social Problem", *Journal of Community & Applied Social Psychology*, Vol. 15 No. 1**,** pp. 17-28.
Amir, M. 1971, *Patterns in Forcible Rape*, University of Chicago Press Chicago.
Anderson, C. L. and Agarwal, R. 2010, "Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions", *MIS quarterly*, Vol. 34 No. 3**,** pp. 613-643.
Anderson, D. M., Strand, A. and Collins, J. M. 2018, "The Impact of Electronic Payments for Vulnerable Consumers: Evidence from Social Security", *Journal of Consumer Affairs*, Vol. 52 No. 1**,** pp. 35-60.
Anderson, I., Beattie, G. and Spencer, C. 2001, "Can Blaming Victims of Rape Be Logical? Attribution Theory and Discourse Analytic Perspectives", *Human Relations*, Vol. 54 No. 4**,** pp. 445-467.
Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T. and Savage, S. 2013, "Measuring the Cost of Cybercrime", *The Economics of Information Security and Privacy*, Springer. pp. 265-300.
Angst, C. M., Block, E. S., D'arcy, J. and Kelley, K. 2017, "When Do It Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches", *Mis Quarterly*, Vol. 41 No. 3**,** pp.
Anshari, M., Alas, Y., Hardaker, G., Jaidin, J., Smith, M. and Ahad, A. 2016, "Smartphone Habit and Behavior in Brunei: Personalization, Gender, and Generation Gap", *Computers in Human Behavior*, Vol. 64 No. 719-727.
Anshel, M. H. and Wells, B. 2000, "Personal and Situational Variables That Describe Coping with Acute Stress in Competitive Sport", *The Journal of social psychology*, Vol. 140 No. 4**,** pp. 434-450.
Anthe, C., Johenson, M., Pavithran, S. and Argyle, E. 2016, "Microsoft Security Intelligence Report", available at: https://www.microsoft.com/security/sir/default.aspx (accessed 21/03/2107).
Apwg Report. 2017, "Phishing Activity Trends Report 4th Quarter 2016", available at: http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf (accessed 18 September 2017).
Arachchilage, N. a. G. and Love, S. 2014, "Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective", *Computers in Human Behavior*, Vol. 38 No. 304-312.
Arachchilage, N. a. G., Love, S. and Beznosov, K. 2016, "Phishing Threat Avoidance Behaviour: An Empirical Investigation", *Computers in Human Behavior*, Vol. 60 No. 185-197.
Arango, C., Huynh, K. P. and Sabetti, L. 2015, "Consumer Payment Choice: Merchant Card Acceptance Versus Pricing Incentives", *Journal of Banking & Finance*, Vol. 55 No. 130-141.
Archer, M. S. 2007, *Making Our Way through the World: Human Reflexivity and Social Mobility*, Cambridge University Press.
Arenas Gaitán, J., Peral Peral, B. and Ramón Jerónimo, M. 2015, "Elderly and Internet Banking: An Application of Utaut2", *Journal of Internet Banking and Commerce*, Vol. 20 No. 1**,** pp. 1-23.
Ariel, B. and Partridge, H. 2017, "Predictable Policing: Measuring the Crime Control Benefits of Hotspots Policing at Bus Stops", *Journal of Quantitative Criminology*, Vol. 33 No. 4**,** pp. 809-833.
Armstrong, L. 1987, *Kiss Daddy Goodnight: Ten Years Later*, Pocket Books New York.
Asudani, P. 2018, "Social Networking Sites and Cybercrime a Study of Deviance among Adolescents of Jaipur City", Vol. No.
Auer, M. M. and Griffiths, M. D. 2016, "Personalized Behavioral Feedback for Online Gamblers: A Real World Empirical Study", *Frontiers in Psychology*, Vol. 7 No. 1875.
Azen, R. and Walker, C. M. 2011, *Categorical Data Analysis for the Behavioral and Social Sciences*, Routledge.
Bachman, R. D. and Schutt, R. K. 2016, *Fundamentals of Research in Criminology and Criminal Justice*, Sage Publications.
Badger, F. and Werrett, J. 2005, "Room for Improvement? Reporting Response Rates and Recruitment in Nursing Research in the Past Decade", *Journal of Advanced Nursing*, Vol. 51 No. 5**,** pp. 502-510.
Balduzzi, M., Gupta, P., Gu, L., Gao, D. and Ahamad, M. (2016), "Mobipot: Understanding Mobile Telephony Threats with Honeycards", paper presented at the *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*,2016, avaialable at.
Balestrat, M. 2016, "Drive-by Downloads: What You Need to Know. available at: https://blog.breachalarm.com/drive-by-downloads-what-you-need-to-know (accessed 23/11/2017).
Bamberger, M. 2000, *Integrating Quantitative and Qualitative Research in Development Projects: Lessons from the Field*, The World Bank.
Bancroft, A. and Scott Reid, P. 2017, "Challenging the Techno-Politics of Anonymity: The Case of Cryptomarket Users", *Information, Communication & Society*, Vol. 20 No. 4**,** pp. 497-512.
Banka, H. 2018, "The Macroeconomic Impact of Payment Cards", *Journal of Payments Strategy & Systems*, Vol. 11 No. 4**,** pp. 313-333.
Banks, J. 2012, "Online Gambling and Crime: A Sure Bet?", *The ETHICOMP Journal*, Vol. No.
Bannister, J. and Fyfe, N. 2001, Introduction: Fear and the City. Sage Publications Sage UK: London, England.

Barnard, J. W. 2001, "Allocution for Victims of Economic Crimes", *Notre Dame L. Rev.*, Vol. 77 No. 39.
Barrett, B. 2016, "Most Top Websites Still Don't Use a Basic Security Feature. available at: https://www.wired.com/2016/03/https-adoption-google-report/ (accessed 10/10/2018).
Barry, K. 1984, *Female Sexual Slavery*, New York Univesity Press, New York.
Bate, L., Hutchinson, A., Underhill, J. and Maskrey, N. 2012, "How Clinical Decisions Are Made", *British Journal of Clinical Pharmacology*, Vol. 74 No. 4**,** pp. 614-620.
Baumgarten, M. 2010, "Paradigm Wars-Validity and Reliability in Qualitative Research", Vol. No.
Bayley, J. E. 1991, "The Concept of Victimhood", *To Be a Victim*, Springer. pp. 53-62.
Bbc. 2017, "Fake Whatsapp App Downloaded More Than One Million Times. available at: https://www.bbc.co.uk/news/technology-41886157.
Beck, C. T. 1993, "Qualitative Research: The Evaluation of Its Credibility, Fittingness, and Auditability", *Western journal of nursing research*, Vol. 15 No. 2**,** pp. 263-266.
Beck, K. H. and Lund, A. K. 1981, "The Effects of Health Threat Seriousness and Personal Efficacy Upon Intentions and Behavior ", *Journal of Applied Social Psychology*, Vol. 11 No. 5**,** pp. 401-415.
Becker, P. and Wetzell, R. F. 2006, *Criminals and Their Scientists: The History of Criminology in International Perspective*, Cambridge University Press.
Bellone, E. T. 2013, "Protecting Business and Preventing Property Theft: A Routine Activities Theory Approach", *Holy Cross JL & Pub. Pol'y*, Vol. 17 No. 44.
Benenson, Z., Gassmann, F. and Landwirth, R. (2017), "Unpacking Spear Phishing Susceptibility", paper presented at the *International Conference on Financial Cryptography and Data Security*,2017, avaialable at.
Benight, C. C. 2012, "Understanding Human Adaptation to Traumatic Stress Exposure: Beyond the Medical Model", *Psychological Trauma: Theory, Research, Practice, and Policy*, Vol. 4 No. 1**,** pp. 1.
Bereska, T. M. 2013, *Deviance, Conformity, and Social Control in Canada*, Pearson Education Canada.
Berg, B. L., Lune, H. and Lune, H. 2004, *Qualitative Research Methods for the Social Sciences*, Pearson Boston, MA.
Berger, R. J. and Searles, P. 1985, "Victim-Offender Interaction in Rape: Victimological, Situational, and Feminist Perspectives", *Women's Studies Quarterly*, Vol. 13 No. 3/4**,** pp. 9-15.
Bergman, M. M. 2008, *Advances in Mixed Methods Research: Theories and Applications*, Sage.
Bettany, A. and Halsey, M. 2017, "What Is Malware?", in: Bettany, A. and Halsey, M. (eds.), *Windows Virus and Malware Troubleshooting*, Springer. pp. 1-8.
Biddix, J. P. 2018, *Research Methods and Applications for Student Affairs*, John Wiley & Sons.
Biernacki, P. and Waldorf, D. 1981, "Snowball Sampling: Problems and Techniques of Chain Referral Sampling", *Sociological methods & research*, Vol. 10 No. 2**,** pp. 141-163.
Binder, E. 1999, "Fear and Anxiety. available at: http://www.csun.edu/~vcpsy00h/students/anxiety.htm (accessed 13/01/2019).
Biradavolu, M. R., Burris, S., George, A., Jena, A. and Blankenship, K. M. 2009, "Can Sex Workers Regulate Police? Learning from an Hiv Prevention Project for Sex Workers in Southern India", *Social science & medicine*, Vol. 68 No. 8**,** pp. 1541-1547.
Birmingham, J. and David, M. 2011, "Live-Streaming: Will Football Fans Continue to Be More Law Abiding Than Music Fans?", *Sport in Society*, Vol. 14 No. 1**,** pp. 69-80.
Blaikie, N. 2003, *Analyzing Quantitative Data: From Description to Explanation*, Sage.
Blanco Hache, A. C. and Ryder, N. 2011, "'Tis the Season to (Be Jolly?) Wise-up to Online Fraudsters. Criminals on the Web Lurking to Scam Shoppers This Christmas: A Critical Analysis of the United Kingdom's Legislative Provisions and Policies to Tackle Online Fraud", *Information & Communications Technology Law*, Vol. 20 No. 1**,** pp. 35-56.
Blankenship, D. 2010, *Applied Research and Evaluation Methods in Recreation*, Human Kinetics.
Blessing, L. T. and Chakrabarti, A. 2009, *Drm, a Design Research Methodology*, Springer Science & Business Media.
Blythe, M., Petrie, H. and Clark, J. A. (2011), "F for Fake: Four Studies on How We Fall for Phish", paper presented at the *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*,2011, avaialable at.
Boateng, F. D. 2016, "Fearfulness in the Community: Empirical Assessments of Influential Factors", *Journal of interpersonal violence*, Vol. No. 0886260516642295.
Bohm, R. M. and Vogel, B. 2010, *A Primer on Crime and Delinquency Theory*, Cengage Learning.
Bossler, A. M. and Holt, T. J. 2009, "Online Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory", *International Journal of Cyber Criminology*, Vol. 3 No. 1**,** pp. 400.
Bossler, A. M. and Holt, T. J. 2010, "The Effect of Self-Control on Victimization in the Cyberworld", *Journal of Criminal Justice*, Vol. 38 No. 3**,** pp. 227-236.

Bowen, B. M., Devarajan, R. and Stolfo, S. (2011), "Measuring the Human Factor Ff Cyber Security", paper presented at the *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*,2011, avaialable at.

Bowen, G. A. 2008, "Naturalistic Inquiry and the Saturation Concept: A Research Note", *Qualitative research*, Vol. 8 No. 1**,** pp. 137-152.

Box, S., Hale, C. and Andrews, G. 1988, "Explaining Fear of Crime", *The British Journal of Criminology*, Vol. 28 No. 3**,** pp. 340-356.

Boyle, M., Koritsas, S., Coles, J. and Stanley, J. 2007, "A Pilot Study of Workplace Violence Towards Paramedics", *Emergency Medicine Journal*, Vol. 24 No. 11**,** pp. 760-763.

Braga, A. A. and Bond, B. J. 2008, "Policing Crime and Disorder Hot Spots: A Randomized Controlled Trial", *Criminology*, Vol. 46 No. 3**,** pp. 577-607.

Brenner, S. W. 2007, "The Council of Europe's Convention on Cybercrime", in: Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S. and Zarsky, T. (eds.), *Cybercrime: Digital Cops in a Networked Environment*, NYU Press. pp. 207-221.

Brenner, S. W. 2010, *Cybercrime: Criminal Threats from Cyberspace*, USA: Prager.

Brenza, S., Pawlowski, A. and Pöpper, C. (2015), "A Practical Investigation of Identity Theft Vulnerabilities in Eduroam", paper presented at the *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*,2015, avaialable at.

Brewer, M. B. and Crano, W. D. 2000, "Research Design and Issues of Validity", *Handbook of research methods in social and personality psychology*, Vol. No. 3-16.

Britten, N. 1995, "Qualitative Research: Qualitative Interviews in Medical Research", *Bmj*, Vol. 311 No. 6999**,** pp. 251-253.

Brody, R. G., Mulig, E. and Kimball, V. 2007, "Phishing, Pharming and Identity Theft", *Academy of Accounting & Financial Studies Journal*, Vol. 11 No. 3**,** pp.

Bröhl, C., Rasche, P., Jablonski, J., Theis, S., Wille, M. and Mertens, A. (2018), "Desktop Pc, Tablet Pc, or Smartphone? An Analysis of Use Preferences in Daily Activities for Different Technology Generations of a Worldwide Sample", paper presented at the *International Conference on Human Aspects of IT for the Aged Population*,2018, avaialable at.

Brunton-Smith, I. 2017, "Fear 2.0: Worry About Cybercrime in England and Wales", *The Routledge International Handbook on Fear of Crime*, Routledge. pp. 113-125.

Bryce, J. and Fraser, J. 2014, "The Role of Disclosure of Personal Information in the Evaluation of Risk and Trust in Young Peoples' Online Interactions", *Computers in Human Behavior*, Vol. No. 30**,** pp. 299-306.

Bryman, A. 2008, *Social Research Methods*, Oxford : Oxford University Press, Oxford.

Buchanan, D. E., Fisher, C. B. and Gable, L. E. 2009, *Research with High-Risk Populations: Balancing Science, Ethics, and Law*, American Psychological Association.

Bulakh, V. and Gupta, M. (2016), "Countering Phishing from Brands' Vantage Point", paper presented at the *Proceedings of the 2016 ACM on International Workshop on Security And Privacy Analytics*,2016, avaialable at.

Bulchand-Gidumal, J., Melián-González, S. and González López-Valcárcel, B. 2011, "Improving Hotel Ratings by Offering Free Wi-Fi", *Journal of Hospitality and Tourism Technology*, Vol. 2 No. 3**,** pp. 235-245.

Bullée, J.-W. H., Montoya, L., Pieters, W., Junger, M. and Hartel, P. H. 2015, "The Persuasion and Security Awareness Experiment: Reducing the Success of Social Engineering Attacks", *Journal of experimental criminology*, Vol. 11 No. 1**,** pp. 97-115.

Buller, D., Buller, M. K., Larkey, L., Sennott-Miller, L., Taren, D., Aickin, M., Wentzel, T. M. and Morrill, C. 2000, "Implementing a 5-a-Day Peer Health Educator Program for Public Sector Labor and Trades Employees", *Health Education & Behavior*, Vol. 27 No. 2**,** pp. 232-240.

Burgard, A. and Schlembach, C. 2013, "Frames of Fraud: A Qualitative Analysis of the Structure and Process of Victimization on the Internet", *International Journal of Cyber Criminology*, Vol. 7 No. 2**,** pp. 112.

Butavicius, M., Parsons, K., Pattinson, M. and Mccormac, A. 2016, "Breaching the Human Firewall: Social Engineering in Phishing and Spear-Phishing Emails", *arXiv preprint arXiv:1606.00887*, Vol. No.

Button, M., Lewis, C. and Tapley, J. 2009, "Fraud Typologies and the Victims of Fraud: Literature Review", Vol. No.

Button, M., Lewis, C. and Tapley, J. 2014a, "Not a Victimless Crime: The Impact of Fraud on Individual Victims and Their Families", *Security Journal*, Vol. 27 No. 1**,** pp. 36-54.

Button, M., Nicholls, C. M., Kerr, J. and Owen, R. 2014b, "Online Frauds: Learning from Victims Why They Fall for These Scams", *Australian & New Zealand Journal of Criminology*, Vol. 47 No. 3**,** pp. 391-408.

Buzzell, T., Foss, D. and Middleton, Z. 2006, "Explaining Use of Online Pornography: A Test of Self-Control Theory and Opportunities for Deviance", *Journal of Criminal Justice and Popular Culture*, Vol. 13 No. 2**,** pp. 96-116.

Caldwell, T. 2013, "Spear-Phishing: How to Spot and Mitigate the Menace", *Computer Fraud & Security*, Vol. 2013 No. 1**,** pp. 11-16.
Campbell, D. T. and Fiske, D. W. 1959, "Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix", *Psychological Bulletin*, Vol. 56 No. 2**,** pp. 81-105.
Cantor, D. and Lynch, J. P. 2000, "Self-Report Surveys as Measures of Crime and Criminal Victimization", Vol. 4 No. 85-138.
Caracelli, V. J. and Greene, J. C. 1993, "Data Analysis Strategies for Mixed-Method Evaluation Designs ", *Educational evaluation and policy analysis*, Vol. 15 No. 2**,** pp. 195-207.
Carmack, H. J. and Heiss, S. N. 2018, "Using the Theory of Planned Behavior to Predict College Students' Intent to Use Linkedin for Job Searches and Professional Networking", *Communication Studies*, Vol. 69 No. 2**,** pp. 145-160.
Carminati, M., Caron, R., Maggi, F., Epifani, I. and Zanero, S. 2015, "Banksealer: A Decision Support System for Online Banking Fraud Analysis and Investigation", *computers & security*, Vol. 53 No. 175-186.
Carmines, E. G. and Zeller, R. A. 1979, *Reliability and Validity Assessment*, Sage publications.
Carter, N., Bryant-Lukosius, D., Dicenso, A., Blythe, J. and Neville, A. J. (2014), "The Use of Triangulation in Qualitative Research", paper presented at the *Oncology nursing forum*,2014, avaialable at.
Caruth, G. D. 2013, "Demystifying Mixed Methods Research Design: A Review of the Literature", *Online Submission*, Vol. 3 No. 2**,** pp. 112-122.
Carvalho, S. and White, H. 1997, *Combining the Quantitative and Qualitative Approaches to Poverty Measurement and Analysis: The Practice and the Potential*, The World Bank.
Casey, E. 2011, "Language of Computer Crime Investigation", in: Casey, E. (ed.) *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Third ed, Elsevier, London. pp. 35-48.
Castells, M. 2002, *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford University Press on Demand.
Cavender, G. 2004, "Media and Crime Policy: A Reconsideration of David Garland's the Culture of Control", *Punishment & Society*, Vol. 6 No. 3**,** pp. 335-348.
Celsi, R. L. and Olson, J. C. 1988, "The Role of Involvement in Attention and Comprehension Processes", *Journal of consumer research*, Vol. 15 No. 2**,** pp. 210-224.
Chainey, S., Tompson, L. and Uhlig, S. 2008, "The Utility of Hotspot Mapping for Predicting Spatial Patterns of Crime", *Security journal*, Vol. 21 No. 1-2**,** pp. 4-28.
Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S. and Rao, H. R. 2016, "Online Shopping Intention in the Context of Data Breach in Online Retail Stores: An Examination of Older and Younger Adults", *Decision Support Systems*, Vol. 83 No. 47-56.
Chandio, F. H., Irani, Z., Zeki, A. M., Shah, A. and Shah, S. C. 2017, "Online Banking Information Systems Acceptance: An Empirical Examination of System Characteristics and Web Security", *Information Systems Management*, Vol. 34 No. 1**,** pp. 50-64.
Chandra, A. and Paul Iii, D. P. 2003, "African American Participation in Clinical Trials: Recruitment Difficulties and Potential Remedies", *Hospital topics*, Vol. 81 No. 2**,** pp. 33-38.
Chang, M. K., Cheung, W. and Tang, M. 2013, "Building Trust Online: Interactions among Trust Building Mechanisms", *Information & Management*, Vol. 50 No. 7**,** pp. 439-445.
Chang, M. L. and Wu, W. Y. 2012, "Revisiting Perceived Risk in the Context of Online Shopping: An Alternative Perspective of Decision-Making Styles", *Psychology & Marketing*, Vol. 29 No. 5**,** pp. 378-400.
Chavez, N. M. 2018, "Can We Learn from Hackers to Protect Victims?", Vol. No.
Check Point. 2014, "Rogue Wi-Fi Hotspots – Why Getting Coffee Is Putting Your Enterprise at Risk (Social Engineering Ep. 4). available at: https://blog.checkpoint.com/2014/05/06/rogue-wifi-hotspots-getting-coffee-putting-enterprise-risk-social-engineering-ep-4/ (accessed 04/12/2017).
Chen, H.-T. and Chen, W. 2015, "Couldn't or Wouldn't? The Influence of Privacy Concerns and Self-Efficacy in Privacy Management on Privacy Protection", *Cyberpsychology, Behavior, and Social Networking*, Vol. 18 No. 1**,** pp. 13-19.
Chen, H., Beaudoin, C. E. and Hong, T. 2016, "Protecting Oneself Online: The Effects of Negative Privacy Experiences on Privacy Protective Behaviors", *Journalism & Mass Communication Quarterly*, Vol. 93 No. 2**,** pp. 409-429.
Chen, H., Beaudoin, C. E. and Hong, T. 2017, "Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviors", *Computers in Human Behavior*, Vol. 70 No. 291-302.
Chen, Y.-T. and Chou, T.-Y. 2012, "Exploring the Continuance Intentions of Consumers for B2c Online Shopping: Perspectives of Fairness and Trust", *Online Information Review*, Vol. 36 No. 1**,** pp. 104-125.
Chen, Y. 2017, "Examining Internet Users' Adaptive and Maladaptive Security Behaviors Using the Extended Parallel Process Model", Vol. No.

Chen, Y. and Zahedi, F. M. 2016, "Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts between the United States and China", *Mis Quarterly*, Vol. 40 No. 1**,** pp. 205-222.
Chenoweth, T., Minch, R. and Gattiker, T. (2009), "Application of Protection Motivation Theory to Adoption of Protective Technologies", paper presented at the *System Sciences, 2009. HICSS'09. 42nd Hawaii International Conference on*,2009, avaialable at.
Cheshire, C., Antin, J. and Churchill, E. 2010, "Behaviors, Adverse Events, and Dispositions: An Empirical Study of Online Discretion and Information Control", *Journal of the Association for Information Science and Technology*, Vol. 61 No. 7**,** pp. 1487-1501.
Ching, A. T. and Hayashi, F. 2010, "Payment Card Rewards Programs and Consumer Payment Choice", *Journal of Banking & Finance*, Vol. 34 No. 8**,** pp. 1773-1787.
Chiu, C.-C. and Yang, H.-E. 2016, "The Impact of Website Design Features on Behavioral Intentions", *International journal of scientific & technology research*, Vol. 9 No. 5**,** pp. 71-78.
Chiu, Y.-N., Leclerc, B. and Townsley, M. 2011, "Crime Script Analysis of Drug Manufacturing in Clandestine Laboratories Implications for Prevention", *British journal of criminology*, Vol. 51 No. 2**,** pp. 355-374.
Choi, K.-S. 2008, "Computer Crime Victimization and Integrated Theory: An Empirical Assessment", *International Journal of Cyber Criminology*, Vol. 2 No. 1**,** pp. 308.
Choi, K.-S. 2011, "Cyber-Routine Activities: Empirical Examination of Online Lifestyle, Digital Guardians, and Computer-Crime Victimization", *Cyber Criminology*, CRC Press. pp. 265-288.
Choi, K.-S., Choo, K. and Sung, Y.-E. 2016, "Demographic Variables and Risk Factors in Computer-Crime: An Empirical Assessment", *Cluster Computing*, Vol. 19 No. 1**,** pp. 369-377.
Chu, B., Holt, T. J. and Ahn, G. J. 2010, "Examining the Creation, Distribution, and Function of Malware on-Line", *National Institute of Justice, Washington, DC*, Vol. No.
Chu, B., Holt, T. J. and Ahn, G. J. 2012, "Examining the Creation, Distribution, and Function of Malware on-Line": BiblioGov, available at: https://www.ncjrs.gov/pdffiles1/nij/grants/230111.pdf (accessed 15/10/2016).
Chun, C.-A., Moos, R. H. and Cronkite, R. C. 2006, "Culture: A Fundamental Context for the Stress and Coping Paradigm", *Handbook of Multicultural Perspectives on Stress and Coping*, Springer. pp. 29-53.
Churchill, G. A. and Doerge, R. W. 1994, "Empirical Threshold Values for Quantitative Trait Mapping", *Genetics*, Vol. 138 No. 3**,** pp. 963-971.
Cialdini, R. B. 2009, *Influence: Science and Practice*, Pearson education Boston, MA.
Cifas 2018, "The Fraudscape", Vol. No.
Claar, C. L. and Johnson, J. 2012, "Analyzing Home Pc Security Adoption Behavior", *Journal of Computer Information Systems*, Vol. 52 No. 4**,** pp. 20-29.
Clark, J. 2003, "Fear in Fear-of-Crime", *Psychiatry, Psychology and Law*, Vol. 10 No. 2**,** pp. 267-282.
Clark, J. W. 2017, "Trends in Social Engineering: Securing the Weakest Link", Vol. No.
Clark, T. 2008, "We're over-Researched Here!' Exploring Accounts of Research Fatigue within Qualitative Research Engagements", *Sociology*, Vol. 42 No. 5**,** pp. 953-970.
Clark, V. L. P. and Creswell, J. W. 2014, *Understanding Research: A Consumer's Guide*, Pearson Higher Ed.
Clarke, R. V. 1995, "Situational Crime Prevention", *Crime and justice*, Vol. No. 91-150.
Clarke, R. V. 2004, "Technology, Criminology and Crime Science", *European Journal on Criminal Policy and Research*, Vol. 10 No. 1**,** pp. 55-63.
Clarke, R. V. and Felson, M. 1998, "Oportunity Makes the Thief: Practical Theory for Crime Prevention", (accessed.
Close, A. G. and Zinkhan, G. M. 2009, "Market-Resistance and Valentine's Day Events", *Journal of Business Research*, Vol. 62 No. 2**,** pp. 200-207.
Close, S., Smaldone, A., Fennoy, I., Reame, N. and Grey, M. 2013, "Using Information Technology and Social Networking for Recruitment of Research Participants: Experience from an Exploratory Study of Pediatric Klinefelter Syndrome", *Journal of medical Internet research*, Vol. 15 No. 3**,** pp.
Clough, J. 2014, "A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation", *Monash UL Rev.*, Vol. 40 No. 698.
Cluley, G. 2010, "Sizing up the Malware Threat–Key Malware Trends for 2010", *Network Security*, Vol. 2010 No. 4**,** pp. 8-10.
Cobbina, J. E., Miller, J. and Brunson, R. K. 2008, "Gender, Neighborhood Danger, and Risk-Avoidance Strategies among Urban African-American Youths", *Criminology*, Vol. 46 No. 3**,** pp. 673-709.
Cohen, L. E. and Cantor, D. 1981, "Residential Burglary in the United States: Life-Style and Demographic Factors Associated with the Probability of Victimization", *Journal of Research in Crime and Delinquency*, Vol. 18 No. 1**,** pp. 113-127.
Cohen, L. E. and Felson, M. 1979, "Social Change and Crime Rate Trends: A Routine Activity Approach", *American Sociological Review*, Vol. 44 No. 4**,** pp. 588-608.

