PERSONALITY TRAITS, VICTIMISATION, AND CYBERCRIME-REPORTING BEHAVIOUR IN MALAYSIA

CHEW JIA YIN

UNIVERSITI SAINS MALAYSIA

2025

PERSONALITY TRAITS, VICTIMISATION, AND CYBERCRIME-REPORTING BEHAVIOUR IN MALAYSIA

by

CHEW JIA YIN

Thesis submitted in fulfilment of the requirements for the degree of Bachelor of Science (Honours) in Forensic Science

February 2025

CERTIFICATE

This is to certify that the dissertation entitled "Personality Traits, Victimisation, and Cybercrime-Reporting Behaviour in Malaysia", is the *bona fide* research work of Ms. Chew Jia Yin (158924), conducted under my supervision from July 2024 to February 2025. I have reviewed this dissertation and find it to meet acceptable scholarly standards, scope, and quality for submission in partial fulfilment of the requirements for the degree of Bachelor of Science (Honours) in Forensic Science.

Supervisor,

(AP Dr Geshina Ayu Mat Saat)

Date: 23rd February 2025

DECLARATION

I hereby declare that this dissertation is the result of my own investigations, except where otherwise stated and duly acknowledged. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at *Universiti Sains Malaysia* or other institutions. I grant *Universiti Sains Malaysia* the right to use this dissertation for teaching, research, and promotional purposes.

(Chew Jia Yin)

Date: 23rd February 2025

ACKNOWLEDGEMENT

I thank God for this invaluable opportunity to conduct my research. I thank Him for the strength He provided during moments of doubt. I thank Him for being the light for my path that guided me through this journey.

I would like to express my utmost gratitude to my supervisor, Associate Professor Dr Geshina Ayu Mat Saat. Her support, guidance, and encouragement have been instrumental in shaping this research. I especially appreciated her keen eye in refining my work and her constructive—often witty—feedback that drove this thesis to completion. Her remarkable contributions greatly enhanced this dissertation.

My heartfelt thanks go to my mates, Harwani Omar and Nursyafizah Azmi, for their dedication in translating the survey battery and for the little trips we took for our meetings. I extend my appreciation to Dr Nur Waliyuddin Hanis Zainal Abidin, the course coordinator of GTF411/8 Research Project, for assisting our lot throughout the ethics application process, and for granting much-needed deadline extensions. I also appreciated my examiners, Dr Wan Nur Syuhaila Mat Desa and Dr Faridah Naim, for their thoughtful feedback during the proposal presentation.

I am deeply grateful to my beloved mother, Lai Yuen Mei, for her countless prayers throughout this journey. I am also thankful to ChatGPT and the creators on YouTube for their guidance whenever I found myself lost in the labyrinth of statistical analysis and spreadsheets. A special thanks to ChatGPT for its useful commands that made Excelling more efficient; and its insightful critiques that helped improve my

writing and word choices.

Lastly, I would also like to acknowledge my friends, batchmates, juniors, all of my survey respondents, and everyone—that I am unable to mention by name—who contributed directly or indirectly to this research. I give thanks to the banana latte-fuelled mornings, the long nights spent chasing deadlines, and the caffeine running in my blood that kept me going. Most of all, I thank myself for persevering through the highs and lows of this journey and seeing it through till the end.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF SYMBOLS

Name	Definition
H_A	Alternative Hypothesis
CI	Confidence Interval
χ^2	Chi Square
c	Confidence Level
$Z(c/100)$	Critical Value
α	Cronbach's Alpha Coefficient or Significance Level
df	Degree of Freedom
r	Fraction of Responses
F	F-statistics
H	Kruskal-Wallis
Λ	Lambda
U	Mann-Whitney
E	Margin of Error
$\bar{x}$	Mean
$-$	Negative
H_O	Null Hypothesis
ηp^2	Partial Eta Squared
%	Percentage
N	Population Size
$+$	Positive
n	Sample Size
p	Statistical Significance
SD	Standard Deviation

LIST OF ABBREVIATIONS, ACRONYMS, AND INITIALISMS

Name	Definition
ANOVA	Analysis of Variance
AB5C	Abridged Big Five Circumplex
BNM	Central Bank of Malaysia
BTS	Bartlett's Test of Sphericity
CAtM	Crimes Against the Machine
CCID	Commercial Crime Investigation Department
CItM	Crimes In the Machine
CUtM	Crimes Using the Machine
CVI	Content Validity Index
DDOS	Distributed Denial-of-Service
DoS	Denial-of-Service
DOSM	Department of Statistics Malaysi
EFA	Exploratory Factor Analysis
Fai	Fairness
FYP	Final Year Project
GreA	Greed-Avoidance
ICT	Information and Communication Technology
IHA	Integrity/Honesty/Authenticity
ImpC	Impulse Control
JEPeM	*Jawatankuasa Etika Penyelidikan Manusia*
KMO	Kaiser-Meyer-Olkin
MANOVA	Multivariate Analysis of Variance
MCMC	Malaysian Communications and Multimedia Commission
Mod	Moderation