Cohen, L. E., Kluegel, J. R. and Land, K. C. 1981, "Social Inequality and Predatory Criminal Victimization: An Exposition and Test of a Formal Theory", *American Sociological Review*, Vol. 46 No. 5**,** pp. 505-524.
Colbourne, L. and Sque, M. 2004, "Split Personalities: Role Conflict between the Nurse and the Nurse Researcher", *NT Research*, Vol. 9 No. 4**,** pp. 297-304.
Collins, J. J., Cox, B. G. and Langan, P. A. 1987, "Job Activities and Personal Crime Victimization: Implications for Theory", *Social Science Research*, Vol. 16 No. 4**,** pp. 345-360.
Collins, K. M., Onwuegbuzie, A. J. and Jiao, Q. G. 2006, "Prevalence of Mixed-Methods Sampling Designs in Social Science Research", *Evaluation & Research in Education*, Vol. 19 No. 2**,** pp. 83-101.
Collins, R. 1984, "Statistics Versus Words", *Sociological theory*, Vol. No. 329-362.
Compas, B. E., Orosan, P. G. and Grant, K. E. 1993, "Adolescent Stress and Coping: Implications for Psychopathology During Adolescence", *Journal of adolescence*, Vol. 16 No. 331-331.
Connelly, L. M. 2016, "Trustworthiness in Qualitative Research", *Medsurg Nursing*, Vol. 25 No. 6**,** pp. 435.
Conteh, N. Y. and Schmick, P. J. 2016, "Cybersecurity: Risks, Vulnerabilities and Countermeasures to Prevent Social Engineering Attacks", *International Journal of Advanced Computer Research*, Vol. 6 No. 23**,** pp. 31.
Convery, A. (2006), "No Victims, No Oppression: Feminist Theory and the Denial of Victimhood", paper presented at the *Actas de la Conferencia APSA, Universidad de Newcastle*,2006, avaialable at.
Cook, C. L. and Fox, K. A. 2011, "Fear of Property Crime: Examining the Effects of Victimization, Vicarious Victimization, and Perceived Risk", *Violence and Victims*, Vol. 26 No. 5**,** pp. 684-700.
Copes, H., Kerley, K. R., Huff, R. and Kane, J. 2010, "Differentiating Identity Theft: An Exploratory Study of Victims Using a National Victimization Survey", *Journal of Criminal Justice*, Vol. 38 No. 5**,** pp. 1045-1052.
Corden, A. and Sainsbury, R. 2006, *Using Verbatim Quotations in Reporting Qualitative Social Research: Researchers' Views*, University of York York.
Cornelius, D. R. 2016. *Online Identity Theft Victimization: An Assessment of Victims and Non-Victims Level of Cyber Security Knowledge.* Colorado Technical University.
Cornish, D. B. (1994), "Crimes as Scripts", paper presented at the *Proceedings of the international seminar on environmental criminology and crime analysis*,1994, avaialable at.
Corre, K., Barais, O., Sunyé, G., Frey, V. and Crom, J.-M. 2017, "Why Can't Users Choose Their Identity Providers on the Web?", *Proceedings on Privacy Enhancing Technologies*, Vol. 3 No. 72-86.
Covington, J. and Taylor, R. B. 1991, "Fear of Crime in Urban Residential Neighborhoods: Implications of between-and within-Neighborhood Sources for Current Models", *The Sociological Quarterly*, Vol. 32 No. 2**,** pp. 231-249.
Cram, W. A., Proudfoot, J. G. and D'arcy, J. 2017, "Organizational Information Security Policies: A Review and Research Framework", *European Journal of Information Systems*, Vol. 26 No. 6**,** pp. 605-641.
Cranor, L. F. 2008, "A Framework for Reasoning About the Human in the Loop", *UPSEC*, Vol. 8 No. 2008**,** pp. 1-15.
Creswell, J. W. 2009, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, Sage Publications, Thousand Oaks, CA London.
Creswell, J. W. and Miller, D. L. 2000, "Determining Validity in Qualitative Inquiry", *Theory into practice*, Vol. 39 No. 3**,** pp. 124-130.
Creswell, J. W. and Plano Clark, V. 2007, "Choosing a Mixed Methods Design", in: Creswell, J. W. and Plano Clark, V. (eds.), *Designing and Conducting Mixed Methods Research*, 2nd ed, Thousand Oaks, Calif. : SAGE Publications, Thousand Oaks, Calif. pp. 53-106.
Creswell, J. W., Plano Clark, V. L., Gutmann, M. L. and Hanson, W. E. 2003, "Advanced Mixed Methods Research Designs", in: Tashakkori, A. and Teddlie, C. (eds.), *Handbook of Mixed Methods in Social and Behavioral Research*, SAGE Publications, Thousand Oaks, Calif. pp. 209-240.
Croskerry, P. 2009, "Clinical Cognition and Diagnostic Error: Applications of a Dual Process Model of Reasoning", *Advances in health sciences education*, Vol. 14 No. 1**,** pp. 27-35.
Cross, C. and Blackshaw, D. 2014, "Improving the Police Response to Online Fraud", *Policing: a journal of policy and practice*, Vol. 9 No. 2**,** pp. 119-128.
Crossler, R. E. (2010), "Protection Motivation Theory: Understanding Determinants to Backing up Personal Data", paper presented at the *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*,2010, avaialable at.
Crow, I. and Semmens, N. 2008, *Researching Criminology*, Open University Press/McGraw-Hill, Maidenhead New York.
Cucu, P. 2017, "Security Alert: Job Seekers, Beware of This Linkedin Scam. available at: https://heimdalsecurity.com/blog/job-seekers-beware-of-this-linkedin-scam/ (accessed 18/07/2018).

Cugelman, B., Thelwall, M. and Dawes, P. 2011, "Online Interventions for Social Marketing Health Behavior Change Campaigns: A Meta-Analysis of Psychological Architectures and Adherence Factors", *Journal of medical Internet research*, Vol. 13 No. 1**,** pp.

Cui, J., Rosoff, H. and John, R. S. (2017a), "Deterrence of Cyber Attackers in a Three-Player Behavioral Game", paper presented at the *International Conference on Decision and Game Theory for Security*,2017a, avaialable at.

Cui, Q., Jourdan, G.-V., Bochmann, G. V., Couturier, R. and Onut, I.-V. (2017b), "Tracking Phishing Attacks over Time", paper presented at the *Proceedings of the 26th International Conference on World Wide Web*,2017b, avaialable at.

Culnan, M. J. and Armstrong, P. K. 1999, "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation", *Organization science*, Vol. 10 No. 1**,** pp. 104-115.

Cunniff Gilson, E. 2016, "Vulnerability and Victimization: Rethinking Key Concepts in Feminist Discourses on Sexual Violence", *Signs: Journal of Women in Culture and Society*, Vol. 42 No. 1**,** pp. 71-98.

Curtis, W., Murphy, M. and Shields, S. 2013, *Research and Education*, Routledge.

D'alessandro, S., Girardi, A. and Tiangsoongnern, L. 2012, "Perceived Risk and Trust as Antecedents of Online Purchasing Behavior in the Usa Gemstone Industry", *Asia Pacific Journal of Marketing and Logistics*, Vol. 24 No. 3**,** pp. 433-460.

Dahiya, M. and Gill, S. 2017, "Detection of Rogue Access Point in Wlan Using Hopfield Neural Network", *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 7 No. 2**,** pp. 1060-1070.

Dai, B., Forsythe, S. and Kwon, W.-S. 2014, "The Impact of Online Shopping Experience on Risk Perceptions and Online Purchase Intentions: Does Product Category Matter?", *Journal of Electronic Commerce Research*, Vol. 15 No. 1**,** pp. 13.

Daigle, L. E. 2017, *Victimology: A Text/Reader*, SAGE Publications.

Dale, A., Arber, S. and Procter, M. 1988, *Doing Secondary Analysis*, Unwin Hyman.

Daley, A. 2010, "Reflections on Reflexivity and Critical Reflection as Critical Research Practices", *Affilia*, Vol. 25 No. 1**,** pp. 68-82.

Daniel, P. S. and Sam, A. G. 2011, *Research Methodology*, Gyan Publishing House.

Darwish, A., El Zarka, A. and Aloul, F. (2012), "Towards Understanding Phishing Victims' Profile", paper presented at the *Computer Systems and Industrial Informatics (ICCSII), 2012 International Conference on*,2012, avaialable at.

Darya Gudkova, Maria Vergelis, Tatyana Shcherbakova and Demidova, N. 2017, "Spam and Phishing in Q2 2017. available at: https://securelist.com/spam-and-phishing-in-q2-2017/81537/ (accessed 18/09/2017).

Das, A., Bonneau, J., Caesar, M., Borisov, N. and Wang, X. (2014), "The Tangled Web of Password Reuse", paper presented at the *NDSS*,2014, avaialable at.

Dasgupta, D., Roy, A. and Nag, A. 2017, "Authentication Basics", *Advances in User Authentication*, Springer. pp. 1-36.

David, M. 2017, "Sharing: Post-Scarcity Beyond Capitalism?", *Cambridge Journal of Regions, Economy and Society*, Vol. 10 No. 2**,** pp. 311-325.

David, M., Kirton, A. and Millward, P. 2014, "Sports Television Broadcasting and the Challenge of Live-Streaming ", in: David, M. and Halbert, D. (eds.), *The Sage Handbook of Intellectual Property*, Sage. pp.

David, M. and Millward, P. 2012, "Football's Coming Home?: Digital Reterritorialization, Contradictions in the Transnational Coverage of Sport and the Sociology of Alternative Football Broadcasts", *The British journal of sociology*, Vol. 63 No. 2**,** pp. 349-369.

David, M. and Sutton, C. D. 2011, *Social Research: An Introduction*, Sage.

Davinson, N. and Sillence, E. 2010, "It Won't Happen to Me: Promoting Secure Behaviour among Internet Users", *Computers in Human Behavior*, Vol. 26 No. 6**,** pp. 1739-1747.

De Jesus, A. C. C., Júnior, M. E. G. and Brandão, W. C. (2018), "Exploiting Linkedin to Predict Employee Resignation Likelihood", paper presented at the *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*,2018, avaialable at.

Deevy, M., Lucich, S. and Beals, M. 2012, "Scams, Schemes and Swindles", *Financial Fraud Research Center*, Vol. No.

Dehue, F., Bolman, C. and Völlink, T. 2008, "Cyberbullying: Youngsters' Experiences and Parental Perception", *CyberPsychology & Behavior*, Vol. 11 No. 2**,** pp. 217-223.

Delongis, A. and Holtzman, S. 2005, "Coping in Context: The Role of Stress, Social Support, and Personality in Coping", *Journal of personality*, Vol. 73 No. 6**,** pp. 1633-1656.

Demetriou, C. and Silke, A. 2003, "A Criminological Internet 'Sting'. Experimental Evidence of Illegal and Deviant Visits to a Website Trap", *British Journal of Criminology*, Vol. 43 No. 1**,** pp. 213-222.

Denis, D. J. 2015, *Applied Univariate, Bivariate, and Multivariate Statistics*, John Wiley & Sons.

Denzin, N. K. 1978, *Sociological Methods: A Sourcebook*, McGraw-Hill Companies.

Denzin, N. K. and Lincoln, Y. S. 2017, *The Sage Handbook of Qualitative Research*, Sage.

Devarajan, R., Stolfo, S. J. and Bowen, B. M. 2012, "Measuring the Human Factor of Cyber Security", Vol. No.
Devers, K. J. and Frankel, R. M. 2000, "Study Design in Qualitative Research 2: Sampling and Data Collection Strategies", *Education for health*, Vol. 13 No. 2**,** pp. 263.
Dinev, T. and Hart, P. 2006, "An Extended Privacy Calculus Model for E-Commerce Transactions", *Information systems research*, Vol. 17 No. 1**,** pp. 61-80.
Dinisman, T. and Moroz, A. 2017, "Understanding Victims of Crime", Vol. No.
Ditton, J., Bannister, J., Gilchrist, E. and Farrall, S. 1999, "Afraid or Angry? Recalibrating the 'Fear'of Crime", *International review of Victimology*, Vol. 6 No. 2**,** pp. 83-99.
Dodel, M. and Mesch, G. 2017, "Cyber-Victimization Preventive Behavior: A Health Belief Model Approach", *Computers in Human Behavior*, Vol. 68 No. 359-367.
Dolliver, D. S. and Poorman, K. 2018, "Understanding Cybercrime", in: Reichel, P. L. and Randa, R. (eds.), *Transnational Crime and Global Security [2 Volumes]*, ABC-CLIO. pp. 139-160.
Donner, C. M., Marcum, C. D., Jennings, W. G., Higgins, G. E. and Banfield, J. 2014, "Low Self-Control and Cybercrime: Exploring the Utility of the General Theory of Crime Beyond Digital Piracy", *Computers in Human Behavior*, Vol. 34 No. 165-172.
Donovan, J. L., Rooshenas, L., Jepson, M., Elliott, D., Wade, J., Avery, K., Mills, N., Wilson, C., Paramasivan, S. and Blazeby, J. M. 2016, "Optimising Recruitment and Informed Consent in Randomised Controlled Trials: The Development and Implementation of the Quintet Recruitment Intervention (Qri)", *Trials*, Vol. 17 No. 1**,** pp. 283.
Doody, O. and Noonan, M. 2013, "Preparing and Conducting Interviews to Collect Data", *Nurse researcher*, Vol. 20 No. 5**,** pp.
Dowling, G. R. 1986, "Perceived Risk: The Concept and Its Measurement", *Psychology & Marketing*, Vol. 3 No. 3**,** pp. 193-210.
Downs, J. S., Holbrook, M. and Cranor, L. F. (2007), "Behavioral Response to Phishing Risk", paper presented at the *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*,2007, avaialable at.
Dörnyei, Z. 2007, *Research Methods in Applied Linguistics: Quantitative, Qualitative, and Mixed Methodologies*, Oxford University Press.
Dredge, R., Gleeson, J. and De La Piedad Garcia, X. 2014, "Cyberbullying in Social Networking Sites: An Adolescent Victim's Perspective", *Computers in Human Behavior*, Vol. 36 No. 13-20.
Driscoll, D. L., Appiah-Yeboah, A., Salib, P. and Rupert, D. J. 2007, "Merging Qualitative and Quantitative Data in Mixed Methods Research: How to and Why Not", Vol. No.
Du Preez, K. P., Landon, J., Bellringer, M., Garrett, N. and Abbott, M. 2016, "The Effects of Pop-up Harm Minimisation Messages on Electronic Gaming Machine Gambling Behaviour in New Zealand", *Journal of gambling studies*, Vol. 32 No. 4**,** pp. 1115-1126.
Duggan, M. and Smith, A. 2015, Cell Internet Use 2013. Pew Research Center.
Dunn, J. L. 2005, "Victims" and "Survivors": Emerging Vocabularies of Motive for "Battered Women Who Stay", *Sociological Inquiry*, Vol. 75 No. 1**,** pp. 1-30.
Dunn, J. L. 2008, "Accounting for Victimization: Social Constructionist Perspectives", *Sociology Compass*, Vol. 2 No. 5**,** pp. 1601-1620.
Durkin, M., Jennings, D., Mulholland, G. and Worthington, S. 2008, "Key Influencers and Inhibitors on Adoption of the Internet for Banking", *Journal of Retailing and Consumer Services*, Vol. 15 No. 5**,** pp. 348-357.
Dusabe, F. 2016, "Rwanda: Assessing the Effectiveness of Legal and Policy Responses to Fight Money Laundering", *Journal of Money Laundering Control*, Vol. 19 No. 1**,** pp. 21-31.
Dusek, G. A., Yurova, Y. V. and Ruppel, C. P. 2015, "Using Social Media and Targeted Snowball Sampling to Survey a Hard-to-Reach Population: A Case Study", *International Journal of Doctoral Studies*, Vol. 10 No. unknown**,** pp. 279-299.
Duxbury, P. 2016, "Gumtree Warns of Phishing Attacks. available at: http://www.mtawa.com.au/membership/member-communication/latest-news/item/2707-gumtree-warns-of-phishing-attacks.html (accessed 18/07/2108).
Dworkin, S. L. 2012, Sample Size Policy for Qualitative Studies Using in-Depth Interviews. Springer.
Dyck, I. 1997, "Dialogue with Difference: A Tale of Two Studies", *Thresholds in Feminist Geography*, Vol. No. 183-202.
Dytham, C. 2011, *Choosing and Using Statistics: A Biologist's Guide*, John Wiley & Sons.
Eastin, M. S. and Larose, R. 2000, "Internet Self-Efficacy and the Psychology of the Digital Divide", *Journal of computer-mediated communication*, Vol. 6 No. 1**,** pp. JCMC611.
Eaton, L. 1999, "As Swindlers Branch out, Victims Want to Be Heard", *The New York Times*, Vol. No.
Eck, J. 1995, "Examining Routine Activity Theory: A Review of Two Books", Vol. No.
Eck, J. 2003, "Police Problems: The Complexity of Problem Theory, Research and Evaluation", *Crime prevention studies*, Vol. 15 No. 79-114.

Eck, J. E. and Clarke, R. V. 2003, "Classifying Common Police Problems: A Routine Activity Approach", *Crime prevention studies*, Vol. 16 No. 7-40.
Eck, J. E., Gersh, J. S. and Taylor, C. 2000, "Finding Crime Hot Spots through Repeat Address Mapping", *Analyzing crime patterns: Frontiers of practice*, Vol. No. 49-64.
Edwards, R. and Holland, J. 2013, *What Is Qualitative Interviewing?*, A&C Black.
Eigenberg, H. and Garland, T. 2008, "Victim Blaming", in: Moriarty, L. J. (ed.) *Controversies in Victimology*, 2nd ed, Routledge. pp. 33-48.
Eisend, M. 2004, "Is It Still Worth to Be Credible? A Meta-Analysis of Temporal Patterns of Source Credibility Effects in Marketing", *ACR North American Advances*, Vol. No.
El-Din, R. S., Cairns, P. and Clark, J. 2014, "Mobile Users' Strategies for Managing Phishing Attacks", *Journal of Management and Strategy*, Vol. 5 No. 2**,** pp. 70.
Elhai, J. D., Chai, S., Amialchuk, A. and Hall, B. J. 2017, "Cross-Cultural and Gender Associations with Anxiety About Electronic Data Hacking", *Computers in Human Behavior*, Vol. 70 No. 161-167.
Emmel, N. 2013, *Sampling and Choosing Cases in Qualitative Research: A Realist Approach*, Sage.
Ena, M. 2008, "Securing Online Transactions: Crime Prevention Is the Key", *Fordham Urb. LJ*, Vol. 35 No. 147-149.
Engel, B. and Keen, A. 1994, "A Simple Approach for the Analysis of Generalizea Linear Mixed Models", *Statistica neerlandica*, Vol. 48 No. 1**,** pp. 1-22.
Etzioni, A. 2017, "Cyber Trust", *Journal of Business Ethics*, Vol. No. 1-13.
European Commission. 2007, "Towards a General Policy on the Fight against Cyber Crime ", available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF (accessed.
European Commission Report. 2015, "Cyber Security Report", available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf (accessed 13/10/2016).
Eurostat. 2016, "E-Commerce Statistics for Individuals. available at: http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals (accessed 27/11/2017).
Evuleocha, S. U. and Ugbah, S. D. 2018, "Profiling: The Efficacy of Using Social Networking Sites for Job Screening", *Journal of Employment Counseling*, Vol. 55 No. 2**,** pp. 48-57.
Fajczak-Kowalska, A. and Kowalska, M. 2017, "Meaning and the Role of the M-Commerce in the 21st Century", *Przedsiębiorczość i Zarządzanie*, Vol. 18 No. 4, cz. 2 Agile Commerce-technologie przyszłości**,** pp. 157-166.
Fang, Q.-P., Hu, Y.-J., Wang, S.-H. and Gu, W. (2016), "A Security Analysis of Wireless Network", paper presented at the *WIRELESS COMMUNICATION AND NETWORK: Proceedings of 2015 International Workshop on Wireless Communication and Network (IWWCN2015)*,2016, avaialable at.
Farrall, S. and Gadd, D. 2004, "Evaluating Crime Fears a Research Note on a Pilot Study to Improve the Measurement of the 'Fear of Crime'as a Performance Indicator", *Evaluation*, Vol. 10 No. 4**,** pp. 493-502.
Farrall, S., Jackson, J. and Gray, E. 2006, "Everyday Emotion and the Fear of Crime: Preliminary Findings from Experience and Expression", Vol. No.
Farrell, G. and Sousa, W. 2001, "Repeat Victimization and Hot Spots: The Overlap and Its Implications for Crime Control and Problem-Orientated Policing", Vol. No.
Farrington, D. P. 1991, "Longitudinal Research Strategies: Advantages, Problems, and Prospects", *Journal of the American Academy of Child & Adolescent Psychiatry*, Vol. 30 No. 3**,** pp. 369-374.
Farrington, D. P. 2006, "Key Longitudinal-Experimental Studies in Criminology", *Journal of Experimental Criminology*, Vol. 2 No. 2**,** pp. 121-141.
Fasick, F. A. 1977, "Some Uses of Untranscribed Tape Recordings in Survey Research", *Public Opinion Quarterly*, Vol. No. 549-552.
Fattah, E. A. 1979, "Some Recent Theoretical Developments in Victimology", *Victimology*, Vol. 4 No. 2**,** pp. 198-213.
Fattah, E. A. 2003, "Violence against the Socially Expendable", *International Handbook of Violence Research*, Springer. pp. 767-783.
Felson, M. and Clarke, R. V. 1998, "Opportunity Makes the Thief", *Police research series, paper*, Vol. 98 No.
Felson, M. and Cohen, L. E. 1980, "Human Ecology and Crime: A Routine Activity Approach", *Human Ecology*, Vol. 8 No. 4**,** pp. 389-406.
Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E. and Wagner, D. (2012), "Android Permissions: User Attention, Comprehension, and Behavior", paper presented at the *Proceedings of the Eighth Symposium on Usable Privacy and Security*,2012, avaialable at.
Fenner, Y., Garland, S. M., Moore, E. E., Jayasinghe, Y., Fletcher, A., Tabrizi, S. N., Gunasekaran, B. and Wark, J. D. 2012, "Web-Based Recruiting for Health Research Using a Social Networking Site: An Exploratory Study", *Journal of medical Internet research*, Vol. 14 No. 1**,** pp.
Ferraro, K. F. 1995, *Fear of Crime: Interpreting Victimization Risk*, SUNY press.

Ferraro, K. F. 1996, "Women's Fear of Victimization: Shadow of Sexual Assault?", *Social forces*, Vol. 75 No. 2**,** pp. 667-690.
Ferraro, K. F. and Grange, R. L. 1987, "The Measurement of Fear of Crime", *Sociological inquiry*, Vol. 57 No. 1**,** pp. 70-97.
Ferreira, A., Coventry, L. and Lenzini, G. (2015), "Principles of Persuasion in Social Engineering and Their Use in Phishing", paper presented at the *International Conference on Human Aspects of Information Security, Privacy, and Trust*,2015, avaialable at.
Ferreira, A. and Lenzini, G. (2015), "An Analysis of Social Engineering Principles in Effective Phishing", paper presented at the *Socio-Technical Aspects in Security and Trust (STAST), 2015 Workshop on*,2015, avaialable at.
Field, A. 2009, *Discovering Statistics Using Spss*, Sage publications.
Fife, E. and Orjuela, J. 2012, "The Privacy Calculus: Mobile Apps and User Perceptions of Privacy and Security", *International Journal of Engineering Business Management*, Vol. 4 No. Godište 2012**,** pp. 4-11.
Finch, E. and Munro, V. E. 2005, "Juror Stereotypes and Blame Attribution in Rape Cases Involving Intoxicants the Findings of a Pilot Study", *British Journal of Criminology*, Vol. 45 No. 1**,** pp. 25-38.
Finkelhor, D. and Asdigian, N. L. 1996, "Risk Factors for Youth Victimization: Beyond a Lifestyles/Routine Activities Theory Approach", *Violence and victims*, Vol. 11 No. 3-20.
Finlay, L. 1998, "Reflexivity: An Essential Component for All Research?", *British Journal of Occupational Therapy*, Vol. 61 No. 10**,** pp. 453-456.
Finlay, L. 2002, "Negotiating the Swamp: The Opportunity and Challenge of Reflexivity in Research Practice", *Qualitative research*, Vol. 2 No. 2**,** pp. 209-230.
Finn, J. 2004, "A Survey of Online Harassment at a University Campus", *Journal of Interpersonal violence*, Vol. 19 No. 4**,** pp. 468-483.
Finset, A., Steine, S., Haugli, L., Steen, E. and Laerum, E. 2002, "The Brief Approach/Avoidance Coping Questionnaire: Development and Validation", *Psychology, health & medicine*, Vol. 7 No. 1**,** pp. 75-85.
Fireeye. 2018, "Spear-Phishing Attacks Why They Are Successful and How to Stop Them", available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/products/pdfs/wp-fireeye-how-stop-spearphishing.pdf (accessed 05/09/2018).
Fisher, B. S., Daigle, L. E. and Cullen, F. T. 2010, "What Distinguishes Single from Recurrent Sexual Victims? The Role of Lifestyle-Routine Activities and First-Incident Characteristics", *Justice Quarterly*, Vol. 27 No. 1**,** pp. 102-129.
Fisher, B. S. and Reyns, B. 2009, "Victimization", in: Miller, J. M. (ed.) *21st Century Criminology: A Reference Handbook*, Sage. pp.
Fisher, B. S. and Sloan, J. J. 2003, "Unraveling the Fear of Victimization among College Women: Is the "Shadow of Sexual Assault Hypothesis" Supported?", *Justice Quarterly*, Vol. 20 No. 3**,** pp. 633-659.
Fitzgerald, J. and Fitzgerald, J. 2013, *Statistics for Criminal Justice and Criminology in Practice and Research: An Introduction*, Sage.
Flick, U. 1992, "Triangulation Revisited: Strategy of Validation or Alternative?", *Journal for the theory of social behaviour*, Vol. 22 No. 2**,** pp. 175-197.
Flick, U. 2008, *Designing Qualitative Research*, Sage.
Floyd, D. L., Prentice-Dunn, S. and Rogers, R. W. 2000, "A Meta-Analysis of Research on Protection Motivation Theory", *Journal of applied social psychology*, Vol. 30 No. 2**,** pp. 407-429.
Forsythe, S., Liu, C., Shannon, D. and Gardner, L. C. 2006, "Development of a Scale to Measure the Perceived Benefits and Risks of Online Shopping", *Journal of interactive marketing*, Vol. 20 No. 2**,** pp. 55-75.
Franklin, C. A. and Franklin, T. W. 2009, "Predicting Fear of Crime: Considering Differences across Gender", *Feminist Criminology*, Vol. 4 No. 1**,** pp. 83-106.
Franks, M. A. 2011, "Sexual Harassment 2.0", *Md. L. Rev.*, Vol. 71 No. 655.
Frieze, I. H. and Bookwala, J. 1996, "Coping with Unusual Stressors: Criminal Victimization", Vol. No.
Frijda, N. H. 1988, "The Laws of Emotion", *American psychologist*, Vol. 43 No. 5**,** pp. 349.
Frost, N. 2009, "Do You Know What I Mean?': The Use of a Pluralistic Narrative Analysis Approach in the Interpretation of an Interview", *Qualitative Research*, Vol. 9 No. 1**,** pp. 9-29.
Furstenberg, F. (1972), "Fear of Crime and Its Effects on Citizen Behavior", paper presented at the *Crime and justice: a symposium. New York: Nailburg*,1972, avaialable at.
Furstenberg, F. F. 1971, "Public Reaction to Crime in the Streets", *The American Scholar*, Vol. 40 No. 4**,** pp. 601-610.
Gale, J.-A. and Coupe, T. 2005, "The Behavioural, Emotional and Psychological Effects of Street Robbery on Victims", *International Review of Victimology*, Vol. 12 No. 1**,** pp. 1-22.
Galea, S. and Tracy, M. 2007, "Participation Rates in Epidemiologic Studies", *Annals of epidemiology*, Vol. 17 No. 9**,** pp. 643-653.

Ganzini, L., Mcfarland, B. and Bloom, J. 1990, "Victims of Fraud: Comparing Victims of White Collar and Violent Crime", *Journal of the American Academy of Psychiatry and the Law Online*, Vol. 18 No. 1**,** pp. 55-63.
Garg, V. and Nilizadeh, S. (2013), "Craigslist Scams and Community Composition: Investigating Online Fraud Victimization", paper presented at the *Security and Privacy Workshops (SPW), 2013 IEEE*,2013, avaialable at.
Garofalo, J. 1981, "The Fear of Crime: Causes and Consequences", *The Journal of Criminal Law and Criminology (1973-)*, Vol. 72 No. 2**,** pp. 839-857.
Garofalo, J. 1986, "Lifestyles and Victimization: An Update", *From Crime Policy to Victim Policy*, Springer. pp. 135-155.
Garton, S. 2014. *An Investigation into the Effects of Extra-Curricular Activity on the Social Developments of Children with Special Educational Needs.* Cardiff Metropolitan University.
Gercke, M. 2012, *Understanding Cybercrimes: Phenomena, Challenges and Legal Response*, International Telecommunication Union.
Gerrish, K. and Lacey, A. 2010, *The Research Process in Nursing*, John Wiley & Sons.
Ghosh, A. K. and Swaminatha, T. M. 2001, "Software Security and Privacy Risks in Mobile E-Commerce", *Communications of the ACM*, Vol. 44 No. 2**,** pp. 51-57.
Ghouzali, S., Lafkih, M., Abdul, W., Mikram, M., El Haziti, M. and Aboutajdine, D. 2016, "Trace Attack against Biometric Mobile Applications", *Mobile Information Systems*, Vol. 2016 No.
Ginley, M. K., Whelan, J. P., Pfund, R. A., Peter, S. C. and Meyers, A. W. 2017, "Warning Messages for Electronic Gambling Machines: Evidence for Regulatory Policies", *Addiction Research & Theory*, Vol. 25 No. 6**,** pp. 495-504.
Given, L. M. 2008, *The Sage Encyclopedia of Qualitative Research Methods*, Sage Publications.
Globalsign. 2017, "How to Spot a Phishing Website. available at: https://www.globalsign.com/en/blog/how-to-spot-a-fake-website/ (accessed 10/10/2018).
Goel, S., Williams, K. and Dincelli, E. 2017, "Got Phished? Internet Security and Human Vulnerability", *Journal of the Association for Information Systems*, Vol. 18 No. 1**,** pp. 22.
Golafshani, N. 2003, "Understanding Reliability and Validity in Qualitative Research", *The qualitative report*, Vol. 8 No. 4**,** pp. 597-606.
Gold, S. 2012, "Wireless Cracking: There's an App for That", *Network Security*, Vol. 2012 No. 5**,** pp. 10-14.
Goldsborough, R. 2017, "Get It for Free over the Internet", *Tech Directions*, Vol. 76 No. 8**,** pp. 12.
Goldsmith, A. and Brewer, R. 2015, "Digital Drift and the Criminal Interaction Order", *Theoretical Criminology*, Vol. 19 No. 1**,** pp. 112-130.
Goode, E. 2015, "The Sociology of Deviance: An Introduction", in: Goode, E. (ed.) *The Handbook of Deviance*, John Wiley & Sons. pp.
Goodman, L. A. 2011, "Comment: On Respondent-Driven Sampling and Snowball Sampling in Hard-to-Reach Populations and Snowball Sampling Not in Hard-to-Reach Populations", *Sociological Methodology*, Vol. 41 No. 1**,** pp. 347-353.
Goodwin, J. 2012, *Sage Secondary Data Analysis*, Sage.
Gordon, R. A. 2012, *Applied Statistics for the Social and Health Sciences*, Routledge.
Gordon, S. and Ford, R. 2006, "On the Definition and Classification of Cybercrime", *Journal in Computer Virology*, Vol. 2 No. 1**,** pp. 13-20.
Gottfredson, M. R. and Hirschi, T. 1990, *A General Theory of Crime*, Stanford University Press.
Goucher, W. 2010, "Being a Cybercrime Victim", *Computer Fraud & Security*, Vol. 2010 No. 10**,** pp. 16-18.
Grabher, G. and König, J. 2017, "Performing Network Theory? Reflexive Relationship Management on Social Network Sites", *Networked Governance*, Springer. pp. 121-140.
Grabosky, P. and Smith, R. 2001, "Telecommunications Fraud in the Digital Age: The Convergence of Technologies", in: Wall, D. (ed.) *Crime and the Internet*, Routledge, London. pp. 23-43.
Grabosky, P. N. 2001, "Virtual Criminality: Old Wine in New Bottles?", *Social and Legal Studies*, Vol. 10 No. 2**,** pp. 243-250.
Granger, S. 2001, "Social Engineering Fundamentals, Part I: Hacker Tactics", *Security Focus, December*, Vol. 18 No.
Grant, J. 2014, "Reflexivity: Interviewing Women and Men Formerly Addicted to Drugs and/or Alcohol", *The qualitative report*, Vol. 19 No. 38**,** pp. 1-15.
Green, D. L. and Pomeroy, E. 2007, "Crime Victimization: Assessing Differences between Violent and Nonviolent Experiences", *Victims and Offenders*, Vol. 2 No. 1**,** pp. 63-76.
Greene, J. 2008, "Is Mixed Methods Social Inquiry a Distinctive Methodology?", *Journal of Mixed Methods Research*, Vol. 2 No. 1**,** pp. 7-22.
Greene, J. C., Caracelli, V. J. and Graham, W. F. 1989, "Toward a Conceptual Framework for Mixed-Method Evaluation Designs", *Educational evaluation and policy analysis*, Vol. 11 No. 3**,** pp. 255-274.

Greene, T. 2015, "Biggest Data Breaches of 2015", *Network World*, Vol. 2015 No. 1-6.
Grégio, A., Bonacin, R., Nabuco, O., Afonso, V. M., De Geus, P. L. and Jino, M. (2014), "Ontology for Malware Behavior: A Core Model Proposal", paper presented at the *2014 IEEE 23rd International WETICE Conference*,2014, avaialable at.
Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D. and Cowley, J. (2014), "Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits", paper presented at the *Security and Privacy Workshops (SPW), 2014 IEEE*,2014, avaialable at.
Greve, W., Leipold, B. and Kappes, C. 2017, "Fear of Crime in Old Age: A Sample Case of Resilience?", *The Journals of Gerontology: Series B*, Vol. No. gbw169.
Grubb, J. A. and Bouffard, L. A. 2015, "The Influence of Direct and Indirect Juvenile Victimization Experiences on Adult Victimization and Fear of Crime", *Journal of interpersonal violence*, Vol. 30 No. 18**,** pp. 3151-3173.
Guba, E. G. 1981, "Criteria for Assessing the Trustworthiness of Naturalistic Inquiries", *Ectj*, Vol. 29 No. 2**,** pp. 75.
Guest, G. and Macqueen, K. M. 2008, *Handbook for Team-Based Qualitative Research*, Rowman Altamira.
Guest, G., Namey, E. E. and Mitchell, M. L. 2012, *Collecting Qualitative Data: A Field Manual for Applied Research*, Sage.
Gull, J. and Flowers, T. 2016, "Prosecuting Copyright Infringement Cases and Emerging Issues", *US Att'ys Bull.*, Vol. 64 No. 18.
Guo, Y. and Zhang, C. 2015, "Legal Risks and Solutions to E-Marketers' Data Mining", *Research on Selected China's Legal Issues of E-Business*, Springer. pp. 23-32.
Gupta, A. 2017, "The Evolution of Fraud: Ethical Implications in the Age of Large-Scale Data Breaches and Widespread Artificial Intelligence Solutions Deployment", Vol. No.
Gupta, B. B., Tewari, A., Jain, A. K. and Agrawal, D. P. 2017, "Fighting against Phishing Attacks: State of the Art and Future Challenges", *Neural Computing and Applications*, Vol. 28 No. 12**,** pp. 3629-3654.
Gutt, T. A. and Randa, R. 2016, "The Influence of an Empathetic Adult on the Relationship between Bullying Victimization and Fear at School", *Journal of crime and justice*, Vol. 39 No. 2**,** pp. 282-302.
Guy, R. S. and Lownes-Jackson, M. 2010, "An Examination of Students' Self-Efficacy Beliefs and Demonstrated Computer Skills", *Issues in Informing Science and Information Technology*, Vol. 7 No. 1**,** pp. 285-295.
H. Akhter, S. 2014, "Privacy Concern and Online Transactions: The Impact of Internet Self-Efficacy and Internet Involvement", *Journal of Consumer Marketing*, Vol. 31 No. 2**,** pp. 118-125.
Haelterman, H. 2016, *Crime Script Analysis: Preventing Crimes against Business*, Springer.
Halcomb, E. J. and Davidson, P. M. 2006, "Is Verbatim Transcription of Interview Data Always Necessary?", *Applied Nursing Research*, Vol. 19 No. 1**,** pp. 38-42.
Hale, C. 1996, "Fear of Crime: A Review of the Literature", *International review of Victimology*, Vol. 4 No. 2**,** pp. 79-150.
Halevi, T., Lewis, J. and Memon, N. 2013a, "Phishing, Personality Traits and Facebook", *arXiv preprint arXiv:1301.7643*, Vol. No.
Halevi, T., Lewis, J. and Memon, N. (2013b), "A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits", paper presented at the *Proceedings of the 22nd International Conference on World Wide Web*,2013b, avaialable at.
Halevi, T., Memon, N. and Nov, O. 2015, "Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks", Vol. No.
Haley, W. E., Levine, E. G., Brown, S. L. and Bartolucci, A. A. 1987, "Stress, Appraisal, Coping, and Social Support as Predictors of Adaptational Outcome among Dementia Caregivers", *Psychology and aging*, Vol. 2 No. 4**,** pp. 323.
Halgas, Z. 2016, "Scareware: Advanced Topics in Computer Security", Vol. No.
Hall, N. and Hall, R. 2008, *Applied Social Research*, Macmillan Education AU.
Hammersley, M. and Atkinson, P. 1995, "Ethnography: Practices and Principles", *New York: Routledge. Retrieved December*, Vol. 2 No. 2008.
Hammersley, M. and Atkinson, P. 2007, *Ethnography: Principles in Practice*, Routledge.
Hanson, W. E., Creswell, J. W., Clark, V. L. P., Petska, K. S. and Creswell, J. D. 2005, "Mixed Methods Research Designs in Counseling Psychology", *Journal of counseling psychology*, Vol. 52 No. 2**,** pp. 224.
Harris, A., Parke, A. and Griffiths, M. D. 2018, "The Case for Using Personally Relevant and Emotionally Stimulating Gambling Messages as a Gambling Harm-Minimisation Strategy", *International journal of mental health and addiction*, Vol. 16 No. 2**,** pp. 266-275.
Harrison, B., Svetieva, E. and Vishwanath, A. 2016, "Individual Processing of Phishing Emails: How Attention and Elaboration Protect against Phishing", *Online Information Review*, Vol. 40 No. 2**,** pp. 265-281.
Harvey, S., Kerr, J., Keeble, J. and Nicholls, C. M. 2014, "Understanding Victims of Financial Crime", Vol. No.

Haselhoff, V., Faupel, U. and H. Holzmüller, H. 2014, "Strategies of Children and Parents During Shopping for Groceries", *Young Consumers*, Vol. 15 No. 1**,** pp. 17-36.
Haslam, K. 2017. *Do Macs Get Viruses, and Do Macs Need Antivirus Software? Macworld* [Online]. Available from: http://www.macworld.co.uk/how-to/mac-software/do-macs-get-viruses-do-macs-need-antivirus-software-3454926/ [Accessed 25/07/2017 2017].
Hawthorn, D. 2007, "Interface Design and Engagement with Older People", *Behaviour & Information Technology*, Vol. 26 No. 4**,** pp. 333-341.
He, D., Chan, S. and Guizani, M. 2015, "Mobile Application Security: Malware Threats and Defenses", *IEEE Wireless Communications*, Vol. 22 No. 1**,** pp. 138-144.
Healey, J. F. 2014, *Statistics: A Tool for Social Research*, Wadsworth Publishing Company, Belmont, CA.
Heartfield, R., Loukas, G. and Gan, D. 2016, "You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks", *IEEE Access*, Vol. 4 No. 6910-6928.
Heath, L. and Gilbert, K. 1996, "Mass Media and Fear of Crime", *American Behavioral Scientist*, Vol. 39 No. 4**,** pp. 379-386.
Henson, B. 2011. *Fear of Crime Online: Examining the Effects of Online Victimization and Perceived Risk on Fear of Cyberstalking Victimization.* University of Cincinnati.
Henson, B. and Reyns, B. W. 2015, "The Only Thing We Have to Fear Is Fear Itself… and Crime: The Current State of the Fear of Crime Literature and Where It Should Go Next", *Sociology Compass*, Vol. 9 No. 2**,** pp. 91-103.
Henson, B., Reyns, B. W. and Fisher, B. S. 2013, "Fear of Crime Online? Examining the Effect of Risk, Previous Victimization, and Exposure on Fear of Online Interpersonal Victimization", *Journal of Contemporary Criminal Justice*, Vol. 29 No. 4**,** pp. 475-497.
Herman-Stabl, M. A., Stemmler, M. and Petersen, A. C. 1995, "Approach and Avoidant Coping: Implications for Adolescent Mental Health", *Journal of Youth and Adolescence*, Vol. 24 No. 6**,** pp. 649-665.
Hernandez-Castro, J. and Boiten, E. 2014, "Cybercrime Prevalence and Impact in the Uk", *Computer Fraud & Security*, Vol. 2014 No. 2**,** pp. 5-8.
Hesse-Biber, S. N. and Johnson, R. B. 2015, *The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry*, Oxford University Press.
Higgins, G. E., Ricketts, M. L. and Vegh, D. T. 2008, "The Role of Self-Control in College Student's Perceived Risk and Fear of Online Victimization", *American Journal of Criminal Justice*, Vol. 33 No. 2**,** pp. 223.
Higgins, G. E. and Wolfe, S. E. 2009, "Cybercrime", in: Miller, J. M. (ed.) *21st Century Criminology: A Reference Handbook*, SAGE. pp. 466-471.
Hill, S. 2015. *Can Macs Get Viruses and Malware? We Ask an Expert*. *Digital Trends* [Online]. Available from: https://www.digitaltrends.com/computing/can-macs-get-viruses/ 2017].
Hille, P., Walsh, G. and Cleveland, M. 2015, "Consumer Fear of Online Identity Theft: Scale Development and Validation", *Journal of Interactive Marketing*, Vol. 30 No. 1-19.
Hills, S. L. 1977, "The Mystification of Social Deviance", *Crime & Delinquency*, Vol. 23 No. 4**,** pp. 417-426.
Hindelang, M. J., Gottfredson, M. R. and Garofalo, J. 1978, *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*, Ballinger Cambridge, MA.
Hjortdal, M. 2011, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence", *Journal of Strategic Security*, Vol. 4 No. 2**,** pp. 2.
Ho, C.-T. B. and Lin, W.-C. 2010, "Measuring the Service Quality of Internet Banking: Scale Development and Validation", *European Business Review*, Vol. 22 No. 1**,** pp. 5-24.
Ho, R. 2013, *Handbook of Univariate and Multivariate Data Analysis with Ibm Spss*, CRC Press.
Hoffman, C. 2014, "Why Using a Public Wi-Fi Network Can Be Dangerous, Even When Accessing Encrypted Websites. available at: https://www.howtogeek.com/178696/why-using-a-public-wi-fi-network-can-be-dangerous-even-when-accessing-encrypted-websites/.
Hoffmann, E. A. 2007, "Open-Ended Interviews, Power, and Emotional Labor", *Journal of contemporary ethnography*, Vol. 36 No. 3**,** pp. 318-346.
Holahan, C. J. and Moos, R. H. 1987, "Personal and Contextual Determinants of Coping Strategies", *Journal of personality and social psychology*, Vol. 52 No. 5**,** pp. 946.
Hollway, W. and Jefferson, T. 1997, "The Risk Society in an Age of Anxiety: Situating Fear of Crime", *British journal of sociology*, Vol. No. 255-266.
Holstein, J. A. and Miller, G. 1990, "Rethinking Victimization: An Interactional Approach to Victimology", *Symbolic Interaction*, Vol. 13 No. 1**,** pp. 103-122.
Holt, T. J. 2007, "Subcultural Evolution? Examining the Influence of on-and Off-Line Experiences on Deviant Subcultures", *Deviant Behavior*, Vol. 28 No. 2**,** pp. 171-198.
Holt, T. J. 2013, "Examining the Forces Shaping Cybercrime Markets Online", *Social Science Computer Review*, Vol. 31 No. 2**,** pp. 165-177.

Holt, T. J. and Bossler, A. 2016, *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*, Routledge.
Holt, T. J. and Bossler, A. M. 2008, "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization", *Deviant Behavior*, Vol. 30 No. 1**,** pp. 1-25.
Holt, T. J. and Bossler, A. M. 2013, "Examining the Relationship between Routine Activities and Malware Infection Indicators", *Journal of Contemporary Criminal Justice*, Vol. 29 No. 4**,** pp. 420-436
Holt, T. J. and Bossler, A. M. 2014, "An Assessment of the Current State of Cybercrime Scholarship", *Deviant Behavior*, Vol. 35 No. 1**,** pp. 20-40.
Holt, T. J. and Copes, H. 2010, "Transferring Subcultural Knowledge on-Line: Practices and Beliefs of Persistent Digital Pirates", *Deviant Behavior*, Vol. 31 No. 7**,** pp. 625-654.
Holt, T. J. and Turner, M. G. 2012, "Examining Risks and Protective Factors of on-Line Identity Theft", *Deviant Behavior*, Vol. 33 No. 4**,** pp. 308-323.
Holtfreter, K., Reisig, M. and Pratt, T. 2008, "Low Self-Control, Routine Activities, and Fraud Victimization", *Criminology*, Vol. 46 No. 1**,** pp. 189-220.
Holtfreter, K., Reisig, M. D. and Blomberg, T. G. 2005, "Consumer Fraud Victimization in Florida: An Empirical Study", . *Thomas L. Rev.*, Vol. 18 No. 761.
Holtfreter, K., Reisig, M. D., Leeper Piquero, N. and Piquero, A. R. 2010, "Low Self-Control and Fraud: Offending, Victimization, and Their Overlap", *Criminal Justice and Behavior*, Vol. 37 No. 2**,** pp. 188-203.
Holton, M. K., Barry, A. E. and Chaney, J. D. 2016, "Employee Stress Management: An Examination of Adaptive and Maladaptive Coping Strategies on Employee Health", *Work*, Vol. 53 No. 2**,** pp. 299-305.
Homant, R. J. 2010, "Risky Altruism as a Predictor of Criminal Victimization", *Criminal Justice and Behavior*, Vol. 37 No. 11**,** pp. 1195-1216.
Hope, T. 2012, "Theory and Method: The Social Epidemiology of Crime Victims", *Handbook of Victims and Victimology*, Willan. pp. 78-106.
Horn, J. V., Eisenberg, M., Nicholls, C. M., Mulder, J., Webster, S., Paskell, C., Brown, A., Stam, J., Kerr, J. and Jago, N. 2015, "Stop It Now! A Pilot Study into the Limits and Benefits of a Free Helpline Preventing Child Sexual Abuse", *Journal of child sexual abuse*, Vol. 24 No. 8**,** pp. 853-872.
House, D. 2013, "An Assessment of User Response to Phishing Attacks: The Effects of Fear and Self-Confidence", Vol. No.
Howard, L., De Salis, I., Tomlin, Z., Thornicroft, G. and Donovan, J. 2009, "Why Is Recruitment to Trials Difficult? An Investigation into Recruitment Difficulties in an Rct of Supported Employment in Patients with Severe Mental Illness", *Contemporary Clinical Trials*, Vol. 30 No. 1**,** pp. 40-46.
Howe, A. E., Ray, I., Roberts, M., Urbanska, M. and Byrne, Z. (2012), "The Psychology of Security for the Home Computer User", paper presented at the *2012 IEEE Symposium on Security and Privacy*,2012, avaialable at.
Hox, J. J. and Boeije, H. R. 2005, "Data Collection, Primary Versus Secondary", Vol. No.
Hsieh, H.-F. and Shannon, S. E. 2005, "Three Approaches to Qualitative Content Analysis", *Qualitative health research*, Vol. 15 No. 9**,** pp. 1277-1288.
Hsu, M.-H. and Chiu, C.-M. 2004, "Internet Self-Efficacy and Electronic Service Acceptance", *Decision support systems*, Vol. 38 No. 3**,** pp. 369-381.
Hu, Y., Wang, D., Pang, K., Xu, G. and Guo, J. 2015, "The Effect of Emotion and Time Pressure on Risk Decision-Making", *Journal of Risk Research*, Vol. 18 No. 5**,** pp. 637-650.
Huang, J., Zhou, J., Liao, G., Mo, F. and Wang, H. 2017, "Investigation of Chinese Students' O2o Shopping through Multiple Devices", *Computers in Human Behavior*, Vol. 75 No. 58-69.
Huber, M., Mulazzani, M. and Weippl, E. (2010), "Who on Earth Is "Mr. Cypher": Automated Friend Injection Attacks on Social Networking Sites", paper presented at the *IFIP International Information Security Conference*,2010, avaialable at.
Hussain, D., Ross, P. and Bednar, P. 2018, "The Perception of the Benefits and Drawbacks of Internet Usage by the Elderly People", *Digital Technology and Organizational Change*, Springer. pp. 199-212.
Hutchings, A. 2013, "Hacking and Fraud: Qualitative Analysis of Online Offending and Victimization", in: Jaishankar, K. and Ronel, N. (eds.), *Global Criminology: Crime and Victimization in the Globalized Era*. pp. 93-114.
Hutchings, A. and Hayes, H. 2008, "Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the Net", *Current Issues Crim. Just.*, Vol. 20 No. 433.
Hutchings, A. and Holt, T. J. 2015, "A Crime Script Analysis of the Online Stolen Data Market", *British Journal of Criminology*, Vol. 55 No. 3**,** pp. 596-614.
Ifinedo, P. 2012, "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory", *Computers & Security*, Vol. 31 No. 1**,** pp. 83-95.

Iovan, S. and Dinu, M. B. 2014, "Impact of the Loss and Theft of Electronic Data on Companies", *Fiability & Durability/Fiabilitate si Durabilitate*, Vol. No. 1**,** pp.
Ipsos Mediact, G. 2012, "Mobile Internet and Smartphone Adoption", *Google Mobile Ads Blog*, Vol. No.
Ivankova, N., Creswell, J. and Stick, S. 2006, "Using Mixed-Methods Sequential Explanatory Design: From Theory to Practice", *Field methods*, Vol. 18 No. 1**,** pp. 3-20.
Ivankova, N. V. 2014, *Mixed Methods Applications in Action Research*, Sage.
Jackson, S. L. 2013, *Statistics Plain and Simple*, Cengage Learning.
Jain, A. K. and Gupta, B. B. 2017, "Phishing Detection: Analysis of Visual Similarity Based Approaches", *Security and Communication Networks*, Vol. 2017 No.
Jain, A. K. and Shanbhag, D. 2012, "Addressing Security and Privacy Risks in Mobile Applications", *IT Professional*, Vol. 14 No. 5**,** pp. 28-33.
Jain, P., Gyanchandani, M. and Khare, N. 2016, "Big Data Privacy: A Technological Perspective and Review", *Journal of Big Data*, Vol. 3 No. 1**,** pp. 25.
Jaishankar, K. 2007, "Establishing a Theory of Cyber Crimes", *International Journal of Cyber Criminology*, Vol. 1 No. 2**,** pp. 7-9.
Jaishankar, K. 2008, "Identity Related Crime in the Cyberspace: Examining Phishing and Its Impact", *International Journal of Cyber Criminology*, Vol. 2 No. 1**,** pp. 10.
Jansen, B. J., Sobel, K. and Cook, G. 2011, "Classifying Ecommerce Information Sharing Behaviour by Youths on Social Networking Sites", *Journal of Information Science*, Vol. 37 No. 2**,** pp. 120-136.
Jansen, J. (2015), "Studying Safe Online Banking Behaviour: A Protection Motivation Theory Approach", paper presented at the *HAISA*,2015, avaialable at.
Jansen, J. and Leukfeldt, R. (2015), "How People Help Fraudsters Steal Their Money: An Analysis of 600 Online Banking Fraud Cases", paper presented at the *Socio-Technical Aspects in Security and Trust (STAST), 2015 Workshop on*,2015, avaialable at.
Jansen, J. and Leukfeldt, R. 2016, "Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization", *International Journal of Cyber Criminology*, Vol. 10 No. 1**,** pp. 79-91.
Jansen, J. and Van Schaik, P. (2016), "Understanding Precautionary Online Behavioural Intentions: A Comparison of Three Models", paper presented at the *HAISA*,2016, avaialable at.
Jansen, J. and Van Schaik, P. 2018, "Persuading End Users to Act Cautiously Online: A Fear Appeals Study on Phishing", *Information & Computer Security*, Vol. No. just-accepted**,** pp. 00-00.
Jansson, K. 2007, "British Crime Survey: Measuring Crime over 25 Years", London: Home Office, available at: http://pgil.pk/wp-content/uploads/2014/04/British-measuring-Crime-for-Last-25-years.pdf (accessed 01/02/2016).
Jayapratha, C. and Gnanasekar, J. 2018, "Threat Detection and Defence Mechanism in Criminology Using Data Mining", Vol. No.
Jefford, E., Fahy, K. and Sundin, D. 2011, "Decision-Making Theories and Their Usefulness to the Midwifery Profession Both in Terms of Midwifery Practice and the Education of Midwives", *International Journal of Nursing Practice*, Vol. 17 No. 3**,** pp. 246-253.
Jennings, W. G., Gover, A. R. and Pudrzynska, D. 2007, "Are Institutions of Higher Learning Safe? A Descriptive Study of Campus Safety Issues and Self-Reported Campus Victimization among Male and Female College Students", *Journal of criminal justice education*, Vol. 18 No. 2**,** pp. 191-208.
Jewkes, Y. 2009, "Public Policing and the Internet", in: Jewkes, Y. and Yar, M. (eds.), *Handbook of Internet Crime*, Routledge. pp.
Johnson, B. and Turner, L. A. 2003, "Data Collection Strategies in Mixed Methods Research", *Handbook of mixed methods in social and behavioral research*, Vol. No. 297-319.
Johnson, K. J., Mueller, N. L., Williams, K. and Gutmann, D. H. 2014, "Evaluation of Participant Recruitment Methods to a Rare Disease Online Registry", *American journal of medical genetics Part A*, Vol. 164 No. 7**,** pp. 1686-1694.
Johnson, M. E., Mcguire, D. and Willey, N. D. (2008), "The Evolution of the Peer-to-Peer File Sharing Industry and the Security Risks for Users", paper presented at the *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*,2008, avaialable at.
Johnson, R. B. and Onwuegbuzie, A. J. 2004, "Mixed Methods Research: A Research Paradigm Whose Time Has Come", *Educational Researcher*, Vol. 33 No. 7**,** pp. 14-26.
Johnson, R. B., Onwuegbuzie, A. J. and Turner, L. A. 2007, "Toward a Definition of Mixed Methods Research", *Journal of mixed methods research*, Vol. 1 No. 2**,** pp. 112-133.
Johnson, S. D. and Bowers, K. J. 2008, "Stable and Fluid Hotspots of Crime: Differentiation and Identification", *Built Environment*, Vol. 34 No. 1**,** pp. 32-45.
Jones, L. M., Mitchell, K. J. and Finkelhor, D. 2013, "Online Harassment in Context: Trends from Three Youth Internet Safety Surveys (2000, 2005, 2010)", *Psychology of Violence*, Vol. 3 No. 1**,** pp. 53.

Jøsang, A., Zomai, M. A. and Suriadi, S. (2007), "Usability and Privacy in Identity Management Architectures", paper presented at the *Proceedings of the fifth Australasian symposium on ACSW frontiers-Volume 68*,2007, avaialable at.

Joslin, R. and Müller, R. 2016, "Identifying Interesting Project Phenomena Using Philosophical and Methodological Triangulation", *International Journal of Project Management*, Vol. No.

Jupp, V. 2006, *The Sage Dictionary of Social Research Methods*, Sage.

Kahn, C. M. and Liñares-Zegarra, J. M. 2016, "Identity Theft and Consumer Payment Choice: Does Security Really Matter?", *Journal of Financial Services Research*, Vol. 50 No. 1**,** pp. 121-159.

Kahneman, D. 2011, *Thinking, Fast and Slow*, Macmillan.

Kamalul Ariffin, S., Mohan, T. and Goh, Y.-N. 2018, "Influence of Consumers' Perceived Risk on Consumers' Online Purchase Intention", *Journal of Research in Interactive Marketing*, Vol. 12 No. 3**,** pp. 309-327.

Kanan, J. W. and Pruitt, M. V. 2002, "Modeling Fear of Crime and Perceived Victimization Risk: The (in) Significance of Neighborhood Integration", *Sociological inquiry*, Vol. 72 No. 4**,** pp. 527-548.

Kang, N. E. and Yoon, W. C. 2008, "Age-and Experience-Related User Behavior Differences in the Use of Complicated Electronic Devices", *International Journal of Human-Computer Studies*, Vol. 66 No. 6**,** pp. 425-437.

Kanyan, K. K. and Mehra, E. R. 2018, "Big Data Storage in Hadoop: A Review of Security Issues and Threats", Vol. No.

Karlof, C., Shankar, U., Tygar, J. D. and Wagner, D. (2007), "Dynamic Pharming Attacks and Locked Same-Origin Policies for Web Browsers", paper presented at the *Proceedings of the 14th ACM conference on Computer and communications security*,2007, avaialable at.

Karmen, A. 2012, *Crime Victims: An Introduction to Victimology*, Cengage Learning.

Karnieli-Miller, O., Strier, R. and Pessach, L. 2009, "Power Relations in Qualitative Research", *Qualitative health research*, Vol. 19 No. 2**,** pp. 279-289.

Kaspersky. 2017, "How to Avoid Public Wifi Security Risks. available at: https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks (accessed 04/12/2017).

Kauzlarich, D., Matthews, R. A. and Miller, W. J. 2001, "Toward a Victimology of State Crime", *Critical Criminology*, Vol. 10 No. 3**,** pp. 173-194.

Keith, S. 2018, "How Do Traditional Bullying and Cyberbullying Victimization Affect Fear and Coping among Students? An Application of General Strain Theory", *American Journal of Criminal Justice*, Vol. 43 No. 1**,** pp. 67-84.

Keller, P. A. and Block, L. G. 1996, "Increasing the Persuasiveness of Fear Appeals: The Effect of Arousal and Elaboration", *Journal of consumer research*, Vol. 22 No. 4**,** pp. 448-459.

Keller, R. 2012, *Doing Discourse Research: An Introduction for Social Scientists*, Sage.

Kesharwani, A. and Singh Bisht, S. 2012, "The Impact of Trust and Perceived Risk on Internet Banking Adoption in India: An Extension of Technology Acceptance Model", *International Journal of Bank Marketing*, Vol. 30 No. 4**,** pp. 303-322.

Khonji, M., Iraqi, Y. and Jones, A. 2013, "Phishing Detection: A Literature Survey", *IEEE Communications Surveys & Tutorials*, Vol. 15 No. 4**,** pp. 2091-2121.

Kidder, L. H. and Fine, M. 1987, "Qualitative and Quantitative Methods: When Stories Converge", *New directions for program evaluation*, Vol. 1987 No. 35**,** pp. 57-75.

Kienzle, D. and Croall, J. 2009, Preventing Data from Being Submitted to a Remote System in Response to a Malicious E-Mail. Google Patents.

Kim, A.-Y. and Kim, T.-S. (2016), "Factors Influencing the Intention to Adopt Identity Theft Protection Services: Severity Vs Vulnerability", paper presented at the *PACIS*,2016, avaialable at.

Kim, D. and Hyun Kim, J. 2013, "Understanding Persuasive Elements in Phishing E-Mails: A Categorical Content and Semantic Network Analysis", *Online Information Review*, Vol. 37 No. 6**,** pp. 835-850.

Kim, D. J., Ferrin, D. L. and Rao, H. R. 2008, "A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents", *Decision support systems*, Vol. 44 No. 2**,** pp. 544-564.

Kim, D. J., Yim, M.-S., Sugumaran, V. and Rao, H. R. 2016, "Web Assurance Seal Services, Trust and Consumers' Concerns: An Investigation of E-Commerce Transaction Intentions across Two Nations", *European Journal of Information Systems*, Vol. 25 No. 3**,** pp. 252-273.

Kim, J. and Lennon, S. J. 2013, "Effects of Reputation and Website Quality on Online Consumers' Emotion, Perceived Risk and Purchase Intention: Based on the Stimulus-Organism-Response Model", *Journal of Research in Interactive Marketing*, Vol. 7 No. 1**,** pp. 33-56.

Kirk, J. 2015, "Starbucks Still Grappling with Fraud in Online Accounts, Gift Cards. available at: http://www.computerworld.com/article/2921567/security/starbucks-still-grappling-with-fraud-in-online-accounts-gift-cards.html (accessed 12/08/2016).

Kirk, J., Miller, M. L. and Miller, M. L. 1986, *Reliability and Validity in Qualitative Research*, Sage.

Kirton, A. and David, M. 2013, "The Challenge of Unauthorized Online Streaming to the English Premier League and Television Broadcasters", *Digital media sport: Technology, power and identity in the network society*, Vol. No. 81-96.
Knapp, K. J. 2004, "Cyber Warfare: Raising Information Security to a Top Priority": AIR FORCE INST OF TECH WRIGHT-PATTERSONAFB OH, (accessed.
Ko, Y., Chee, W. and Im, E.-O. 2016, "Factors Associated with Perceived Health Status of Multiracial/Ethnic Midlife Women in the United States", *Journal of Obstetric, Gynecologic & Neonatal Nursing*, Vol. 45 No. 3**,** pp. 378-390.
Koetsier, J. 2018, "App Scams: Sneaky 'Utility' Apps Are Stealing $260, $2500, or Even $4700 Each Year ... Per User. available at: https://www.forbes.com/sites/johnkoetsier/2018/10/04/app-scams-cheap-utility-apps-are-stealing-260-2500-or-even-4700-each-year-per-user/#3e3ba603162a (accessed 10/02/2019).
Koops, B.-J. 2010, "The Internet and Its Opportunities for Cybercrime", *Transnational Criminology Manual*, Vol. 1 No. 735-754.
Koops, T., Dekker, A. and Briken, P. 2018, "Online Sexual Activity Involving Webcams—an Overview of Existing Literature and Implications for Sexual Boundary Violations of Children and Adolescents", *Behavioral sciences & the law*, Vol. 36 No. 2**,** pp. 182-197.
Koper, C. S. 1995, "Just Enough Police Presence: Reducing Crime and Disorderly Behavior by Optimizing Patrol Time in Crime Hot Spots", *Justice quarterly*, Vol. 12 No. 4**,** pp. 649-672.
Korkodeilou, J. 2017, "'No Place to Hide' Stalking Victimisation and Its Psycho-Social Effects", *International review of victimology*, Vol. 23 No. 1**,** pp. 17-32.
Koss, M. P. and Dinero, T. E. 1989, "Discriminant Analysis of Risk Factors for Sexual Victimization among a National Sample of College Women", *Journal of consulting and clinical psychology*, Vol. 57 No. 2**,** pp. 242.
Kothari, C. R. 2004, *Research Methodology: Methods and Techniques*, New Age International.
Koyame-Marsh, R. O. and Marsh, J. L. 2014, "Data Breaches and Identity Theft: Costs and Responses", *IOSR Journal of Economics and Finance*, Vol. 5 No. 6**,** pp. 36-45.
Kraemer-Mbula, E., Tang, P. and Rush, H. 2013, "The Cybercrime Ecosystem: Online Innovation in the Shadows?", *Technological Forecasting and Social Change*, Vol. 80 No. 3**,** pp. 541-555.
Krasnova, H. and Veltri, N. F. (2011), "Behind the Curtains of Privacy Calculus on Social Networking Sites: The Study of Germany and the USA", paper presented at the *10th International Conference on Wirtschaftsinformatik, A. Bernstein and G. Schwabe*,2011, avaialable at.
Krasnova, H., Veltri, N. F. and Günther, O. 2012, "Self-Disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture", *Business & Information Systems Engineering*, Vol. 4 No. 3**,** pp. 127-135.
Krippendorff, K. 2004, *Content Analysis: An Introduction to Its Methodology*, Sage.
Krombholz, K., Hobel, H., Huber, M. and Weippl, E. 2015, "Advanced Social Engineering Attacks", *Journal of Information Security and applications*, Vol. 22 No. 113-122.
Kshetri, N. 2010, "The Global Cybercrime Industry and Its Structure: Relevant Actors, Motivations, Threats, and Countermeasures", *The Global Cybercrime Industry*, Springer. pp. 1-34.
Kukar-Kinney, M. and Close, A. G. 2010, "The Determinants of Consumers' Online Shopping Cart Abandonment", *Journal of the Academy of Marketing Science*, Vol. 38 No. 2**,** pp. 240-250.
Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A. and Pham, T. (2009), "School of Phish: A Real-World Evaluation of Anti-Phishing Training", paper presented at the *Proceedings of the 5th Symposium on Usable Privacy and Security*,2009, avaialable at.
Kümpel Nørgaard, M., Bruns, K., Haudrup Christensen, P. and Romero Mikkelsen, M. 2007, "Children's Influence on and Participation in the Family Decision Process During Food Buying", *Young Consumers*, Vol. 8 No. 3**,** pp. 197-216.
Kvale, S. 2006, "Dominance through Interviews and Dialogues", *Qualitative inquiry*, Vol. 12 No. 3**,** pp. 480-500.
Kwok, S. H., Lang, K. R. and Tam, K. Y. 2002, "Peer-to-Peer Technology Business and Service Models: Risks and Opportunities", *Electronic Markets*, Vol. 12 No. 3**,** pp. 175-183.
Lab, S. P. 1990, "Citizen Crime Prevention: Domains and Participation", *Justice Quarterly*, Vol. 7 No. 3**,** pp. 467-491.
Lagazio, M., Sherif, N. and Cushman, M. 2014, "A Multi-Level Approach to Understanding the Impact of Cyber Crime on the Financial Sector", *Computers & Security*, Vol. 45 No. 58-74.
Lagrange, R. L. and Ferraro, K. F. 1989, "Assessing Age and Gender Differences in Perceived Risk and Fear of Crime", *Criminology*, Vol. 27 No. 4**,** pp. 697-720.
Lagrange, R. L., Ferraro, K. F. and Supancic, M. 1992, "Perceived Risk and Fear of Crime: Role of Social and Physical Incivilities", *Journal of research in crime and delinquency*, Vol. 29 No. 3**,** pp. 311-334.
Lai, F., Li, D. and Hsieh, C.-T. 2012, "Fighting Identity Theft: The Coping Perspective", *Decision Support Systems*, Vol. 52 No. 2**,** pp. 353-363.

Laka, P. and Mazurczyk, W. 2018, "User Perspective and Security of a New Mobile Authentication Method", *Telecommunication Systems*, Vol. No. 1-15.
Lakshmi, V. S. and Vijaya, M. 2012, "Efficient Prediction of Phishing Websites Using Supervised Learning Algorithms", *Procedia Engineering*, Vol. 30 No. 798-805.
Lamb, S. 1999, "Constructing the Victim: Popular Images and Lasting Labels", Vol. No.
Lambert, A., Mcquire, S. and Papastergiadis, N. 2018, "Public Space and the Development of Wireless Media", *New Approaches, Methods, and Tools in Urban E-Planning*, IGI Global. pp. 289-309.
Landman, M. (2010), "Managing Smart Phone Security Risks", paper presented at the *2010 Information Security Curriculum Development Conference*,2010, avaialable at.
Lanier, M. and Henry, S. 1998, "Essential Criminology", Vol. No.
Larrimore, N. P. 2018, "Risk Management Strategies to Prevent and Mitigate Emerging Operational Security Threats", Vol. No.
Latha, P. and Vasantha, R. 2015, "Novel Key-Management to Resist Illegitimate Intrusion from Rogue Access Points in Wlan", *Emerging Research in Computing, Information, Communication and Applications*, Springer. pp. 231-237.
Laufer, R. S. and Wolfe, M. 1977, "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory", *Journal of social Issues*, Vol. 33 No. 3**,** pp. 22-42.
Lauritsen, J. L., Sampson, R. J. and Laub, J. H. 1991, "The Link between Offending and Victimization among Adolescents", *Criminology*, Vol. 29 No. 2**,** pp. 265-292.
Lazarsfeld, P. F. 1958, "Evidence and Inference in Social Research", *Daedalus*, Vol. 87 No. 4**,** pp. 99-130.
Lazarus, R. S. 1980, "Stress and Coping Paradigm", *Competence and coping during adulthood/Lynne A. Bond and James C. Rosen, editors*, Vol. No.
Lazarus, R. S. and Folkman, S. 1984, *Stress, Appraisal, and Coping*, Springer Publishing Company.
Lease, M. L. and Burke, T. W. 2000, "Identity Theft: A Fast-Growing Crime", *FBI L. Enforcement Bull.*, Vol. 69 No. 8.
Leclerc, B. and Wortley, R. 2013, *Cognition and Crime: Offender Decision Making and Script Analyses*, Routledge.
Lee, B., Chen, Y. and Hewitt, L. 2011, "Age Differences in Constraints Encountered by Seniors in Their Use of Computers and the Internet", *Computers in Human Behavior*, Vol. 27 No. 3**,** pp. 1231-1237.
Lee, H., Lim, D., Kim, H., Zo, H. and Ciganek, A. P. 2015, "Compensation Paradox: The Influence of Monetary Rewards on User Behaviour", *Behaviour & Information Technology*, Vol. 34 No. 1**,** pp. 45-56.
Leisenring, A. 2006, "Confronting "Victim" Discourses: The Identity Work of Battered Women", *Symbolic interaction*, Vol. 29 No. 3**,** pp. 307-330.
Leitenberg, H., Greenwald, E. and Cado, S. 1992, "A Retrospective Study of Long-Term Methods of Coping with Having Been Sexually Abused During Childhood", *Child Abuse & Neglect*, Vol. 16 No. 3**,** pp. 399-407.
Leontiadis, I., Efstratiou, C., Picone, M. and Mascolo, C. (2012), "Don't Kill My Ads! Balancing Privacy in an Ad-Supported Mobile Application Market", paper presented at the *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications*,2012, avaialable at.
Leukfeldt, E. 2015, "Comparing Victims of Phishing and Malware Attacks", *International Journal of advanced studies in Computer Science and Engineering*, Vol. 4 No. 5**,** pp. 26-32.
Leukfeldt, E. R. 2014, "Phishing for Suitable Targets in the Netherlands: Routine Activity Theory and Phishing Victimization", *Cyberpsychology, Behavior, and Social Networking*, Vol. 17 No. 8**,** pp. 551-555.
Leukfeldt, E. R. and Yar, M. 2016, "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis", *Deviant Behavior*, Vol. 37 No. 3**,** pp. 263-280.
Levi, M. 2001, ""Between the Risk and the Reality Falls the Shadow"-Evidence and Urban Legends in Computer Fraud", *Crime and the Internet, London: Routledge*, Vol. No. 44-58.
Levi, M. (2009), "E-Gaming and Money Laundering Risks: A European Overview", paper presented at the *ERA Forum*,2009, avaialable at.
Levi, M. 2016, "Trends and Costs of Fraud", *Fraud*, Routledge. pp. 37-48.
Levi, M. 2017, "Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues", *Crime, Law and Social Change*, Vol. 67 No. 1**,** pp. 3-20.
Levi, M., Doig, A., Gundur, R., Wall, D. and Williams, M. 2017, "Cyberfraud and the Implications for Effective Risk-Based Responses: Themes from Uk Research", *Crime, Law and Social Change*, Vol. 67 No. 1**,** pp. 77-96.
Levi, M., Doig, A., Gundur, R., Wall, D. and Williams, M. L. 2015, "The Implications of Economic Cybercrime for Policing": City of London Corporation, available at: https://www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Documents/Research-2015/Economic-Cybercrime-FullReport.pdf. (accessed 11 June 2017).
Levi, M. and Pithouse, A. 1992, "The Victims of Fraud", *Unravelling Criminal Justice*, Springer. pp. 229-246.

Lewis, J. 2013, "Design Issues", in: Ritchie, J., Lewis, J., Nicholls, C. M. and Ormston, R. (eds.), *Qualitative Research Practice: A Guide for Social Science Students and Researchers*, sage. pp.
Li, Q. 2006, "Cyberbullying in Schools: A Research of Gender Differences", *School psychology international*, Vol. 27 No. 2**,** pp. 157-170.
Li, T. B. Q. 2005, "Cyber-Harassment: Aastudy of a New Method for an Old Behavior", *Journal of educational computing research*, Vol. 32 No. 3**,** pp. 265-277.
Liamputtong, P. 2007, *Researching the Vulnerable: A Guide to Sensitive Research Methods*, Sage.
Liang, H. and Xue, Y. 2009, "Avoidance of Information Technology Threats: A Theoretical Perspective", *MIS quarterly*, Vol. No. 71-90.
Liang, H. and Xue, Y. 2010, "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective", *Journal of the Association for Information Systems*, Vol. 11 No. 7**,** pp. 394.
Lin, K.-Y. and Lu, H.-P. 2011, "Why People Use Social Networking Sites: An Empirical Study Integrating Network Externalities and Motivation Theory", *Computers in human behavior*, Vol. 27 No. 3**,** pp. 1152-1161.
Lincoln, Y. S. and Guba, E. G. 1985, *Naturalistic Inquiry*, Sage.
Liska, A. E., Lawrence, J. J. and Sanchirico, A. 1982, "Fear of Crime as a Social Fact", *Social Forces*, Vol. 60 No. 3**,** pp. 760-770.
Liska, A. E., Sanchirico, A. and Reed, M. D. 1988, "Fear of Crime and Constrained Behavior Specifying and Estimating a Reciprocal Effects Model", *Social Forces*, Vol. 66 No. 3**,** pp. 827-837.
Little, C. B. 2007, "Deviance, Absolutist Definitions Of", *The Blackwell Encyclopedia of Sociology*, Vol. No.
Livingstone, S. 2008, "Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression", *New media & society*, Vol. 10 No. 3**,** pp. 393-411.
Lobiondo-Wood, G. and Haber, J. 2014, *Nursing Research-E-Book: Methods and Critical Appraisal for Evidence-Based Practice*, Elsevier Health Sciences.
Locke, L. F., Spirduso, W. W. and Silverman, S. J. 2014, *Proposals That Work*, Sage.
Logan, T., Walker, R., Shannon, L. and Cole, J. 2008, "Combining Ethical Considerations with Recruitment and Follow-up Strategies for Partner Violence Victimization Research", *Violence Against Women*, Vol. 14 No. 11**,** pp. 1226-1251.
Lotz, R. 1979, "Public Anxiety About Crime", *Pacific Sociological Review*, Vol. 22 No. 2**,** pp. 241-254.
Lowry, P. B., Dinev, T. and Willison, R. 2017, "Why Security and Privacy Research Lies at the Centre of the Information Systems (Is) Artefact: Proposing a Bold Research Agenda", *European Journal of Information Systems*, Vol. 26 No. 6**,** pp. 546-563.
Lu, Y. and Thabtah, F. (2017), "Intelligent Smart Bait Fishing: A New Mobile App Business Model", paper presented at the *Proceedings of the International Conference on Business and Information Management*,2017, avaialable at.
Lumsden, K. and Winter, A. 2014, "Reflexivity in Criminological Research", *Reflexivity in Criminological Research*, Springer. pp. 1-19.
Luo, X. R., Zhang, W., Burd, S. and Seazzu, A. 2013, "Investigating Phishing Victimization with the Heuristic–Systematic Model: A Theoretical Framework and an Exploration", *Computers & Security*, Vol. 38 No. 28-38.
Lustgarten, S. D. 2015, "Emerging Ethical Threats to Client Privacy in Cloud Communication and Data Storage", *Professional Psychology: Research and Practice*, Vol. 46 No. 3**,** pp. 154.
Lwin, M. O., Li, B. and Ang, R. P. 2012, "Stop Bugging Me: An Examination of Adolescents' Protection Behavior against Online Harassment", *Journal of adolescence*, Vol. 35 No. 1**,** pp. 31-41.
Lykeridou, K., Gourounti, K., Sarantaki, A., Loutradis, D., Vaslamatzis, G. and Deltsidou, A. 2011, "Occupational Social Class, Coping Responses and Infertility-Related Stress of Women Undergoing Infertility Treatment", *Journal of clinical nursing*, Vol. 20 No. 13-14**,** pp. 1971-1980.
Lynch, J. 2005, "Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks", *Berkeley Technology Law Journal*, Vol. No. 259-300.
Ma, W., Duan, P., Liu, S., Gu, G. and Liu, J.-C. 2012, "Shadow Attacks: Automatically Evading System-Call-Behavior Based Malware Detection", *Journal in Computer Virology*, Vol. 8 No. 1-2**,** pp. 1-13.
Machackova, H., Cerna, A., Sevcikova, A., Dedkova, L. and Daneback, K. 2013, "Effectiveness of Coping Strategies for Victims of Cyberbullying", *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, Vol. 7 No. 3**,** pp.
Machmutow, K., Perren, S., Sticca, F. and Alsaker, F. D. 2012, "Peer Victimisation and Depressive Symptoms: Can Specific Coping Strategies Buffer the Negative Impact of Cybervictimisation?", *Emotional and Behavioural Difficulties*, Vol. 17 No. 3-4**,** pp. 403-420.
Macwan, A. 2004, "Approach for Identification and Analysis of Human Vulnerabilities in Protecting Telecommunications Infrastructure", *Bell Labs Technical Journal*, Vol. 9 No. 2**,** pp. 85-89.

Maddison, J. and Jeske, D. 2014, "Fear and Perceived Likelihood of Victimization in Traditional and Cyber Settings", *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL)*, Vol. 4 No. 4**,** pp. 23-40.
Maddux, J. E. and Rogers, R. W. 1983, "Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change", *Journal of experimental social psychology*, Vol. 19 No. 5**,** pp. 469-479.
Madensen, T. D. and Eck, J. E. 2008, "Violence in Bars: Exploring the Impact of Place Manager Decision-Making", *Crime Prevention and Community Safety*, Vol. 10 No. 2**,** pp. 111-125.
Madriz, E. 1997, *Nothing Bad Happens to Good Girls: Fear of Crime in Women's Lives*, Univ of California Press.
Maheswaran, D. and Chaiken, S. 1991, "Promoting Systematic Processing in Low-Motivation Settings: Effect of Incongruent Information on Processing and Judgment", *Journal of personality and social psychology*, Vol. 61 No. 1**,** pp. 13.
Maimon, D. and Browning, C. R. 2012, "Adolescents' Violent Victimization in the Neighbourhood: Situational and Contextual Determinants", *British Journal of Criminology*, Vol. 52 No. 4**,** pp. 808-833.
Maimon, D., Wilson, T., Ren, W. and Berenblum, T. 2015, "On the Relevance of Spatial and Temporal Dimensions in Assessing Computer Susceptibility to System Trespassing Incidents", *British Journal of Criminology*, Vol. 55 No. 3**,** pp. 615-634.
Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S. and Ignatuschtschenko, E. 2013, "Comprehensive Study on Cybercrime", *United Nations Office on Drugs and Crime, Tech. Rep*, Vol. No.
Malhotra, N. and Birks, D. F. 2012, *Marketing Research: An Applied Approach*, Harlow : Financial Times/Prentice Hall, Harlow.
Malleson, N. and Andresen, M. A. 2015, "Spatio-Temporal Crime Hotspots and the Ambient Population", *Crime science*, Vol. 4 No. 1**,** pp. 10.
Malterud, K. 2001, "Qualitative Research: Standards, Challenges, and Guidelines", *The lancet*, Vol. 358 No. 9280**,** pp. 483-488.
Man, A. D., Dolan, D., Pelletier, R. and Reid, C. 1994, "Adolescent Running Away Behavior: Active or Passive Avoidance?", *The Journal of genetic psychology*, Vol. 155 No. 1**,** pp. 59-64.
Mann, C. and Stewart, F. 2000, *Internet Communication and Qualitative Research: A Handbook for Researching Online*, Sage.
Mansfield, P. R., Lexchin, J., Wen, L. S., Grandori, L., Mccoy, C. P., Hoffman, J. R., Ramos, J. and Jureidini, J. N. 2006, "Educating Health Professionals About Drug and Device Promotion: Advocates' Recommendations", *PLoS medicine*, Vol. 3 No. 11**,** pp. e451.
Manyiwa, S. and Brennan, R. 2012, "Fear Appeals in Anti-Smoking Advertising: How Important Is Self-Efficacy?", *Journal of Marketing Management*, Vol. 28 No. 11-12**,** pp. 1419-1437.
Marcum, C. D. 2011, "Adolescent Online Victimization and Constructs of Routine Activities Theory", *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*, Vol. No. 253-276.
Marcum, C. D., Higgins, G. E. and Ricketts, M. L. 2010, "Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory", *Deviant Behavior*, Vol. 31 No. 5**,** pp. 381-410.
Mariel, C., Jackie, G., Paige, M., Rigoberto, S., Marissa, T. and Gabriela, V. 2018, "Science Blogs", Vol. No.
Mark, M. M. 2015, "Mixed and Multimethods in Predominantly Quantitative Studies, Especially Experiments and Quasi-Experiments", in: Hesse-Biber, S. N. and Johnson, R. B. (eds.), *The Oxford Handbook of Multimethod and Mixed Methods Research Inquiry*, Oxford University Press, London, England. pp. 21-41.
Marler, W. 2018, "Mobile Phones and Inequality: Findings, Trends, and Future Directions", *New Media & Society*, Vol. No. 1461444818765154.
Marshall, B., Cardon, P., Poddar, A. and Fontenot, R. 2013, "Does Sample Size Matter in Qualitative Research?: A Review of Qualitative Interviews in Is Research", *Journal of Computer Information Systems*, Vol. 54 No. 1**,** pp. 11-22.
Marshall, P. J. 2010, "Online Banking: Information Security Vs. Hackers Research Paper", *International Journal of Scientific & Engineering Research*, Vol. 1 No. 1**,** pp.
Martellini, M., Abaimov, S., Gaycken, S. and Wilson, C. 2017, "Future Attack Patterns", *Information Security of Highly Critical Wireless Networks*, Springer. pp. 59-62.
Martin, B. 1996, "Technological Vulnerability", *Technology in Society*, Vol. 18 No. 4**,** pp. 511-523.
Martin, J. 2014, "Lost on the Silk Road: Online Drug Distribution and the 'Cryptomarket'", *Criminology & Criminal Justice*, Vol. 14 No. 3**,** pp. 351-367.
Mason, K. A. and Benson, M. L. 1996, "The Effect of Social Support on Fraud Victims' Reporting Behavior: A Research Note", *Justice Quarterly*, Vol. 13 No. 3**,** pp. 511-524.
Mason, M. (2010), "Sample Size and Saturation in Phd Studies Using Qualitative Interviews", paper presented at the *Forum qualitative Sozialforschung/Forum: qualitative social research*,2010, avaialable at.

Masson, K. and Bancroft, A. 2018, "'Nice People Doing Shady Things': Drugs and the Morality of Exchange in the Darknet Cryptomarkets", *International Journal of Drug Policy*, Vol. 58 No. 78-84.
Mathew, A. R., Al Hajj, A. and Al Ruqeishi, K. (2010), "Cybercrimes: Threats and Protection", paper presented at the *2010 International Conference on Networking and Information Technology*,2010, avaialable at.
Mattern, B. 2017, "Cyber Security and Hacktivism in Latin America: Past and Future", *Coha. org*, Vol. No.
Mattson, M. 2002, "Impact of Hiv Test Counseling on College Students' Sexual Beliefs and Behaviors", *American Journal of Health Behavior*, Vol. 26 No. 2**,** pp. 121-136.
Maume Jr, D. J. 1989, "Inequality and Metropolitan Rape Rates: A Routine Activity Approach", *Justice Quarterly*, Vol. 6 No. 4**,** pp. 513-527.
Maurushat, A. 2010, "Australia's Accession to the Cybercrime Convention: Is the Convention Still Relevant in Combating Cybercrime in the Era of Botnets and Obfuscation Crime Tools", *UNSWLJ*, Vol. 33 No. 431.
Maxfield, M. G. 1987, "Lifestyle and Routine Activity Theories of Crime: Empirical Studies of Victimization, Delinquency, and Offender Decision-Making", *Journal of Quantitative Criminology*, Vol. 3 No. 4**,** pp. 275-282.
Maxfield, M. G. and Babbie, E. R. 2015, *Basics of Research Methods for Criminal Justice and Criminology*, Wadsworth, Belmont, CA.
Maxwell, J. 1992, "Understanding and Validity in Qualitative Research", *Harvard educational review*, Vol. 62 No. 3**,** pp. 279-301.
Maxwell, J. A. 2012, *Qualitative Research Design: An Interactive Approach*, Sage publications.
May, D. C., Rader, N. E. and Goodrum, S. 2010, "A Gendered Assessment of the ''Threat of Victimization'': Examining Gender Differences in Fear of Crime, Perceived Risk, Avoidance, and Defensive Behaviors", *Criminal Justice Review*, Vol. 35 No. 2**,** pp. 159-182.
Mcafee. 2013, "What Is a "Drive-by" Download? available at: https://securingtomorrow.mcafee.com/consumer/family-safety/drive-by-download/ (accessed 23/11/2017).
Mccorkle, D., Reardon, J., Dalenberg, D., Pryor, A. and Wicks, J. 2012, "Purchase or Pirate: A Model of Consumer Intellectual Property Theft", *Journal of Marketing Theory and Practice*, Vol. 20 No. 1**,** pp. 73-86.
Mccoy, C. 2010, "Perceived Self-Efficacy and Technology Proficiency in Undergraduate College Students", *Computers & Education*, Vol. 55 No. 4**,** pp. 1614-1617.
Mccudden, C. 2015. *Constructing Meaning in Occupational Therapy Practice: The Experience of a Posture and Mobility Service in Wales.* University of Brighton.
Mcguire, M. and Dowling, S. 2013, "Improving the Cyber Crime Evidence Base": Home Office, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246756/horr75-chap4.pdf (accessed 09 July 2019).
Mckown, C. 2017, "The American Greed Report: Online Shopping Scams: Eight Signs You're on a Fake Site. available at: https://www.cnbc.com/2017/06/16/online-shopping-scams-how-to-identify-fake-sites.html (accessed 11/10/2018).
Mcmullan, J. L. and Rege, A. 2010, "Online Crime and Internet Gambling", *Journal of Gambling Issues*, Vol. No. 24**,** pp. 54-85.
Mcneeley, S. 2015, "Lifestyle-Routine Activities and Crime Events", *Journal of Contemporary Criminal Justice*, Vol. No. 1043986214552607.
Mcquade, S. C. 2006, *Understanding and Managing Cybercrime*, Pearson/Allyn and Bacon Boston, MA.
Mehdi, M. M. 2018, "Factors Influencing the Usage of Social Networking Sites", *International Journal of Marketing & Business Communication*, Vol. 7 No. 1**,** pp.
Mehta, P. 2001, "Control Variable in Research", *International encyclopedia of the social & behavioral sciences: Elsevier Science*, Vol. No. 2727-2730.
Meier, R. F. and Miethe, T. D. 1993, "Understanding Theories of Criminal Victimization", *Crime and Justice*, Vol. 17 No. 459-499.
Mellon, C. A. 1990, "Naturalistic Inquiry for Library Science: Methods and Applications for Research", *Evaluation and Teaching. New York: Greenwood*, Vol. No.
Melossi, D. 1994, "The Economy of Illegalities: Normal Crimes, Elites and Social Control in Comparative Analysis", *The Futures of Criminology. London: Sage*, Vol. No. 202-19.
Mende, M., Scott, M. L., Garvey, A. M. and Bolton, L. E. 2019, "The Marketing of Love: How Attachment Styles Affect Romantic Consumption Journeys", *Journal of the Academy of Marketing Science*, Vol. No. 1-19.
Mendelsohn, B. 1968, "Rape in Criminology", in: Schafer, S. (ed.) *The Victim and His Criminal: A Study in Functional Responsibility*, Random House New York. pp.
Menon, S. and Guan Siew, T. 2012, "Key Challenges in Tackling Economic and Cyber Crimes: Creating a Multilateral Platform for International Co-Operation", *Journal of Money Laundering Control*, Vol. 15 No. 3**,** pp. 243-256.

Merriam, S. B. 1998, *Qualitative Research and Case Study Applications in Education. Revised and Expanded from" Case Study Research in Education."*, ERIC.
Mertens, D. M. and Tarsilla, M. 2015, "Mixed Methods Evaluation", in: Hesse-Biber, S. N. and Johnson, R. B. (eds.), *The Oxford Handbook of Multi and Mixed Methods Research Inquiry*, Oxford University Press, London. pp. 426-446.
Metcalfe, S. E. and Sexton, E. H. 2014, "An Academic-Community Partnership to Address the Flu Vaccination Rates of the Homeless", *Public health nursing*, Vol. 31 No. 2**,** pp. 175-182.
Meyer, I. H., Schwartz, S. and Frost, D. M. 2008, "Social Patterning of Stress and Coping: Does Disadvantaged Social Statuses Confer More Stress and Fewer Coping Resources?", *Social science & medicine*, Vol. 67 No. 3**,** pp. 368-379.
Miers, D. 1989, "Positivist Victimology: A Critique", *International review of victimology*, Vol. 1 No. 1**,** pp. 3-22.
Miers, D. 1990, "Positivist Victimology: A Critique Part 2: Critical Victimology", *International review of victimology*, Vol. 1 No. 3**,** pp. 219-230.
Miethe, T., Stafford, M. and Long, J. 1987, "Social Differentiation in Criminal Victimization: A Test of Routine Activities/Lifestyle Theories", *American Sociological Review*, Vol. 52 No. 2**,** pp. 184-184.
Miethe, T. D. 1985, "The Myth or Reality of Victim Involvement in Crime", *Sociological focus*, Vol. 18 No. 3**,** pp. 209.
Miethe, T. D. and Mcdowall, D. 1993, "Contextual Effects in Models of Criminal Victimization", *Social Forces*, Vol. 71 No. 3**,** pp. 741-759.
Miethe, T. D. and Meier, R. F. 1990, "Opportunity, Choice, and Criminal Victimization: A Test of a Theoretical Model", *Journal of research in Crime and Delinquency*, Vol. 27 No. 3**,** pp. 243-266.
Miethe, T. D. and Meier, R. F. 1994, *Crime and Its Social Context: Toward an Integrated Theory of Offenders, Victims, and Situations*, Suny Press.
Miles, M., Huberman, A. M. and Saldaña, J. 2014, *Qualitative Data Analysis: A Methods Sourcebook*, Sage, London.
Miles, M. B. and Huberman, A. M. 1994, *Qualitative Data Analysis: An Expanded Sourcebook*, Sage.
Milne, G. R., Labrecque, L. I. and Cromer, C. 2009, "Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices", *Journal of Consumer Affairs*, Vol. 43 No. 3**,** pp. 449-473.
Milne, G. R., Rohm, A. J. and Bahl, S. 2004, "Consumers' Protection of Online Privacy and Identity", *Journal of Consumer Affairs*, Vol. 38 No. 2**,** pp. 217-232.
Miltgen, C. L. and Smith, H. J. 2015, "Exploring Information Privacy Regulation, Risks, Trust, and Behavior", *Information & Management*, Vol. 52 No. 6**,** pp. 741-759.
Mishra, M., Gaurav, A. J. and Jain, A. 2012, "A Preventive Anti-Phishing Technique Using Code Word", *International Journal of Computer Science and Information Technologies*, Vol. 3 No. 3**,** pp. 4248-4250.
Mitchell, V.-W. 1999, "Consumer Perceived Risk: Conceptualisations and Models", *European Journal of marketing*, Vol. 33 No. 1/2**,** pp. 163-195.
Mitchell, V.-W. and Greatorex, M. 1993, "Risk Perception and Reduction in the Purchase of Consumer Services", *Service Industries Journal*, Vol. 13 No. 4**,** pp. 179-200.
Mobile Iron. 2016, "Mobile Security and Risk Review", available at: https://www.mobileiron.com/en/quarterly-security-reports/q4-2015-mobile-security-and-risk-review (accessed 10/11/2016).
Mohamed, N. and Ahmad, I. H. 2012, "Information Privacy Concerns, Antecedents and Privacy Measure Use in Social Networking Sites: Evidence from Malaysia", *Computers in Human Behavior*, Vol. 28 No. 6**,** pp. 2366-2375.
Mohammad, R. M., Thabtah, F. and Mccluskey, L. 2015, "Tutorial and Critical Analysis of Phishing Websites Methods", *Computer Science Review*, Vol. 17 No. 1-24.
Mohebzada, J. G., El Zarka, A., Bhojani, A. H. and Darwish, A. (2012), "Phishing in a University Community: Two Large Scale Phishing Experiments", paper presented at the *2012 International Conference on Innovations in Information Technology (IIT)*,2012, avaialable at.
Montague, D. A. 2010, *Essentials of Online Payment Security and Fraud Prevention*, John Wiley & Sons.
Moore, K. E., Folk, J. B., Boren, E. A., Tangney, J. P., Fischer, S. and Schrader, S. W. 2016, "Pilot Study of a Brief Dialectical Behavior Therapy Skills Group for Jail Inmates", Vol. No.
Moore, S. and Shepherd, J. 2006, "The Elements and Prevalence of Fear", *British Journal of Criminology*, Vol. 47 No. 1**,** pp. 154-162.
Moore, T. and Clayton, R. (2012), "Discovering Phishing Dropboxes Using Email Metadata", paper presented at the *eCrime Researchers Summit (eCrime), 2012*,2012, avaialable at.
Moquin, R. and Wakefield, R. L. 2016, "The Roles of Awareness, Sanctions, and Ethics in Software Compliance", *Journal of Computer Information Systems*, Vol. 56 No. 3**,** pp. 261-270.
Moriarty, L. J. and Williams, J. E. 1996, "Examining the Relationship between Routine Activities Theory and Social Disorganization: An Analysis of Property Crime Victimization", *American Journal of Criminal Justice*, Vol. 21 No. 1**,** pp. 43-59.

Morris, T. 2006, *Social Work Research Methods: Four Alternative Paradigms*, Sage.
Morse, J. M. 1991, "Approaches to Qualitative-Quantitative Methodological Triangulation", *Nursing research*, Vol. 40 No. 2**,** pp. 120-123.
Morse, J. M. 2000, Determining Sample Size. Sage Publications Sage CA: Thousand Oaks, CA.
Morton, A. 2014, "'All My Mates Have Got It, So It Must Be Okay': Constructing a Richer Understanding of Privacy Concerns—an Exploratory Focus Group Study", *Reloading Data Protection*, Springer. pp. 259-298.
Mowery, D. C. and Simcoe, T. 2002, "Is the Internet a Us Invention?—an Economic and Technological History of Computer Networking", *Research Policy*, Vol. 31 No. 8-9**,** pp. 1369-1387.
Muehlenhard, C. L. and Macnaughton, J. S. 1988, "Women's Beliefs About Women Who "Lead Men On"", *Journal of Social and Clinical Psychology*, Vol. 7 No. 1**,** pp. 65-79.
Mujere, N. 2016, "Sampling in Research", in: Baran, M. L. (ed.) *Mixed Methods Research for Improved Scientific Study*, IGI Global. pp.
Mukherjee, A. and Dubé, L. 2012, "Mixing Emotions: The Use of Humor in Fear Advertising", *Journal of Consumer Behaviour*, Vol. 11 No. 2**,** pp. 147-161.
Munjal, S. 2016, "Cyber Crimes–Threat for the E-Commerce", Vol. No.
Mustaine, E. and Tewksbury, R. 2000a, "Comparing the Lifestyles of Victims, Offenders, and Victim-Offenders: A Routine Activity Theory Assessment of Similarities and Differences for Criminal Incident Participants", *Sociological Focus*, Vol. 33 No. 3**,** pp. 339.
Mustaine, E. E. and Tewksbury, R. 1998, "Predicting Risks of Larceny Theft Victimization: A Routine Activity Analysis Using Refined Lifestyle Measures", *Criminology*, Vol. 36 No. 4**,** pp. 829-858.
Mustaine, E. E. and Tewksbury, R. 2000b, "Comparing the Lifestyles of Victims, Offenders, and Victim-Offenders: A Routine Activity Theory Assessment of Similarities and Differences for Criminal Incident Participants", *Sociological Focus*, Vol. 33 No. 3**,** pp. 339-362.
Mustaine, E. E. and Tewksbury, R. 2002, "Sexual Assault of College Women: A Feminist Interpretation of a Routine Activities Analysis", *Criminal Justice Review*, Vol. 27 No. 1**,** pp. 89-123.
Mwagwabi, F., Mcgill, T. and Dixon, M. (2014), "Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines", paper presented at the *2014 47th Hawaii International Conference on System Sciences (HICSS)*,2014, avaialable at.
Myers, S. 2007, "Introducton to Phishing", in: Jakobsson, M. and Myers, S. (eds.), *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*, John Wiley & Sons. pp.
Myles, S., Tocci, C., Falk, M., Lynch, S., Torres, C., Brown, B., Leopanto Firman, B., Lake, M., Maser, C. A. and Onativia, A. 2018, "A Multicenter Investigation of Factors Influencing Women's Participation in Clinical Trials", *Journal of Women's Health*, Vol. 27 No. 3**,** pp. 258-270.
Nadkarni, A. and Hofmann, S. G. 2012, "Why Do People Use Facebook?", *Personality and individual differences*, Vol. 52 No. 3**,** pp. 243-249.
Naidoo, R. (2015), "Analysing Urgency and Trust Cues Exploited in Phishing Scam Designs", paper presented at the *10th International Conference on Cyber Warfare and Security*,2015, avaialable at.
Narang, K., Dumais, S. T., Craswell, N., Liebling, D. and Ai, Q. (2017), "Large-Scale Analysis of Email Search and Organizational Strategies", paper presented at the *Proceedings of the 2017 Conference on Conference Human Information Interaction and Retrieval*,2017, avaialable at.
Narvaez, J., Endicott-Popovsky, B., Seifert, C., Aval, C. and Frincke, D. A. (2010), "Drive-by-Downloads", paper presented at the *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*,2010, avaialable at.
Nash, K. and Scott, A. 2008, *The Blackwell Companion to Political Sociology*, John Wiley & Sons.
Neergaard, H. and Ulhøi, J. P. 2007, *Handbook of Qualitative Research Methods in Entrepreneurship*, Edward Elgar Publishing.
Newman, G. R. and Clarke, R. V. 2003, *Superhighway Robbery: Crime Prevention and E-Commerce Crime*, Cullompton : Willan, Cullompton.
Newman, G. R. and Clarke, R. V. 2013, *Superhighway Robbery*, Routledge.
Ngo, F. and Paternoster, R. 2011, "Cybercrime Victimization: An Examination of Individual and Situational Level Factors", *International Journal of Cyber Criminology*, Vol. 5 No. 1**,** pp. 773-793.
Nieminen, R. 2016, "Consumer Perceptions and Attitudes Towards Second-Hand C2c Online Buying", Vol. No.
Nirmal, K., Ewards, S. V. and Geetha, K. (2010), "Maximizing Online Security by Providing a 3 Factor Authentication System to Counter-Attack'phishing'", paper presented at the *Emerging Trends in Robotics and Communication Technologies (INTERACT), 2010 International Conference on*,2010, avaialable at.
Noguti, V., Singh, S. and Waller, D. S. 2018, "Gender Differences in Motivations to Use Social Networking Sites", *Social Media Marketing: Breakthroughs in Research and Practice*, IGI Global. pp. 680-695.

Noor, M. M. and Hassan, W. H. 2013, "Wireless Networks: Developments, Threats and Countermeasures", *International Journal of Digital Information and Wireless Communications (IJDIWC)*, Vol. 3 No. 1**,** pp. 125-140.
Nørgaard, M. K. and Brunsø, K. 2011, "Family Conflicts and Conflict Resolution Regarding Food Choices", *Journal of Consumer Behaviour*, Vol. 10 No. 3**,** pp. 141-151.
Norman, P., Boer, H. and Seydel, E. R. 2005, "Protection Motivation Theory", *Predicting health behaviour*, Vol. 81 No. 126.
Norton. 2017, "The Risks of Public Wi-Fi. available at: https://us.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html (accessed 04/12/2017).
Norton. 2018, "Mobile Scams: How to Identify Them and Protect Yourself. available at: https://us.norton.com/internetsecurity-mobile-mobile-scams-how-to-identify-them-and-protect-yourself.html (accessed 11/11/2018).
Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. and Whitty, M. (2014), "Understanding Insider Threat: A Framework for Characterising Attacks", paper presented at the *Security and Privacy Workshops (SPW), 2014 IEEE*,2014, avaialable at.
Nyamathi, A. 1989, "Comprehensive Health Seeking and Coping Paradigm", *Journal of advanced nursing*, Vol. 14 No. 4**,** pp. 281-290.
O'dea, B. and Campbell, A. 2012, "Online Social Networking and the Experience of Cyber-Bullying", *Studies In Health Technology And Informatics*, Vol. 181 No. 212-216.
O'dwyer, L. M. and Bernauer, J. A. 2013, *Quantitative Research for the Qualitative Researcher*, Sage Publications.
O'flaherty, B. and Whalley, J. 2004, "Qualitative Analysis Software Applied to Is Research-Developing a Coding Strategy", *ECIS 2004 Proceedings*, Vol. No. 123.
O'donnell, A. 2017, "The Dangers of Evil Twin Wi-Fi Hotspots. available at: https://www.lifewire.com/dangers-of-evil-twin-wi-fi-hotspots-2487659 (accessed 04/12/2017).
O'leary, N. 2014, "Negotiating 'Victim Communities': Reflexivity and Method in Researching High-Profile Crimes", in: Lumsden, K. and Winter, A. (eds.), *Reflexivity in Criminological Research: Experiences with the Powerful Adn the Powerless*, Palgrave Macmillan. pp. 23-34.
Office for National Statistics. 2015, "Crime Survey for England and Wales' ": Office for National Statistics, available at: http://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2015-08-06 (accessed 02/02/2016).
Office for National Statistics. 2016a, "Crime Survey for England and Wales, 2014-2015, [Data Collection]", available at: http://dx.doi.org/10.5255/UKDA-SN-7889-1. (accessed 03 January 2017).
Office for National Statistics. 2016b, "Crime Survey for England and Wales, 2014-2015, Questionnaire", available at: https://beta.ukdataservice.ac.uk/datacatalogue/studies/study?id=7619&type=Data%20catalogue (accessed.
Office for National Statistics. 2016b, "Crime Survey for England and Wales Technical Report 2014/15", available at: http://doc.ukdataservice.ac.uk/doc/7889/mrdoc/pdf/7889_csew_technical_report.pdf (accessed 03 January 2017).
Office for National Statistics. 2018, "Statistical Bulletin Internet Access Households and Individuals, Great Britain", available at: https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/bulletins/internetaccesshouseholdsandindividuals/2018 (accessed 05 June 2019).
Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T. and Ebner, N. (2017), "Dissecting Spear Phishing Emails for Older Vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing", paper presented at the *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*,2017, avaialable at.
Oliver, D. G., Serovich, J. M. and Mason, T. L. 2005, "Constraints and Opportunities with Interview Transcription: Towards Reflection in Qualitative Research", *Social forces*, Vol. 84 No. 2**,** pp. 1273-1289.
Olsen, R. B., Orr, L. L., Bell, S. H. and Stuart, E. A. 2013, "External Validity in Policy Evaluations That Choose Sites Purposively", *Journal of Policy Analysis and Management*, Vol. 32 No. 1**,** pp. 107-121.
Olson, K. E., O'brien, M. A., Rogers, W. A. and Charness, N. 2011, "Diffusion of Technology: Frequency of Use for Younger and Older Adults", *Ageing international*, Vol. 36 No. 1**,** pp. 123-145.
Ong, E. Y., Ang, R. P., Ho, J. C., Lim, J. C., Goh, D. H., Lee, C. S. and Chua, A. Y. 2011, "Narcissism, Extraversion and Adolescents' Self-Presentation on Facebook", *Personality and individual differences*, Vol. 50 No. 2**,** pp. 180-185.
Onwuegbuzie, A. J. and Collins, K. M. 2007, "A Typology of Mixed Methods Sampling Designs in Social Science Research", *The qualitative report*, Vol. 12 No. 2**,** pp. 281-316.

Onwuegbuzie, A. J. and Daniel, L. G. 2003, "Typology of Analytical and Interpretational Errors in Quantitative and Qualitative Educational Research", *Current Issues in Education*, Vol. 6 No.
Onwuegbuzie, A. J. and Dickinson, W. B. 2008, "Mixed Methods Analysis and Information Visualization: Graphical Display for Effective Communication of Research Results", *Qualitative report*, Vol. 13 No. 2**,** pp. 204-225.
Onwuegbuzie, A. J. and Johnson, R. B. 2006, "The Validity Issue in Mixed Research", *Research in the Schools*, Vol. 13 No. 1**,** pp. 48-63.
Onwuegbuzie, A. J. and Leech, N. L. 2006, "Linking Research Questions to Mixed Methods Data Analysis Procedures", *The qualitative report*, Vol. 11 No. 3**,** pp. 474-498.
Onwuegbuzie, A. J. and Leech, N. L. 2007, "A Call for Qualitative Power Analyses", *Quality & Quantity*, Vol. 41 No. 1**,** pp. 105-121.
Onwuegbuzie, A. J. and Teddlie, C. 2003, "A Framework for Analyzing Data in Mixed Methods Research", *Handbook of mixed methods in social and behavioral research*, Vol. 2 No. 397-430.
Ortega, S. T. and Myles, J. L. 1987, "Race and Gender Effects on Fear of Crime: An Interactive Model with Age", *Criminology*, Vol. 25 No. 1**,** pp. 133-152.
Osborne, J. W. 2014, *Best Practices in Logistic Regression*, Sage Publications.
Osgood, D. W., Wilson, J. K., O'malley, P. M., Bachman, J. G. and Johnston, L. D. 1996, "Routine Activities and Individual Deviant Behavior", *American Sociological Review*, Vol. No. 635-655.
Oxley, A. 2011, *A Best Practices Guide for Mitigating Risk in the Use of Social Media*, IBM Center for the Business of Government.
Padgett, D. K. 2016, *Qualitative Methods in Social Work Research*, Sage Publications.
Paek, S. Y. and Nalla, M. K. 2015, "The Relationship between Receiving Phishing Attempt and Identity Theft Victimization in South Korea", *International Journal of Law, Crime and Justice*, Vol. 43 No. 4**,** pp. 626-642.
Pain, R. 2001, "Gender, Race, Age and Fear in the City", *Urban studies*, Vol. 38 No. 5-6**,** pp. 899-913.
Palmer, D. 2017, "1.4 Million Phishing Websites Are Created Every Month: Here's Who the Scammers Are Pretending to Be. available at: https://www.zdnet.com/article/1-4-million-phishing-websites-are-created-every-month-heres-who-the-scammers-are-pretending-to-be/ (accessed 10/10/2018).
Pamphlet, T. 2010, "Cyberspace Operations Concept Capability Plan", Vol. No.
Pamplin, B. A. 2014. *Virtual Currencies and the Implications for Us Anti-Money Laundering Regulations.* Utica College.
Panwar, A. 2014, "Cyber Crime through Social Engineering", Vol. No.
Papantoniou, M. 2017, "Economic Fraud Crimes on the Internet: Development of New 'Weapons' and Strategies to Annihilate the Danger", *Eu Internet Law*, Springer. pp. 407-433.
Pappas, N. 2016, "Marketing Strategies, Perceived Risks, and Consumer Trust in Online Buying Behaviour", *Journal of Retailing and Consumer Services*, Vol. 29 No. 92-103.
Park, G. and Taylor, J. M. 2015, "Using Syntactic Features for Phishing Detection", *arXiv preprint arXiv:1506.00037*, Vol. No.
Park, H., Choi, S. and Chae, H. (2018), "Analysis of Sns Activity as Leisure Consumption-Focused on the Sns Market Activity of Women Consumers of the Twenties to Thirties", paper presented at the *2018 Global Marketing Conference at Tokyo*,2018, avaialable at.
Parris, L., Varjas, K., Meyers, J. and Cutts, H. 2012, "High School Students' Perceptions of Coping with Cyberbullying", *Youth & Society*, Vol. 44 No. 2**,** pp. 284-306.
Parrish Jr, J. L., Bailey, J. L. and Courtney, J. F. 2009, "A Personality Based Model for Determining Susceptibility to Phishing Attacks", *Little Rock: University of Arkansas*, Vol. No.
Pathak, P. 2016a, "Cybercrime: A Global Threat to Cybercommunity", *International Journal of Computer Science & Engineering Technology (IJCSET)*, Vol. 7 No. 3**,** pp. 46-49.
Pathak, P. 2016b, "The Review of Terms and Concepts Used to Understand Cybercrime to Safeguard Ourselves from Cybercriminals", *International Journal of Advanced Research in Computer Science*, Vol. 7 No. 1**,** pp.
Patton, M. Q. 1990, *Qualitative Evaluation and Research Methods*, SAGE Publications, inc.
Patton, M. Q. 2002, *Qualitative Research and Evaluation Methods* Thousand Oaks, Calif.: Sage.
Patzer, G. L. 1995, *Using Secondary Data in Marketing Research: United States and Worldwide*, Greenwood Publishing Group.
Pauwels, L. J. and Svensson, R. 2011, "Exploring the Relationship between Offending and Victimization: What Is the Role of Risky Lifestyles and Low Self-Control? A Test in Two Urban Samples", *European journal on criminal policy and research*, Vol. 17 No. 3**,** pp. 163-177.
Payton, M. E., Greenstone, M. H. and Schenker, N. 2003, "Overlapping Confidence Intervals or Standard Error Intervals: What Do They Mean in Terms of Statistical Significance?", *Journal of Insect Science*, Vol. 3 No. 1**,** pp. 34.

Pease, K. 2001, "Crime Futures and Foresight: Challenging Criminal Behaviour in the Information Age", in: Wall, D. S. (ed.) *Crime and the Internet*, Routledge, Newyork. pp.
Peguero, A. A. and Popp, A. M. 2012, "Youth Violence at School and the Intersection of Gender, Race, and Ethnicity", *Journal of Criminal Justice*, Vol. 40 No. 1**,** pp. 1-9.
Penny, L., Chew, W., Raja, R. and Lim, H. 2016, "Online Shopping Preference and M-Payment Acceptance: A Case Study among Klang Valley Online Shoppers", *Pertanika Journal of Social Sciences & Humanities*, Vol. 24 No. 3**,** pp.
Penrod, J., Preston, D. B., Cain, R. E. and Starks, M. T. 2003, "A Discussion of Chain Referral as a Method of Sampling Hard-to-Reach Populations", *Journal of Transcultural nursing*, Vol. 14 No. 2**,** pp. 100-107.
Pereira, F. and Matos, M. 2016, "Cyber-Stalking Victimization: What Predicts Fear among Portuguese Adolescents?", *European Journal on Criminal Policy and Research*, Vol. 22 No. 2**,** pp. 253-270.
Pereira, F., Spitzberg, B. H. and Matos, M. 2016, "Cyber-Harassment Victimization in Portugal: Prevalence, Fear and Help-Seeking among Adolescents", *Computers in Human Behavior*, Vol. 62 No. 136-146.
Perrin, R. D. 2001, "When Religion Becomes Deviance: Introducing Religion in Deviance and Social Problems Courses", *Teaching sociology*, Vol. No. 134-152.
Peterson, B. D., Pirritano, M., Block, J. M. and Schmidt, L. 2011, "Marital Benefit and Coping Strategies in Men and Women Undergoing Unsuccessful Fertility Treatments over a 5-Year Period", *Fertility and sterility*, Vol. 95 No. 5**,** pp. 1759-1763. e1.
Petter, S. C. and Gallivan, M. J. (2004), "Toward a Framework for Classifying and Guiding Mixed Method Research in Information Systems", paper presented at the *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*,2004, avaialable at.
Phillips, L. 2000, *Flirting with Danger: Young Women's Reflections on Sexuality and Domination*, NYU Press.
Phuanukoonnon, S., Brough, M. and Bryan, J. H. 2006, "Folk Knowledge About Dengue Mosquitoes and Contributions of Health Belief Model in Dengue Control Promotion in Northeast Thailand", *Acta tropica*, Vol. 99 No. 1**,** pp. 6-14.
Pikkarainen, T., Pikkarainen, K., Karjaluoto, H. and Pahnila, S. 2004, "Consumer Acceptance of Online Banking: An Extension of the Technology Acceptance Model", *Internet research*, Vol. 14 No. 3**,** pp. 224-235.
Piko, B. 2001, "Gender Differences and Similarities in Adolescents' Ways of Coping", *The Psychological Record*, Vol. 51 No. 2**,** pp. 223-235.
Piquero, N. L., Carmichael, S. and Piquero, A. R. 2007, "Research Note: Assessing the Perceived Seriousness of White-Collar and Street Crimes", *Crime & Delinquency*, Vol. No.
Pitney, W. A. and Parker, J. 2009, *Qualitative Research in Physical Activity and the Health Professions*, Human Kinetics Champaign, IL.
Pituch, K. A. and Stevens, J. P. 2016, *Applied Multivariate Statistics for the Social Sciences: Analyses with Sas and Ibm's Spss*, Routledge.
Polgar, S. and Thomas, S. A. 2011, *Introduction to Research in the Health Sciences E-Book*, Elsevier Health Sciences.
Policastro, C. and Payne, B. 2014, "Can You Hear Me Now? Telemarketing Fraud Victimization and Lifestyles", *The Journal of the Southern Criminal Justice Association*, Vol. 40 No. 3**,** pp. 620-638.
Pollacia, L., Ding, Y. Z. and Yang, S. (2014), "Why Phishing Works: Project for an Information Security Capstone Course", paper presented at the *Proceedings of the Information Systems Educators Conference ISSN*,2014, avaialable at.
Ponemon Institute. 2016, "Mobile Risk Is a Real Number", available at: https://www.lookout.com/enterprise-mobile-risk (accessed 17/11/2016).
Pontell, H. N. and Geis, G. 2007, "New Times, New Crimes:"Blocking" Financial Identity Fraud", *The Organized Crime Community*, Springer. pp. 45-58.
Poulter, S. 2017, "Gumtree Is Hit by 250 Fraud Claims a Week: Consumers Warned Criminals Are Using the Small Ads Site to Steal Millions. available at: http://www.dailymail.co.uk/news/article-2678728/Gumtree-hit-250-fraud-claims-week-Consumers-warned-criminals-using-small-ads-site-steal-millions.html (accessed 05/12/2017).
Power, A., Barton, H. and O'hagan, L. 2018, "Cybertrends: An Exploratory Study of Why Individuals Conform on Social Networking Sites", *Cyberpsychology and Society*, Routledge. pp. 79-89.
Pratt, T., Holtfreter, K. and Reisig, M. 2010, "Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory", *The Journal of Research in Crime and Delinquency*, Vol. 47 No. 3**,** pp. 267.
Pratt, T. C. and Turanovic, J. J. 2016, "Lifestyle and Routine Activity Theories Revisited: The Importance of "Risk" to the Study of Victimization", *Victims & Offenders*, Vol. 11 No. 3**,** pp. 335-354.
Prensky, M. 2001, "Digital Natives, Digital Immigrants Part 1", *On the horizon*, Vol. 9 No. 5**,** pp. 1-6.
Prentice-Dunn, S. and Rogers, R. W. 1986, "Protection Motivation Theory and Preventive Health: Beyond the Health Belief Model", *Health education research*, Vol. 1 No. 3**,** pp. 153-161.

Price, M. and Dalgleish, J. 2010, "Cyberbullying: Experiences, Impacts and Coping Strategies as Described by Australian Young People", *Youth Studies Australia*, Vol. 29 No. 2**,** pp. 51.
Price, R. 2017. *New Report: Apple's Mac Is No Longer Virus-Free*. *Business Insider* [Online]. Available from: https://www.inc.com/business-insider/malware-macs-apple-744-2016.html [Accessed 25/07/2017 2017].
Purkait, S. 2012, "Phishing Counter Measures and Their Effectiveness–Literature Review", *Information Management & Computer Security*, Vol. 20 No. 5**,** pp. 382-420.
Pursiainen, E. 2016, "Co-Creating an Engaging Live-Streamed Concert with Potential Viewers", Vol. No.
Qi, M. and Yang, C. (2006), "Research and Design of Phishing Alarm System at Client Terminal", paper presented at the *Services Computing, 2006. APSCC'06. IEEE Asia-Pacific Conference on*,2006, avaialable at.
Quick, M., Li, G. and Law, J. 2018, "Spatiotemporal Modeling of Correlated Small-Area Outcomes: Analyzing the Shared and Type-Specific Patterns of Crime and Disorder", *Geographical Analysis*, Vol. No.
Quinney, R. 1972, "Who Is the Victim", *Criminology*, Vol. 10 No. 314.
Rachman, S. 1976, "The Passing of the Two-Stage Theory of Fear and Avoidance: Fresh Possibilities", *Behaviour Research and Therapy*, Vol. 14 No. 2**,** pp. 125-131.
Rader, N. E. 2004, "The Threat of Victimization: A Theoretical Reconceptualization of Fear of Crime", *Sociological Spectrum*, Vol. 24 No. 6**,** pp. 689-704.
Rader, N. E. and Haynes, S. H. 2011, "Gendered Fear of Crime Socialization: An Extension of Akers's Social Learning Theory", *Feminist Criminology*, Vol. 6 No. 4**,** pp. 291-307.
Rader, N. E., May, D. C. and Goodrum, S. 2007, "An Empirical Assessment of the "Threat of Victimization:" Considering Fear of Crime, Perceived Risk, Avoidance, and Defensive Behaviors", *Sociological Spectrum*, Vol. 27 No. 5**,** pp. 475-505.
Rafique, M. Z., Van Goethem, T., Joosen, W., Huygens, C. and Nikiforakis, N. (2016), "It's Free for a Reason: Exploring the Ecosystem of Free Live Streaming Services", paper presented at the *Proceedings of the 23rd Network and Distributed System Security Symposium (NDSS 2016)*,2016, avaialable at.
Rait, M. A., Prochaska, J. J. and Rubinstein, M. L. 2015, "Recruitment of Adolescents for a Smoking Study: Use of Traditional Strategies and Social Media", *Translational behavioral medicine*, Vol. 5 No. 3**,** pp. 254-259.
Ramirez Jr, A. and Bryant, E. M. 2014, "Relational Reconnection on Social Network Sites: An Examination of Relationship Persistence and Modality Switching", *Communication Reports*, Vol. 27 No. 1**,** pp. 1-12.
Ramo, D. E. and Prochaska, J. J. 2012, "Broad Reach and Targeted Recruitment Using Facebook for an Online Survey of Young Adult Substance Use", *Journal of medical Internet research*, Vol. 14 No. 1**,** pp.
Randa, R. 2013, "The Influence of the Cyber-Social Environment on Fear of Victimization: Cyberbullying and School", *Security Journal*, Vol. 26 No. 4**,** pp. 331-348.
Randall, A. 2011, "Beneficial Inteview Effects in Virtual Worlds: A Case Study", in: Salmons, J. (ed.) *Cases in Online Interview Research*, Sage Publications. pp.
Rao, C. C., Ramana, A. and Sowmya, B. 2018, "Detection of Phishing Websites Using Hybrid Model", *GPH-Journal Of Computer Science and Engineering*, Vol. 1 No. 1**,** pp. 15-22.
Raven, G. 2006, "Methodological Reflexivity: Towards Evolving Methodological Frameworks through Critical and Reflexive Deliberations", *Environmental Education Research*, Vol. 12 No. 3-4**,** pp. 559-569.
Ravenscroft, N. 2004, "Tales from the Tracks: Discourses of Constraint in the Use of Mixed Cycle and Walking Routes", *International review for the sociology of sport*, Vol. 39 No. 1**,** pp. 27-44.
Raworth, K., Sweetman, C., Narayan, S., Rowlands, J. and Hopkins, A. 2012, *Conducting Semi-Structured Interviews*, Oxfam.
Ray, A. and Kaushik, A. 2017, "State Transgression on Electronic Expression: Is It for Real?", *Information & Computer Security*, Vol. 25 No. 4**,** pp. 382-401.
Rees, C. 2011, *An Introduction to Research for Midwives E-Book*, Elsevier Health Sciences.
Rege, A. 2009, "What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud", *International Journal of Cyber Criminology*, Vol. 3 No. 2**,** pp. 494-512.
Reisig, M. D. and Holtfreter, K. 2013, "Shopping Fraud Victimization among the Elderly", *Journal of Financial Crime*, Vol. 20 No. 3**,** pp. 324-337.
Reisig, M. D., Pratt, T. C. and Holtfreter, K. 2009, "Perceived Risk of Internet Theft Victimization", *Criminal Justice and Behavior*, Vol. 36 No. 4**,** pp. 369-384.
Rengifo, A. F. and Bolton, A. 2012, "Routine Activities and Fear of Crime: Specifying Individual-Level Mechanisms", *European Journal of Criminology*, Vol. 9 No. 2**,** pp. 99-119.
Reurink, A. 2016, "Financial Fraud: A Literature Review": MPIfG Discussion Paper, (accessed.
Reynolds, S. 2003, Should There Be a New Language of Widening Participation. SCUTREA.
Reyns, B. W. 2013, "Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory Beyond Direct-Contact Offenses", *Journal of research in crime and delinquency*, Vol. 50 No. 2**,** pp. 216-238.

Reyns, B. W. 2015, "A Routine Activity Perspective on Online Victimisation: Results from the Canadian General Social Survey", *Journal of Financial Crime*, Vol. 22 No. 4**,** pp. 396-411.
Reyns, B. W. and Henson, B. 2016, "The Thief with a Thousand Faces and the Victim with None: Identifying Determinants for Online Identity Theft Victimization with Routine Activity Theory", *International Journal of Offender Therapy and Comparative Criminology*, Vol. 60 No. 10**,** pp. 1119-1139.
Reyns, B. W., Henson, B. and Fisher, B. S. 2011, "Being Pursued Online", *Criminal Justice and Behavior*, Vol. 38 No. 11**,** pp. 1149-1169.
Reyns, B. W., Henson, B. and Fisher, B. S. 2014, "Digital Deviance: Low Self-Control and Opportunity as Explanations of Sexting among College Students", *Sociological Spectrum*, Vol. 34 No. 3**,** pp. 273-292.
Reyns, B. W., Henson, B. and Fisher, B. S. 2015, "Guardians of the Cyber Galaxy an Empirical and Theoretical Analysis of the Guardianship Concept from Routine Activity Theory as It Applies to Online Forms of Victimization", *Journal of Contemporary Criminal Justice*, Vol. No. 1043986215621378.
Reyns, B. W., Henson, B., Fisher, B. S., Fox, K. A. and Nobles, M. R. 2016, "A Gendered Lifestyle-Routine Activity Approach to Explaining Stalking Victimization in Canada", *Journal of interpersonal violence*, Vol. 31 No. 9**,** pp. 1719-1743.
Riek, M., Bohme, R. and Moore, T. 2016, "Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance", *IEEE Transactions on Dependable and Secure Computing*, Vol. 13 No. 2**,** pp. 261-273.
Riek, M., Böhme, R. and Moore, T. (2014), "Understanding the Influence of Cybercrime Risk on the E-Service Adoption of European Internet Users", paper presented at the *Proceedings of the 13th Workshop on the Economics of Information Security (WEIS)*,2014, avaialable at.
Riger, S., Gordon, M. T. and Lebailly, R. K. 1982, "Coping with Urban Crime: Women's Use of Precautionary Behaviors", *American Journal of Community Psychology*, Vol. 10 No. 4**,** pp. 369-386.
Rijnetu, I. 2018, "13+ Warning Signs That Your Computer Is Malware-Infected. available at: https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/ (accessed 11/11/2018).
Ritchie, J., Lewis, J., Nicholls, C. M. and Ormston, R. 2013, *Qualitative Research Practice: A Guide for Social Science Students and Researchers*, Sage.
Ritland, R. and Rodriguez, L. 2014, "The Influence of Antiobesity Media Content on Intention to Eat Healthily and Exercise: A Test of the Ordered Protection Motivation Theory", *Journal of obesity*, Vol. 2014 No.
Roberts, L. D., Indermaur, D. and Spiranovic, C. 2013, "Fear of Cyber-Identity Theft and Related Fraudulent Activity", *Psychiatry, Psychology and Law*, Vol. 20 No. 3**,** pp. 315-328.
Roberts, R., Sanders, T., Myers, E. and Smith, D. 2010, "Participation in Sex Work: Students' Views", *Sex Education*, Vol. 10 No. 2**,** pp. 145-156.
Robinson, M. B. and Robinson, C. E. 1997, "Environmental Characteristics Associated with Residential Burglaries of Student Apartment Complexes", *Environment and Behavior*, Vol. 29 No. 5**,** pp. 657-675.
Robinson, O. C. 2014, "Sampling in Interview-Based Qualitative Research: A Theoretical and Practical Guide", *Qualitative research in psychology*, Vol. 11 No. 1**,** pp. 25-41.
Rocco, T., Bliss, L., Gallagher, S. G. S., Pérez, A. P. A. and Prado, P. 2003, "Taking the Next Step: Mixed Methods Taking the Next Step: Mixed Methods Research in Organizational Systems Research in Organizational Systems", *Information Technology, Learning, and Performance Journal*, Vol. 21 No. 1**,** pp. 19.
Rogers, R. W. 1975, "A Protection Motivation Theory of Fear Appeals and Attitude Change", *The journal of psychology*, Vol. 91 No. 1**,** pp. 93-114.
Rogers, R. W. 1983, "Cognitive and Psychological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation", *Social psychophysiology: A sourcebook*, Vol. No. 153-176.
Rosenbaum, D. P. 1988, "Community Crime Prevention: A Review and Synthesis of the Literature", *Justice Quarterly*, Vol. 5 No. 3**,** pp. 323-395.
Rosenblum, S. and Louis, K. 1981, "Stability and Change", *Journal Innovation in an Educational Context*, Vol. No.
Rosenthal, G. and Rosenthal, J. A. 2011, *Statistics and Data Interpretation for Social Work*, Springer Publishing Company.
Rossman, G. B. and Wilson, B. L. 1985, "Numbers and Words: Combining Quantitative and Qualitative Methods in a Single Large-Scale Evaluation Study", *Evaluation review*, Vol. 9 No. 5**,** pp. 627-643.
Roth, S. and Cohen, L. J. 1986, "Approach, Avoidance, and Coping with Stress", *American psychologist*, Vol. 41 No. 7**,** pp. 813.
Roughead, E. E., Harvey, K. J. and Gilbert, A. L. 1998, "Commercial Detailing Techniques Used by Pharmaceutical Representatives to Influence Prescribing", *Internal Medicine Journal*, Vol. 28 No. 3**,** pp. 306-310.

Rountree, P. W. and Clayton, R. R. 1999, "A Contextual Model of Adolescent Alcohol Use across the Rural-Urban Continuum", *Substance use & misuse*, Vol. 34 No. 4-5**,** pp. 495-519.
Rountree, P. W. and Land, K. C. 1996, "Perceived Risk Versus Fear of Crime: Empirical Evidence of Conceptually Distinct Reactions in Survey Data", *Social forces*, Vol. 74 No. 4**,** pp. 1353-1376.
Rountree, P. W., Land, K. C. and Miethe, T. D. 1994, "Macro-Micro Integration in the Study of Victimization: A Hierarchical Logistic Model Analysis across Seattle Neighborhoods", *Criminology*, Vol. 32 No. 3**,** pp. 387-414.
Rousseau, G. and Rogers, W. 1998, "Computer Usage Patterns of University Faculty Members across the Life Span", *Computers in Human Behavior*, Vol. 14 No. 3**,** pp. 417-428.
Rowstron, A. and Druschel, P. (2001), "Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems", paper presented at the *IFIP/ACM International Conference on Distributed Systems Platforms and Open Distributed Processing*,2001, avaialable at.
Ruben, A. and Babbie, E. 2009, "Essential Research Methods for Social Work", *Belmont: Brook/Cole Cengage Learning*, Vol. No.
Russo, R. 2004, *Statistics for the Behavioural Sciences: An Introduction*, Psychology Press.
Russo, S. and Roccato, M. 2010, "How Long Does Victimization Foster Fear of Crime? A Longitudinal Study", *Journal of Community Psychology*, Vol. 38 No. 8**,** pp. 960-974.
Rutledge, D. N. 1987, "Factors Related to Women's Practice of Breast Self-Examination", *Nursing Research*, Vol. 36 No. 2**,** pp. 117-121.
Ryan, T. P. 2013, *Sample Size Determination and Power*, John Wiley & Sons.
Ryder, H., Maltby, J., Rai, L., Jones, P. and Flowe, H. D. 2016, "Women's Fear of Crime and Preference for Formidable Mates: How Specific Are the Underlying Psychological Mechanisms?", *Evolution and Human Behavior*, Vol. 37 No. 4**,** pp. 293-302.
Sacco, V. F. and Kennedy, L. W. 2010, *The Criminal Event: An Introduction to Criminology in Canada*, Cengage Learning.
Sadler, G. R., Lee, H. C., Lim, R. S. H. and Fullerton, J. 2010, "Recruitment of Hard-to-Reach Population Subgroups Via Adaptations of the Snowball Sampling Strategy", *Nursing & health sciences*, Vol. 12 No. 3**,** pp. 369-374.
Saldaña, J. 2015, *The Coding Manual for Qualitative Researchers*, Sage.
Salleh, N., Hussein, R., Mohamed, N. and Aditiawarman, U. (2013), "An Empirical Study of the Factors Influencing Information Disclosure Behaviour in Social Networking Sites", paper presented at the *Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on*,2013, avaialable at.
Salmons, J. 2017, "Using Social Media in Data Collection: Designing Studies with the Qualitative E-Research Framework", in: Sloan, L. and Quan-Haase, A. (eds.), *The Sage Handbook of Social Media Research Methods*, Sage. pp.
Salston, M. and Figley, C. R. 2003, "Secondary Traumatic Stress Effects of Working with Survivors of Criminal Victimization", *Journal of traumatic stress*, Vol. 16 No. 2**,** pp. 167-174.
Sampson, R. J. 1987, "Personal Violence by Strangers: An Extension and Test of the Opportunity Model of Predatory Victimization", *J. Crim. L. & Criminology*, Vol. 78 No. 327.
Sampson, R. J. and Lauritsen, J. L. 1990, "Deviant Lifestyles, Proximity to Crime, and the Offender-Victim Link in Personal Violence", *Journal of research in crime and delinquency*, Vol. 27 No. 2**,** pp. 110-139.
Sampson, R. J. and Wooldredge, J. D. 1987, "Linking the Micro-and Macro-Level Dimensions of Lifestyle-Routine Activity and Opportunity Models of Predatory Victimization", *Journal of Quantitative Criminology*, Vol. 3 No. 4**,** pp. 371-393.
Sandelowski, M. 1995, "Sample Size in Qualitative Research", *Research in nursing & health*, Vol. 18 No. 2**,** pp. 179-183.
Sanders, T., Scoular, J., Campbell, R., Pitcher, J. and Cunningham, S. 2018, "Introduction: Technology, Social Change and Commercial Sex Online", *Internet Sex Work*, Springer. pp. 1-21.
Saqib, N. U. and Chan, E. Y. 2015, "Time Pressure Reverses Risk Preferences", *Organizational Behavior and Human Decision Processes*, Vol. 130 No. 58-68.
Sarno, D. M., Lewis, J. E., Bohil, C. J., Shoss, M. K. and Neider, M. B. (2017), "Who Are Phishers Luring?: A Demographic Analysis of Those Susceptible to Fake Emails", paper presented at the *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*,2017, avaialable at.
Sasse, S. 2005, "“Motivation” and Routine Activities Theory", *Deviant Behavior*, Vol. 26 No. 6**,** pp. 547-570.
Sato, D., Kobayashi, M., Takagi, H., Asakawa, C. and Tanaka, J. (2011), "How Voice Augmentation Supports Elderly Web Users", paper presented at the *The proceedings of the 13th international ACM SIGACCESS conference on Computers and accessibility*,2011, avaialable at.

Saunders, K. M. and Zucker, B. 1999, "Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act", *International Review of Law, Computers & Technology*, Vol. 13 No. 2**,** pp. 183-192.
Savage, M., Devine, F., Cunningham, N., Taylor, M., Li, Y., Hjellbrekke, J., Le Roux, B., Friedman, S. and Miles, A. 2013, "A New Model of Social Class? Findings from the Bbc's Great British Class Survey Experiment", *Sociology*, Vol. 47 No. 2**,** pp. 219-250.
Savage, N. 2016, "The Myth of Anonymity", *Nature*, Vol. 537 No. 7619**,** pp. S70-S72.
Scarpa, A., Haden, S. C. and Hurley, J. 2006, "Community Violence Victimization and Symptoms of Posttraumatic Stress Disorder: The Moderating Effects of Coping and Social Support", *Journal of Interpersonal Violence*, Vol. 21 No. 4**,** pp. 446-469.
Schafer, J. A., Huebner, B. M. and Bynum, T. S. 2006, "Fear of Crime and Criminal Victimization: Gender-Based Contrasts", *Journal of Criminal Justice*, Vol. 34 No. 3**,** pp. 285-301.
Schafer, S. 1968, *The Victim and His Criminal: A Study in Functional Responsibility*, Random House New York.
Schilling, J. 2006, "On the Pragmatics of Qualitative Assessment", *European journal of psychological assessment*, Vol. 22 No. 1**,** pp. 28-37.
Schmidt, L., Holstein, B. E., Christensen, U. and Boivin, J. 2005, "Communication and Coping as Predictors of Fertility Problem Stress: Cohort Study of 816 Participants Who Did Not Achieve a Delivery after 12 Months of Fertility Treatment", *Human reproduction*, Vol. 20 No. 11**,** pp. 3248-3256.
Schneider, G. P. 2011, *E-Business*, Cengage Learning.
Schneider, Z. and Whitehead, D. 2013, *Nursing and Midwifery Research: Methods and Appraisal for Evidence-Based Practice*, Elsevier Australia.
Schuetz, S., Lowry, P. B. and Thatcher, J. 2016, "Defending against Spear-Phishing: Motivating Users through Fear Appeal Manipulations", Vol. No.
Schutten, D., Stokes, K. A. and Arnell, K. M. 2017, "I Want to Media Multitask and I Want to Do It Now: Individual Differences in Media Multitasking Predict Delay of Gratification and System-1 Thinking", *Cognitive research: principles and implications*, Vol. 2 No. 1**,** pp. 8.
Schwarz, N. 2000, "Emotion, Cognition, and Decision Making", *Cognition & Emotion*, Vol. 14 No. 4**,** pp. 433-440.
Scotia, N. 2010, "Explaining Odds Ratios", *J Can Acad Child Adolesc Psychiatry*, Vol. 19 No. 227.
Scurlock-Evans, L. and Mahoney, B. 2016, "Using the Crime Survey for England and Wales to Research Sexuality and Criminal Victimisation Experiences: A Magic Bullet for Exploring Sensitive Topics?", *Also in this issue: Doing research in LGBT*, Vol. No. 54-59.
Seals, T. 2017, "Phishing Awareness Grows, but Volumes Increase. available at: https://www.infosecurity-magazine.com/news/phishing-awareness-grows-but/ (accessed 18/09/2017).
Seda, L. 2014, "Identity Theft and University Students: Do They Know, Do They Care?", *Journal of Financial Crime*, Vol. 21 No. 4**,** pp. 461-483.
See-To, E. W., Papagiannidis, S. and Westland, J. C. 2014, "The Moderating Role of Income on Consumers' Preferences and Usage for Online and Offline Payment Methods", *Electronic Commerce Research*, Vol. 14 No. 2**,** pp. 189-213.
Seidman, G. 2013a, "Self-Presentation and Belonging on Facebook: How Personality Influences Social Media Use and Motivations", *Personality and Individual Differences*, Vol. 54 No. 3**,** pp. 402-407.
Seidman, I. 2013b, *Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences*, Teachers college press.
Sekaran, U. and Bougie, R. 2016, *Research Methods for Business: A Skill Building Approach*, John Wiley & Sons.
Sen, R. and Borle, S. 2015, "Estimating the Contextual Risk of Data Breach: An Empirical Approach", *Journal of Management Information Systems*, Vol. 32 No. 2**,** pp. 314-341.
Sendo, M. R., Sherman, R. S. and Kaltwasser, J. C. 2005, Methods and Apparatus for Conducting Secure, Online Monetary Transactions. Google Patents.
Sengupta, A. and Chaudhuri, A. 2011, "Are Social Networking Sites a Source of Online Harassment for Teens? Evidence from Survey Data", *Children and Youth Services Review*, Vol. 33 No. 2**,** pp. 284-290.
Serfaty, M., Ridgewell, A., Drennan, V., Kessel, A., Brewin, C. R., Wright, A., Laycock, G. and Blanchard, M. 2016, "Helping Aged Victims of Crime (the Havoc Study): Common Crime, Older People and Mental Illness", *Behavioural and cognitive psychotherapy*, Vol. 44 No. 2**,** pp. 140-155.
Shaghaghi, A., Bhopal, R. S. and Sheikh, A. 2011, "Approaches to Recruiting 'Hard-to-Reach'populations into Research: A Review of the Literature", *Health Promotion Perspectives*, Vol. 1 No. 2**,** pp. 86.
Shahzad, R. K. and Lavesson, N. 2011, *Detecting Scareware by Mining Variable Length Instruction Sequences*, IEEE.
Shapira, N. A., Lessig, M. C., Goldsmith, T. D., Szabo, S. T., Lazoritz, M., Gold, M. S. and Stein, D. J. 2003, "Problematic Internet Use: Proposed Classification and Diagnostic Criteria", *Depression and anxiety*, Vol. 17 No. 4**,** pp. 207-216.

Sharma, K. 2010, "An Anatomy of Phishing Messages as Deceiving Persuasion: A Categorical Content and Semantic Network Study", *EDPACS*, Vol. 42 No. 6**,** pp. 1-19.
Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F. and Downs, J. (2010), "Who Falls for Phish?: A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions", paper presented at the *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*,2010, avaialable at.
Sheng, S., Wardman, B., Warner, G., Cranor, L. F., Hong, J. and Zhang, C. (2009), "An Empirical Analysis of Phishing Blacklists", paper presented at the *Proceedings of Sixth Conference on Email and Anti-Spam (CEAS)*,2009, avaialable at.
Shenton, A. K. 2004, "Strategies for Ensuring Trustworthiness in Qualitative Research Projects", *Education for information*, Vol. 22 No. 2**,** pp. 63-75.
Sherman, L. W., Gartin, P. R. and Buerger, M. E. 1989, "Hot Spots of Predatory Crime: Routine Activities and the Criminology of Place", *Criminology*, Vol. 27 No. 1**,** pp. 27-56.
Sherman, L. W. and Weisburd, D. 1995, "Does Patrol Prevent Crime? The Minneapolis Hot Spots Experiment", *Miyazawa, Koichi; Miyazawa, Setsuo (Hg.)*, Vol. No. 87-94.
Shi, J., Hu, P., Lai, K. K. and Chen, G. 2018, "Determinants of Users' Information Dissemination Behavior on Social Networking Sites: An Elaboration Likelihood Model Perspective", *Internet Research*, Vol. 28 No. 2**,** pp. 393-418.
Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., Larose, R. and Rifon, N. J. 2015, "Online Safety Begins with You and Me: Convincing Internet Users to Protect Themselves", *Computers in Human Behavior*, Vol. 48 No. 199-207.
Shimmen, J. 2011. *Teaching Methods Used in Undergraduate Dance Technique Classes and the Students' Response.* University of Wales.
Short, E., Guppy, A., Hart, J. A. and Barnes, J. 2015, "The Impact of Cyberstalking", *Studies in Media and Communication*, Vol. 3 No. 2**,** pp. 23-37.
Siegel, K., Anderman, S. J. and Schrimshaw, E. W. 2001, "Religion and Coping with Health-Related Stress", *Psychology and Health*, Vol. 16 No. 6**,** pp. 631-653.
Sihvonen, J. and Turunen, L. L. M. 2016, "As Good as New–Valuing Fashion Brands in the Online Second-Hand Markets", *Journal of Product & Brand Management*, Vol. 25 No. 3**,** pp. 285-295.
Silic, M. and Back, A. 2016, "The Dark Side of Social Networking Sites: Understanding Phishing Risks", *Computers in Human Behavior*, Vol. 60 No. 35-43.
Silverman, R. A. and Kennedy, L. W. 1985, "Loneliness, Satisfaction and Fear of Crime: A Test for Non-Recursive Effects", *Canadian J. Criminology*, Vol. 27 No. 1.
Simkiss, D., Edmond, K., Bose, A., Troy, S. and Bassat, Q. 2015. *Research Methods Ii: Multivariate Analysis: Analysing Categorical Data: Log-Linear Analysis* Journal of Tropical Pediatrics. [Online]. Available: http://www.oxfordjournals.org/our_journals/tropej/online/ma.html.
Sinacore, A. L., Jaghori, B. and Rezazadeh, S. M. 2015, "Female University Students Working in the Sex Trade: A Narrative Analysis", *Canadian Journal of Counselling and Psychotherapy/Revue canadienne de counseling et de psychothérapie*, Vol. 49 No. 1**,** pp.
Singh, K. 2007, *Quantitative Social Research Methods*, Sage.
Sironi, E. and Bonazzi, L. M. 2016, "Direct Victimization Experiences and Fear of Crime: A Gender Perspective", *Peace Economics, Peace Science and Public Policy*, Vol. 22 No. 2**,** pp. 159-172.
Skogan, W. 1986, "Fear of Crime and Neighborhood Change", *Crime and justice*, Vol. 8 No. 203-229.
Skogan, W. G. and Maxfield, M. G. 1981, *Coping with Crime: Individual and Neighborhood Reactions*, Sage Publications Beverly Hills, CA.
Skroupa, C. P. 2017, "Shareholders Sue Companies for Lying About Cyber Security. available at: https://www.forbes.com/sites/christopherskroupa/2016/10/27/exposing-litigation-the-hidden-risks-of-cyber-breach/#2f49893831a1 (accessed 24/11/2017).
Šléglová, V. and Cerna, A. 2011, "Cyberbullying in Adolescent Victims: Perception and Coping", *Cyberpsychology: journal of psychosocial research on cyberspace*, Vol. 5 No. 2**,** pp.
Smit, E. G., Van Noort, G. and Voorveld, H. A. 2014, "Understanding Online Behavioural Advertising: User Knowledge, Privacy Concerns and Online Coping Behaviour in Europe", *Computers in Human Behavior*, Vol. 32 No. 15-22.
Smith, E. 2008, "Pitfalls and Promises: The Use of Secondary Data Analysis in Educational Research", *British Journal of Educational Studies*, Vol. 56 No. 3**,** pp. 323-339.
Smith, J. K. 1983, "Quantitative Versus Qualitative Research: An Attempt to Clarify the Issue", *Educational researcher*, Vol. 12 No. 3**,** pp. 6-13.
Smith, L. N. and Hill, G. D. 1991, "Victimization and Fear of Crime", *Criminal justice and behavior*, Vol. 18 No. 2**,** pp. 217-239.

Smith, R. 2010, "Identity Theft and Fraud", in: Jewkes, Y. and Yar, M. (eds.), *Handbook of Internet Crime*. pp. 273-301.
Smith, S. J. 1984, "Crime and the Structure of Social Relations", *Transactions of the Institute of British Geographers*, Vol. No. 427-442.
Snedker, K. A. 2015, "Neighborhood Conditions and Fear of Crime: A Reconsideration of Sex Differences", *Crime & Delinquency*, Vol. 61 No. 1**,** pp. 45-70.
Soghoian, C. (2008), "Legal Risks for Phishing Researchers", paper presented at the *2008 eCrime Researchers Summit*,2008, avaialable at.
Soltani, S., Seno, S. a. H., Nezhadkamali, M. and Budiarto, R. 2014, "A Survey on Real World Botnets and Detection Mechanisms", *International Journal of Information and Network Security*, Vol. 3 No. 2**,** pp. 116.
Sood, A. K. and Enbody, R. 2011, "Chain Exploitation—Social Networks Malware", *ISACA Journal*, Vol. 1 No. 31.
Sood, A. K. and Enbody, R. J. 2013, "Targeted Cyberattacks: A Superset of Advanced Persistent Threats", *IEEE security & privacy*, Vol. 11 No. 1**,** pp. 54-61.
South, P. 2015, "Illegal Football Streams War Shows No Sign of Ending for Premier League. available at: https://www.givemesport.com/539759-illegal-football-streams-war-shows-no-sign-of-ending-for-premier-league (accessed 02/03/2019).
Spalek, B. 2016, *Crime Victims: Theory, Policy and Practice*, Macmillan International Higher Education.
Spano, R. and Nagy, S. 2005, "Social Guardianship and Social Isolation: An Application and Extension of Lifestyle/Routine Activities Theory to Rural Adolescents", *Rural sociology*, Vol. 70 No. 3**,** pp. 414-437.
Sparks, R. F. 1982, *Research on Victims of Crime: Accomplishments, Issues, and New Directions*, US Dept. of Health and Human Services, Public Health Service, Alcohol, Drug ….
Spicer, J. 2005, *Making Sense of Multivariate Data Analysis: An Intuitive Approach*, Sage.
Sproule, S. and Archer, N. (2007), "Defining Identity Theft", paper presented at the *Management of eBusiness, 2007. WCMeB 2007. Eighth World Congress on the*,2007, avaialable at.
Srivastava, S. 2012, "Pessimistic Side of Information & Communication Technology: Cyber Bullying and Legislature Laws", *International Journal*, Vol. 1 No. 1**,** pp.
Stafford, M., Chandola, T. and Marmot, M. 2007, "Association between Fear of Crime and Mental Health and Physical Functioning", *American journal of public health*, Vol. 97 No. 11**,** pp. 2076-2081.
Stahl, G. K. and Caligiuri, P. 2005, "The Effectiveness of Expatriate Coping Strategies: The Moderating Role of Cultural Distance, Position Level, and Time on the International Assignment", *Journal of Applied Psychology*, Vol. 90 No. 4**,** pp. 603.
Stalans, L. J. and Finn, M. A. 2016, Understanding How the Internet Facilitates Crime and Deviance. Taylor & Francis.
Stamm, S., Ramzan, Z. and Jakobsson, M. (2007), "Drive-by Pharming", paper presented at the *International Conference on Information and Communications Security*,2007, avaialable at.
Stanko, E. A. 1995, "Women, Crime, and Fear", *The Annals of the American Academy of Political and Social Science*, Vol. 539 No. 1**,** pp. 46-58.
Statista. 2018, "Number of Ebay's Active Users from 1st Quarter 2010 to 1st Quarter 2018 (in Millions). available at: https://www.statista.com/statistics/242235/number-of-ebays-total-active-users/ (accessed 19/07/2018).
Staymartonline. 2016, "Gumtree Warns of Phishing Attacks after Security Breach. available at: https://www.staysmartonline.gov.au/alert-service/gumtree-warns-phishing-attacks-after-security-breach (accessed 18/07/2108).
Stenbacka, C. 2001, "Qualitative Research Requires Quality Concepts of Its Own", *Management decision*, Vol. 39 No. 7**,** pp. 551-556.
Sterner, A. and Sheng, S. 2013, "The Effect of Social Stigma on Fare Evasion in Stockholm's Public Transport", *Journal of Transport Literature*, Vol. 7 No. 4**,** pp. 50-74.
Stommel, M. and Wills, C. 2004, *Clinical Research: Concepts and Principles for Advanced Practice Nurses*, Lippincott Williams & Wilkins.
Strauss, A. and Corbin, J. M. 1990, *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*, Sage Publications, Inc.
Straw, K. 2013, "Free Wi-Fi: The Hidden Dangers", in: Kestle, R. and Self, R. (eds.), *Is Practices for Sme Success Series*. pp. 123-126.
Strickland, J. 2017, *Logistic Regression inside and Out*, Lulu. com.
Stringer, R. 2014, *Knowing Victims: Feminism, Agency and Victim Politics in Neoliberal Times*, Routledge.
Strobl, R. 2004, "Constructing the Victim: Theoretical Reflections and Empirical Examples", *International review of victimology*, Vol. 11 No. 2-3**,** pp. 295-311.
Strobl, R. 2010, "Becoming a Victim", *International handbook of victimology*, Vol. No. 3-25.

Sudarno, B. E. P. 2012, "Analysis Tracking Online Payment System", *International Journal Of Scientific & Technology Research (IJSTR) Volume*, Vol. 1 No.

Sullivan, B. 2015, "Hackers Target Starbucks Gift Cardholders. available at: http://www.cnbc.com/2015/05/13/hackers-target-starbucks-gift-cardholders.html (accessed 10/08/2016).

Sumner, C., Byers, A. and Shearing, M. 2011, "Determining Personality Traits and Privacy Concerns from Facebook Activity", *Black Hat Briefings*, Vol. 11 No. 197-221.

Sun, J. C.-Y., Yu, S.-J., Lin, S. S. and Tseng, S.-S. 2016, "The Mediating Effect of Anti-Phishing Self-Efficacy between College Students' Internet Self-Efficacy and Anti-Phishing Behavior and Gender Difference", *Computers in Human Behavior*, Vol. 59 No. 249-257.

Sundeen, R. A. and Mathieu, J. T. 1976, "The Fear of Crime and Its Consequences among Elderly in Three Urban Communities", *The Gerontologist*, Vol. 16 No. 3**,** pp. 211-219.

Sundie, J. M., Cialdini, R. B., Griskevicius, V. and Kenrick, D. T. 2012, "The World's (Truly) Oldest Profession: Social Influence in Evolutionary Perspective", *Social Influence*, Vol. 7 No. 3**,** pp. 134-153.

Sutton, M. 2014, "Fencing/Receiving Stolen Goods", *Encyclopedia of Criminology and Criminal Justice*, Springer. pp. 1627-1637.

Swaray, R. 2007, "On the Relationship between the Public's Worry About Safety from Burglary and Probabilities of Burglary: Some Evidence from Simultaneous Equation Models", *Social Indicators Research*, Vol. 80 No. 2**,** pp. 361-378.

Symantec. 2016, "Internet Security Threat Report 2016", available at: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf (accessed 13/10/2016).

Symantec. 2017, "Internet Security Threat Report. available at: https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq_ (accessed 06/09/2017).

Symantec 2018, "Internet Security Threat Report", Vol. No.

Symantec. 2019, "Internet Security Threat Report February 2019", available at: https://img03.en25.com/Web/Symantec/%7B1a7cfc98-319b-4b97-88a7-1306a3539445%7D_ISTR_24_2019_en.pdf (accessed 27 February 2019).

Şeitan, O., Gherman, C. and Bulgărea, C. N. 2010, "E-Commerce with Online Payment through Bank Card", *Annals of the University of Petrosani, Economics*, Vol. 10 No. 4**,** pp. 309-316.

Tacq, J. J. and Tacq, J. 1997, *Multivariate Analysis Techniques in Social Science Research: From Problem to Analysis*, Sage.

Tansey, R., White, M., Long, R. G. and Smith, M. 1996, "A Comparison of Loglinear Modeling and Logistic Regression in Management Research", *Journal of Management*, Vol. 22 No. 2**,** pp. 339-358.

Tashakkori, A. and Creswell, J. W. 2007, Exploring the Nature of Research Questions in Mixed Methods Research. Sage Publications Sage CA: Los Angeles, CA.

Tashakkori, A. and Teddlie, C. 2003, "Major Issues and Controversies in the Use of Mixed Methods in the Social and Behvioral Sciences", in: Tashakkori, A. and Teddlie, C. (eds.), *Handbook of Mixed Methods in Social & Behavioral Research*, Thousand Oaks, Calif. : SAGE Publications, Thousand Oaks, Calif. pp. 3-50.

Tashakkori, A. and Teddlie, C. 2008, "Quality of Inferences in Mixed Methods Research: Calling for an Integrative Framework", in: Bergman, M. M. (ed.) *Advances in Mixed Methods Research*. pp. 101-119.

Taylor, G. 2002, "The Council of Europe Cybercrime Convention a Civil Liberties Perspective", *Retrieved June*, Vol. 13 No. 2006.

Taylor, M. 2009, "The Impact of Life Events on Financial Capability: Evidence from the Bhps", *London: Financial Services Authority*, Vol. No.

Taylor, R. B. (1996), "Neighborhood Responses to Disorder and Local Attachments: The Systemic Model of Attachment, Social Disorganization, and Neighborhood Use Value", paper presented at the *Sociological Forum*,1996, avaialable at.

Teddlie, C. and Tashakkori, A. 2006, "A General Typology of Research Designs Featuring Mixed Methods", *Research in the Schools*, Vol. 13 No. 1**,** pp. 12-28.

Teddlie, C. and Tashakkori, A. 2010, "Overview of Contemporary Issues in Mixed Methods Research", *Handbook of mixed methods in social and behavioral research*, Vol. No. 1-41.

Teddlie, C. and Yu, F. 2007, "Mixed Methods Sampling: A Typology with Examples", *Journal of mixed methods research*, Vol. 1 No. 1**,** pp. 77-100.

Tejay, G. P. and Zadig, S. M. (2012), "Investigating the Effectiveness of Is Security Countermeasures Towards Cyber Attacker Deterrence", paper presented at the *System Science (HICSS), 2012 45th Hawaii International Conference on*,2012, avaialable at.

Tenenbaum, L. S., Varjas, K., Meyers, J. and Parris, L. 2011, "Coping Strategies and Perceived Effectiveness in Fourth through Eighth Grade Victims of Bullying", *School Psychology International*, Vol. 32 No. 3**,** pp. 263-287.

Tewksbury, R. and Mustaine, E. 2001, "Lifestyle Factors Associated with the Sexual Assault of Men: A Routine Activity Theory Analysis", *The Journal of Men's Studies*, Vol. 9 No. 2**,** pp. 153-182.

The Council of Europe Convention on Cybercrime 2001, Convention on Cybercrime, In: Europe, T. C. O. (ed.). Budapest: European Treaty Series - No. 185.

The Uk Cards Association Card Expenditure Report. 2017, "Card Expenditure Statistics April 2017", available at: http://www.theukcardsassociation.org.uk/wm_documents/Card%20Expenditure%20Report%20-%20April%202017.pdf (accessed 18/08/2018).

Thomas, D. and Loader, B. 2000, "Cybercrime: Law Enforcement, Security and Surveillance in the Information Age", in: Thomas, D. and Loader, B. (eds.), *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Routledge, London. pp.

Thompson, N., Mcgill, T. J. and Wang, X. 2017, "“Security Begins at Home”: Determinants of Home Computer and Mobile Device Security Behavior", *Computers & Security*, Vol. 70 No. 376-391.

Thompson, W. E. and Gibbs, J. C. 2016, *Deviance and Deviants: A Sociological Approach*, John Wiley & Sons.

Thomson, S. B. 2010, "Sample Size and Grounded Theory", *Thomson, SB (2010). Grounded Theory-Sample Size. Journal of Administration and Governance*, Vol. 5 No. 1**,** pp. 45-52.

Tilley, N., Farrell, G. and Clarke, R. V. 2015, "Target Suitability and the Crime Drop", *Target Suitability and the Crime Drop*, Springer. pp. 59-76.

Tillyer, M. S. and Eck, J. E. 2009, "Routine Activities", *21st Century Criminology: A Reference Handbook*, Vol. 1 No. 279-287.

Tillyer, M. S., Fisher, B. S. and Wilcox, P. 2011, "The Effects of School Crime Prevention on Students' Violent Victimization, Risk Perception, and Fear of Crime: A Multilevel Opportunity Perspective", *Justice Quarterly*, Vol. 28 No. 2**,** pp. 249-277.

Timmer, D. A. and Norman, W. H. 1984, "The Ideology of Victim Precipitation", *Criminal Justice Review*, Vol. 9 No. 2**,** pp. 63-68.

Tittle, C. R. 2018, *Control Balance: Toward a General Theory of Deviance*, Routledge.

Titus, R. M. and Gover, A. R. 2001, "Personal Fraud: The Victims and the Scams", *Crime Prevention Studies*, Vol. 12 No. 133-152.

Titus, R. M., Heinzelmann, F. and Boyle, J. M. 1995, "Victimization of Persons by Fraud", *Crime & Delinquency*, Vol. 41 No. 1**,** pp. 54-72.

Togher, L., Hand, L. and Code, C. 1997, "Analysing Discourse in the Traumatic Brain Injury Population: Telephone Interactions with Different Communication Partners", *Brain Injury*, Vol. 11 No. 3**,** pp. 169-190.

Torres, L. 2010, "Predicting Levels of Latino Depression: Acculturation, Acculturative Stress, and Coping", *Cultural Diversity and Ethnic Minority Psychology*, Vol. 16 No. 2**,** pp. 256.

Townsley, M. and Pease, K. 2002, Winter in Bermuda and Summer in Alaska: Hot Spots, Crime and Climate. Analysis for Crime Prevention. Monsey, NY: Criminal Justice Press.

Treiman, D. J. 2014, *Quantitative Data Analysis: Doing Social Research to Test Ideas*, John Wiley & Sons.

Tsai, H.-Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J. and Cotten, S. R. 2016, "Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective", *Computers & Security*, Vol. 59 No. 138-150.

Tsakalidis, G. and Vergidis, K. 2017, "A Systematic Approach toward Description and Classification of Cybercrime Incidents", *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Vol. No. 99**,** pp. 1-20.

Tseloni, A., Wittebrood, K., Farrell, G. and Pease, K. 2004, "Burglary Victimization in England and Wales, the United States and the Netherlands: A Cross-National Comparative Test of Routine Activities and Lifestyle Theories", *British Journal of Criminology*, Vol. 44 No. 1**,** pp. 66-91.

Tseloni, A. and Zarafonitou, C. 2008, "Fear of Crime and Victimization: A Multivariate Multilevel Analysis of Competing Measurements", *European Journal of Criminology*, Vol. 5 No. 4**,** pp. 387-409.

Tsetsi, E. and Rains, S. A. 2017, "Smartphone Internet Access and Use: Extending the Digital Divide and Usage Gap", *Mobile Media & Communication*, Vol. 5 No. 3**,** pp. 239-255.

Tuli, K. and Juneja, N. 2016, "Cyber Security Challenges and Online Frauds on Internet", *International Journal of Advanced Research in IT and Engineering*, Vol. 5 No. 2**,** pp. 1-12.

Tun, W., Katzen, L. L., Abbott, S. A., Srikrishnan, A. K., Kelly, C. A., Sarna, A., Friedland, B. A., Solomon, S. and Mensch, B. S. 2015, "Using a 2-Stage Strategy with Respondent-Driven Sampling to Recruit a Hard-to-Reach Population for a Placebo Microbicide Gel Clinical Trial in Nellore, Andhra Pradesh (India)", *AIDS and Behavior*, Vol. 19 No. 2**,** pp. 369-379.

Turban, E., King, D., Lee, J. K., Liang, T.-P. and Turban, D. C. 2015, *Electronic Commerce: A Managerial and Social Networks Perspective*, Springer.
Uebelacker, S. and Quiel, S. (2014), "The Social Engineering Personality Framework", paper presented at the *Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop on*,2014, avaialable at.
Un Congress. (2000), "Crimes Related to Computer Networks", paper presented at the *10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders*,2000, Vienna, avaialable at.
Un Manual. 1994, "United Nations Manual on the Prevention and Control of Computer-Related Crime", available at: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf (accessed 21/03/2017).
Usher, R. 2002, "Textuality and Reflexivity in Educational Research", *Understanding Educational Research*, Routledge. pp. 41-59.
Vakhitova, Z. I., Reynald, D. M. and Townsley, M. 2015, "Toward the Adaptation of Routine Activity and Lifestyle Exposure Theories to Account for Cyber Abuse Victimization", *Journal of Contemporary Criminal Justice*, Vol. 32 No. 2**,** pp. 169-188.
Van Achterberg, T., Huisman-De Waal, G. G., Ketelaar, N. A., Oostendorp, R. A., Jacobs, J. E. and Wollersheim, H. C. 2010, "How to Promote Healthy Behaviours in Patients? An Overview of Evidence for Behaviour Change Techniques", *Health promotion international*, Vol. 26 No. 2**,** pp. 148-162.
Van Deursen, A. J. and Van Dijk, J. A. 2015, "Toward a Multifaceted Model of Internet Access for Understanding Digital Divides: An Empirical Investigation", *The Information Society*, Vol. 31 No. 5**,** pp. 379-391.
Van Dijk, J. and Sarkeshikian, H. 2013, "On the Contrasting Concepts of Victimhood in Christian and Islamic Cultures", *Kriminologie-Kriminalpolitik-Strafrecht*, Vol. No. 291-303.
Van Doorn, N. and Velthuis, O. 2018, "A Good Hustle: The Moral Economy of Market Competition in Adult Webcam Modeling", *Journal of Cultural Economy*, Vol. 11 No. 3**,** pp. 177-192.
Van Eijk, G. 2017, "Between Risk and Resistance: Gender Socialization, Equality, and Ambiguous Norms in Fear of Crime and Safekeeping", *Feminist Criminology*, Vol. 12 No. 2**,** pp. 103-124.
Van Heumen, L. 2015. *Social Relations of Older Adults with Intellectual Disabilities from a Life Course Perspective.*
Van Teijlingen, E. and Hundley, V. 2002, "The Importance of Pilot Studies", *Nursing Standard*, Vol. 16 No. 40**,** pp. 33-36.
Van Wilsem, J. 2011, "Worlds Tied Together? Online and Non-Domestic Routine Activities and Their Impact on Digital and Traditional Threat Victimization", *European Journal of Criminology*, Vol. 8 No. 2**,** pp. 115.
Van Wilsem, J. 2013a, "Bought It, but Never Got It' Assessing Risk Factors for Online Consumer Fraud Victimization", *European Sociological Review*, Vol. 29 No. 2**,** pp. 168-178.
Van Wilsem, J. 2013b, "Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization", *Journal of Contemporary Criminal Justice*, Vol. 29 No. 4**,** pp. 437-453.
Van Wyk, J. and Benson, M. L. 1997, "Fraud Victimization: Risky Business or Just Bad Luck?", *American Journal of Criminal Justice*, Vol. 21 No. 2**,** pp. 163-179.
Vance, A., Eargle, D., Ouimet, K. and Straub, D. (2013), "Enhancing Password Security through Interactive Fear Appeals: A Web-Based Field Experiment", paper presented at the *System Sciences (HICSS), 2013 46th Hawaii International Conference on*,2013, avaialable at.
Vartanian, T. P. 2010, *Secondary Data Analysis,* Oxford University Press.
Vashisht, S., Gupta, S., Singh, D. and Mudgal, A. (2016), "Emerging Threats in Mobile Communication System", paper presented at the *Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 International Conference on*,2016, avaialable at.
Vatanasombut, B., Igbaria, M., Stylianou, A. C. and Rodgers, W. 2008, "Information Systems Continuance Intention of Web-Based Applications Customers: The Case of Online Banking", *Information & Management*, Vol. 45 No. 7**,** pp. 419-428.
Vazsonyi, A. T., Pickering, L. E., Belliston, L. M., Hessing, D. and Junger, M. 2002, "Routine Activities and Deviant Behaviors: American, Dutch, Hungarian, and Swiss Youth", *Journal of Quantitative Criminology*, Vol. 18 No. 4**,** pp. 397-422.
Verhaeghe, S., Defloor, T. and Grypdonck, M. 2005, "Stress and Coping among Families of Patients with Traumatic Brain Injury: A Review of the Literature", *Journal of clinical nursing*, Vol. 14 No. 8**,** pp. 1004-1012.
Verma, J. 2012, *Data Analysis in Management with Spss Software,* Springer Science & Business Media.
Vieno, A., Roccato, M. and Russo, S. 2013, "Is Fear of Crime Mainly Social and Economic Insecurity in Disguise? A Multilevel Multinational Analysis", *Journal of Community & Applied Social Psychology*, Vol. 23 No. 6**,** pp. 519-535.

Viljoen, E., Terblanche-Smit, M. and Terblanche, N. 2010, "Breaching the Tension Threshold in Fear Appeals: An Experimental Investigation", *Management Dynamics: Journal of the Southern African Institute for Management Scientists*, Vol. 19 No. 2**,** pp. 2-16.
Virtanen, S. M. 2017, "Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities", *Psychiatry, Psychology and Law*, Vol. 24 No. 3**,** pp. 323-338.
Vishal, V. and Johari, R. (2018), "Soaice: Simulation of Attacks in Cloud Computing Environment", paper presented at the *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*,2018, avaialable at.
Vishwanath, A., Herath, T., Chen, R., Wang, J. and Rao, H. R. 2011, "Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model", *Decision Support Systems*, Vol. 51 No. 3**,** pp. 576-586.
Vitelli, R. and Endler, N. S. 1993, "Psychological Determinants of Fear of Crime: A Comparison of General and Situational Prediction Models", *Personality and Individual Differences*, Vol. 14 No. 1**,** pp. 77-85.
Von Hentig, H. 1941, "Remarks on the Interaction Fo Perpetrator and Victim", *Am. Inst. Crim. L. & Criminology*, Vol. 31 No. 303.
Von Hentig, H. 1948, "The Criminal and His Victim: Studies in the Sociobiology of Crime", *New Haven, CT: Yale University Press*, Vol. No.
Vynck, G. D. and Barr, A. 2018, "Shopify Battles the Scammers Behind Fake Web Stores. available at: https://adage.com/article/digital/shopify-battles-scammers-fake-web-stores/314564/ (accessed 10/10/2018).
Wade, J. 2004, "The Music Industry's War on Piracy", *Risk Management*, Vol. 51 No. 2**,** pp. 10.
Walker, J. T. and Maddan, S. 2008, *Statistics in Criminology and Criminal Justice: Analysis and Interpretation*, Jones & Bartlett Publishers.
Walklate, S. 1989, *Victimology: The Victim and the Criminal Justice System*, Unwin Hyman, London.
Walklate, S. 2012, *Handbook of Victims and Victimology*, Routledge.
Wall, D. S. 2001, "Cybercrime and the Internet", in: Wall, D. (ed.) *Crime and the Internet*, Routledge. pp.
Wall, D. S. 2004, "Digital Realism and the Governance of Spam as Cybercrime", *European journal on criminal policy and research*, Vol. 10 No. 4**,** pp. 309-335.
Wall, D. S. 2005, "Digital Realism and the Governance of Spam as Cybercrime", *European journal on criminal policy and research*, Vol. 10 No. 4**,** pp. 309-335.
Wall, D. S. 2007, *Cybercrime: The Transformation of Crime in the Information Age*, Cambridge: Polity Press.
Wall, D. S. 2008a, "Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime", *International Review of Law, Computers & Technology*, Vol. 22 No. 1-2**,** pp. 45-63.
Wall, D. S. 2008b, "Hunting, Shooting and Phishing: New Cybercrime Challenges for Cybercanadians in the 21st Century", *Eccles Centre for North American Studies, London*, Vol. No.
Wall, D. S. 2010a, "Criminalising Cyberspace: The Rise of the Internet as a 'Crime Problem'", in: Jewkes, Y. and Yar, M. (eds.), *Handbook of Internet Crime*, Cullompton : Willan, Cullompton. pp. 88-103.
Wall, D. S. 2010b, "Micro-Frauds: Virtual Robberies, Stings and Scams in the Information Age", in: Holt, T. and Schell, B. (eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, IGI Global. pp. 68-85.
Wall, D. S. 2010c, "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace (Revised May 2010)", *Police Practice and Research*, Vol. 8 No. 2**,** pp. 183-205.
Wall, D. S. 2013a, "Criminalising Cyberspace: The Rise of the Internet as a 'Crime Problem'", *Handbook of Internet Crime*, Willan. pp. 106-121.
Wall, D. S. 2013b, "Future Identities: Changing Identities in the Uk—the Next 10 Years/Identity Related Crime in the Uk": Technical report, UK Govern-ment's Foresight project, (accessed.
Wall, D. S. 2013c, "Insecurity and the Policing of Cyberspace", *Crime and Insecurity*, Willan. pp. 198-222.
Wall, D. S. 2013d, "Policing Identity Crimes", in: Wall, D. S. and Williams, M. L. (eds.), *Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing*, Taylor & Francis. pp. 29-52.
Wall, D. S. 2015, "The Internet as a Conduit for Criminal Activity", *Information Technology and the Criminal Justice System*, Vol. No. 77-98.
Wall, D. S. 2017, *Crime and Deviance in Cyberspace*, Routledge.
Wall, D. S. and Williams, M. 2007, "Policing Diversity in the Digital Age: Maintaining Order in Virtual Communities", *Criminology & Criminal Justice*, Vol. 7 No. 4**,** pp. 391-415.
Walsh, R. 2003, "The Methods of Reflexivity", *The Humanistic Psychologist*, Vol. 31 No. 4**,** pp. 51-66.
Walters, K. L. and Simoni, J. M. 2002, "Reconceptualizing Native Women's Health: An "Indigenist" Stress-Coping Model", *American Journal of Public Health*, Vol. 92 No. 4**,** pp. 520-524.

Wang, J.-L., Jackson, L. A., Wang, H.-Z. and Gaskin, J. 2015, "Predicting Social Networking Site (Sns) Use: Personality, Attitudes, Motivation and Internet Self-Efficacy", *Personality and Individual Differences*, Vol. 80 No. 119-124.
Wang, J., Herath, T., Chen, R., Vishwanath, A. and Rao, H. R. 2012, "Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear Phishing Email", *IEEE transactions on professional communication*, Vol. 55 No. 4**,** pp. 345-362.
Wang, J., Li, Y. and Rao, H. R. 2017, "Coping Responses in Phishing Detection: An Investigation of Antecedents and Consequences", *Information Systems Research*, Vol. No.
Warkentin, M., Johnston, A. C., Shropshire, J. and Barnett, W. D. 2016, "Continuance of Protective Security Behavior: A Longitudinal Study", *Decision Support Systems*, Vol. 92 No. 25-35.
Warr, M. 1993, "Fear of Victimization", *Public Perspective*, Vol. 5 No. 25-28.
Warr, M. 2000, "Fear of Crime in the United States: Avenues for Research and Policy", *Criminal justice*, Vol. 4 No. 4**,** pp. 451-489.
Watson, J. 2018, "70+ Common Online Scams Used by Cyber Criminals and Fraudsters. available at: https://www.comparitech.com/vpn/avoiding-common-scams-schemes/ (accessed 10/02/2019).
Watt, L. D. 2001, "Pregnancy Prevention in Primary Care for Adolescent Males", *Journal of Pediatric Health Care*, Vol. 15 No. 5**,** pp. 223-228.
Watts, S. 2016, "Secure Authentication Is the Only Solution for Vulnerable Public Wi-Fi", *Computer Fraud & Security*, Vol. 2016 No. 1**,** pp. 18-20.
Weekes, R. B. 2003, "Cyber-Zoning a Mature Domain: The Solution to Preventing Inadvertent Access to Sexually Explicit Content on the Internet", *Va. JL & Tech.*, Vol. 8 No. 1.
Wei, W., Li, J., Cao, L., Ou, Y. and Chen, J. 2013, "Effective Detection of Sophisticated Online Banking Fraud on Extremely Imbalanced Data", *World Wide Web*, Vol. 16 No. 4**,** pp. 449-475.
Weinberg, A. M. 1966, "Can Technology Replace Social Engineering?", *Bulletin of the Atomic Scientists*, Vol. 22 No. 10**,** pp. 4-8.
Weinstein, J. A. 2010, *Applying Social Statistics: An Introduction to Quantitative Reasoning in Sociology*, Rowman & Littlefield Publishers.
Weise, E. 2017, "Just Say No to Linkedin Requests from Strangers; Some May Be Phishing Scams. available at: https://eu.usatoday.com/story/tech/2017/10/06/just-say-no-linkedin-requests-strangers-some-may-phishing-scams/723528001/ (accessed 18/07/2018).
Weishäupl, E., Yasasin, E. and Schryen, G. 2018, "Information Security Investments: An Exploratory Multiple Case Study on Decision-Making, Evaluation and Learning", *Computers & Security*, Vol. No.
Wells, K. B. 1999, "Treatment Research at the Crossroads: The Scientific Interface of Clinical Trials and Effectiveness Research", *American Journal of Psychiatry*, Vol. 156 No. 1**,** pp. 5-10.
Welsh, A. and Lavoie, J. 2012, "Risky Ebusiness: An Examination of Risk-Taking, Online Disclosiveness, and Cyberstalking Victimization", *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, Vol. 6 No. 1**,** pp. 1-13.
Wengraf, T. 2001, *Qualitative Research Interviewing: Biographic Narrative and Semi-Structured Methods*, Sage.
Wertenbroch, K., Dhar, R. and Khan, U. 2005, "A Behavioral Decision Theory Perspective on Hedonic and Utilitarian Choice", *Inside Consumption*, Routledge. pp. 166-187.
Wheatley, S., Maillart, T. and Sornette, D. 2016, "The Extreme Risk of Personal Data Breaches and the Erosion of Privacy", *The European Physical Journal B*, Vol. 89 No. 1**,** pp. 7.
White, C. and Verduyn, C. 2006, "The Children and Parents Service (Caps): A Multi-Agency Early Intervention Initiative for Young Children and Their Families", *Child and Adolescent Mental Health*, Vol. 11 No. 4**,** pp. 192-197.
Whittaker, C., Ryner, B. and Nazif, M. (2010), "Large-Scale Automatic Classification of Phishing Pages", paper presented at the *NDSS*,2010, avaialable at.
Whittemore, R., Chase, S. K. and Mandle, C. L. 2001, "Validity in Qualitative Research", *Qualitative health research*, Vol. 11 No. 4**,** pp. 522-537.
Williams, E. J., Beardmore, A. and Joinson, A. N. 2017, "Individual Differences in Susceptibility to Online Influence: A Theoretical Review", *Computers in Human Behavior*, Vol. 72 No. 412-421.
Williams, K. C. 2012, "Fear Appeal Theory", *Research in Business and Economics Journal*, Vol. 5 No. 1.
Williams, L., Patterson, J. and Edwards, T. M. 2018, *Clinician's Guide to Research Methods in Family Therapy: Foundations of Evidence-Based Practice*, Guilford Publications.
Williams, M. 2000, "Virtually Criminal: Discourse, Deviance and Anxiety within Virtual Communities", *International Review of Law, Computers & Technology*, Vol. 14 No. 1**,** pp. 95-104.
Williams, M. and Levi, M. 2015, "Perceptions of the Ecrime Controllers: Modelling the Influence of Cooperation and Data Source Factors", *Security Journal*, Vol. 28 No. 3**,** pp. 252-271.

Williams, M. L. 2015, "Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level", *British Journal of Criminology*, Vol. 56 No. 1**,** pp. 21-48.
Williams, M. L. and Levi, M. 2017, "Cybercrime Prevention", *Handbook of crime prevention and community safety*, Vol. No. 454-469.
Willig, C. 2013, *Introducing Qualitative Research in Psychology*, McGraw-Hill Education (UK).
Wilson, J. K. 2009, *The Praeger Handbook of Victimology*, ABC-CLIO.
Witte, K. 1992, "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model", *Communications Monographs*, Vol. 59 No. 4**,** pp. 329-349.
Witte, K. and Allen, M. 2000, "A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns", *Health education & behavior*, Vol. 27 No. 5**,** pp. 591-615.
Wolfe, S. E., Marcum, C. D., Higgins, G. E. and Ricketts, M. L. 2016, "Routine Cell Phone Activity and Exposure to Sext Messages: Extending the Generality of Routine Activity Theory and Exploring the Etiology of a Risky Teenage Behavior", *Crime & Delinquency*, Vol. 62 No. 5**,** pp. 614-644.
Wolfgang, M. E. 1957, "Victim Precipitated Criminal Homicide", *The Journal of Criminal Law, Criminology, and Police Science*, Vol. 48 No. 1**,** pp. 1-11.
Wolfgang, M. E. 1958, "Patterns in Criminal Homicide", Vol. No.
Wong, D. 2016, "The Epl Drama–Paving the Way for More Illegal Streaming? Digital Piracy of Live Sports Broadcasts in Singapore", *Leisure Studies*, Vol. 35 No. 5**,** pp. 534-548.
Wooldredge, J. D., Cullen, F. T. and Latessa, E. J. 1992, "Research Note Victimization in the Workplace: A Test of Routine Activities Theory", *Justice Quarterly*, Vol. 9 No. 2**,** pp. 325-335.
Woon, I., Tan, G.-W. and Low, R. 2005, "A Protection Motivation Theory Approach to Home Wireless Security", *ICIS 2005 proceedings*, Vol. No. 31.
Workman, M. 2007, "Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security", *Journal of the Association for Information Science and Technology*, Vol. 59 No. 4**,** pp. 662-674.
Workman, M. 2008, "Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security", *Journal of the American Society for Information Science and Technology*, Vol. 59 No. 4**,** pp. 662-674.
Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M. and Marett, K. 2014, "Research Note—Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance", *Information Systems Research*, Vol. 25 No. 2**,** pp. 385-400.
Wueest, C. 2015. *Underground Black Market: Thriving Trade in Stolen Data, Malware, and Attack Services*. *Symantec Official Blog* [Online]. Available from: https://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services [Accessed 26/07/2017 2017].
Wyant, B. R. 2008, "Multilevel Impacts of Perceived Incivilities and Perceptions of Crime Risk on Fear of Crime: Isolating Endogenous Impacts", *Journal of Research in Crime and Delinquency*, Vol. 45 No. 1**,** pp. 39-64.
Xu, H., Dinev, T., Smith, J. and Hart, P. 2011, "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances", *Journal of the Association for Information Systems*, Vol. 12 No. 12**,** pp. 798.
Xu, Z., Hu, Q. and Zhang, C. 2013, "Why Computer Talents Become Computer Hackers", *Communications of the ACM*, Vol. 56 No. 4**,** pp. 64-74.
Yap, K. B., Wong, D. H., Loh, C. and Bak, R. 2010, "Offline and Online Banking–Where to Draw the Line When Building Trust in E-Banking?", *International Journal of Bank Marketing*, Vol. 28 No. 1**,** pp. 27-46.
Yar, M. 2005, "The Novelty of 'Cybercrime' an Assessment in Light of Routine Activity Theory", *European Journal of Criminology*, Vol. 2 No. 4**,** pp. 407-427.
Ybarra, M. L. and Mitchell, K. J. 2008, "How Risky Are Social Networking Sites? A Comparison of Places Online Where Youth Sexual Solicitation and Harassment Occurs", *Pediatrics*, Vol. 121 No. 2**,** pp. e350-e357.
Yeboah-Boateng, E. O. and Amanor, P. M. 2014, "Phishing, Smishing and Vishing: An Assessment of Threats against Mobile Devices", *Journal of Emerging Trends in Computing and Information Sciences*, Vol. 5 No. 4**,** pp. 297-307.
Yin, P. P. 1980, "Fear of Crime among the Elderly: Some Issues and Suggestions", *Social problems*, Vol. 27 No. 4**,** pp. 492-504.
Youn, S. 2005, "Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk–Benefit Appraisal Approach", *Journal of Broadcasting & Electronic Media*, Vol. 49 No. 1**,** pp. 86-110.
Youn, S. 2009, "Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors among Young Adolescents", *Journal of Consumer affairs*, Vol. 43 No. 3**,** pp. 389-418.

Young, D. L., Goodie, A. S., Hall, D. B. and Wu, E. 2012, "Decision Making under Time Pressure, Modeled in a Prospect Theory Framework", *Organizational behavior and human decision processes*, Vol. 118 No. 2**,** pp. 179-188.

Yu, S. 2014, "Fear of Cyber Crime among College Students in the United States: An Exploratory Study", *International Journal of Cyber Criminology*, Vol. 8 No. 1**,** pp.

Yuan, P., Bare, M. G., Johnson, M. O. and Saberi, P. 2014, "Using Online Social Media for Recruitment of Human Immunodeficiency Virus-Positive Participants: A Cross-Sectional Survey", *Journal of medical Internet research*, Vol. 16 No. 5**,** pp.

Yuill, J., Denning, D. and Feer, F. (2007), "Psychological Vulnerabilities to Deception, for Use in Computer Security", paper presented at the *DoD Cyber Crime Conference 2007*,2007, avaialable at.

Zahedi, F. M., Abbasi, A. and Chen, Y. 2015, "Fake-Website Detection Tools: Identifying Elements That Promote Individuals' Use and Enhance Their Performance", *Journal of the Association for Information Systems*, Vol. 16 No. 6**,** pp. 448.

Zaykowski, H. 2015, "Reconceptualizing Victimization and Victimization Responses", *Crime & Delinquency*, Vol. 61 No. 2**,** pp. 271-296.

Zhang, L. and Mcdowell, W. C. 2009, "Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords", *Journal of Internet Commerce*, Vol. 8 No. 3-4**,** pp. 180-197.

Zhang, W., Luo, X., Burd, S. D. and Seazzu, A. F. (2012), "How Could I Fall for That? Exploring Phishing Victimization with the Heuristic-Systematic Model", paper presented at the *System Science (HICSS), 2012 45th Hawaii International Conference on*,2012, avaialable at.

Zhang, X., Tsang, A., Yue, W. T. and Chau, M. 2015, "The Classification of Hackers by Knowledge Exchange Behaviors", *Information Systems Frontiers*, Vol. 17 No. 6**,** pp. 1239-1251.

Zhao, X., Deng, S. and Zhou, Y. 2017, "The Impact of Reference Effects on Online Purchase Intention of Agricultural Products: The Moderating Role of Consumers' Food Safety Consciousness", *Internet Research*, Vol. 27 No. 2**,** pp. 233-255.

Zhao, X., Xue, L. and Whinston, A. B. 2013, "Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements", *Journal of Management Information Systems*, Vol. 30 No. 1**,** pp. 123-152.

Zielinska, O. A., Tembe, R., Hong, K. W., Ge, X., Murphy-Hill, E. and Mayhorn, C. B. (2014), "One Phish, Two Phish, How to Avoid the Internet Phish: Analysis of Training Strategies to Detect Phishing Emails", paper presented at the *Proceedings of the human factors and ergonomics society annual meeting*,2014, avaialable at.

Zurkus, K. 2016, "Best and Worst Online Retailers for Security. available at: https://www.csoonline.com/article/3152827/security/best-and-worst-security-practices-for-online-retailers.html (accessed 10/10/2018).