MyCERT	Malaysia Computer Emergency Response Team
MPQ	Multidimensional Personality Questionnaire
NFCC	National Anti-Financial Crime Centre
No	Number
NSRC	National Scam Response Center
OR	Odds Ratio
PAF	Principal Axis Factoring
Pat	Patience
PhD	Doctoral Degree
Pru	Prudence
PSoC	Perceived Seriousness of Cybercrime
RisA	Risk-Avoidance
RMP	Royal Malaysian Police
SCT	Self-Control Theory
SPSS	Statistical Product and Service Solutions
TCI	Temperament and Character Inventory
TttP	Trust towards the Police
U.K.	United Kingdom
U.S.	United States
UNODC	United Nations Office on Drugs and Crime
USM	*Universiti Sains Malaysia*
VOR	Victim-Offender Relationship
VPT	Victim Precipitation Theory
WHO	World Health Organisation

CIRI-CIRI PERSONALITI, KEMANGSAAN, DAN TINGKAH LAKU PELAPORAN JENAYAH SIBER DI MALAYSIA

ABSTRAK

Jenayah siber semakin menjadi kebimbangan global, namun ramai mangsa tidak melaporkan kejadian yang dialami, menyebabkan jurang dalam statistik jenayah dan menyukarkan sokongan kepada mangsa. Kajian kuantitatif ini meneliti hubungan antara ciri-ciri personaliti, jenis kemangsaan jenayah siber, dan tingkah laku pelaporan di Malaysia, dengan tumpuan kepada halangan dalam pelaporan serta kesedaran mengenai platform pelaporan yang sedia ada. Kajian keratan rentas ini melibatkan 91 orang dewasa di Malaysia (berumur 18 tahun ke atas) yang direkrut melalui persampelan kemudahan. Peserta-peserta melengkapkan soal selidik dalam talian yang dikendalikan sendiri, untuk mengukur pengalaman mereka dengan jenayah siber, kesedaran mereka mengenai platform pelaporan, tingkah laku pelaporan, halangan untuk melaporkan, serta ciri-ciri personaliti mereka.

Ujian multivariat dan bukan parametrik digunakan untuk membandingkan ciri-ciri personaliti antara mangsa dan bukan mangsa, serta merentasi pelbagai jenis jenayah siber. Analisis tambahan turut dijalankan bagi mengkaji hubungan antara tingkah laku pelaporan, kemangsaan jenayah siber, dan halangan dalam pelaporan. Keputusan kajian menunjukkan tiada perbezaan signifikan dalam ciri-ciri personaliti antara mangsa dan bukan mangsa atau merentasi jenis jenayah siber. Selain itu, jenis jenayah siber dan halangan dalam pelaporan juga tidak menunjukkan hubungan yang signifikan dengan tingkah laku pelaporan.

Penemuan ini menunjukkan bahawa ciri-ciri personaliti mungkin memainkan peranan yang terhad dalam kemangsaan jenayah siber. Hal ini menekankan keperluan untuk meneroka faktor alternatif seperti pengaruh psikologi, sosiologi, atau kriminologi. Walaupun dapatan kajian ini tidak signifikan, ia tetap menyumbang kepada bidang viktimologi siber dengan mencabar teori mengenai peranan ciri-ciri personaliti dalam kemangsaan jenayah siber. Implikasi terhadap pencegahan jenayah siber, kesedaran mengenai pilihan pelaporan jenayah siber, dan kajian masa hadapan turut dibincangkan.

PERSONALITY TRAITS, VICTIMISATION, AND CYBERCRIME-REPORTING BEHAVIOUR IN MALAYSIA

ABSTRACT

Cybercrime is a growing global concern, yet many victims do not report incidents, leading to gaps in crime statistics and complicating victim support. This quantitative study examines the relationship between personality traits, cybercrime victimisation, and reporting behaviour in Malaysia, with a focus on barriers to reporting and awareness of existing reporting platforms. A cross-sectional study was conducted with 91 Malaysian adults (aged 18 and above) recruited via convenience sampling. Participants completed an online self-administered survey battery, measuring their experiences with cybercrime, awareness of reporting platforms, cybercrime-reporting behaviour, barriers to reporting, and personality traits.

Multivariate and non-parametric tests were used to compare personality traits between victims and non-victims, as well as across different types of cybercrime. Additional analyses examined associations between reporting behaviour, cybercrime victimisation and barriers to reporting. The results showed no significant differences in personality traits between victims and non-victims or across cybercrime types. Furthermore, cybercrime types and perceived barriers to reporting were not significantly associated with reporting behaviour.

These findings indicate that personality traits may play a limited role in cybercrime victimisation, highlighting the need to explore alternative study factors, such as those of psychological, sociological, or criminological influences. Despite these non-significant findings, the current study contributes to the field of cyber victimology by challenging theories regarding the role of personality traits in cybercrime victimisation. Implications for cybercrime prevention, awareness of cybercrime-reporting options, and future research are discussed.

CHAPTER 1: INTRODUCTION

1.0 Introduction

This is an undergraduate Final Year Project (FYP) regarding personality traits, victimisation, and cybercrime-reporting behaviour in Malaysia. This chapter describes pertinent issues that prompted the selection of this research. Issues described include information on the study background, problem statements, study rationales, research questions, research objectives, hypotheses, operational definition of terms used, significance of the study, and outline of the thesis.

1.1 Study Background

This section discusses the background of this research. The first study background discusses the global prevalence of cybercrime. The second background considers issues related to unreported cybercrime in Malaysia. The third background presents challenges of the current cybercrime-reporting system in Malaysia.

1.1.1 Global Prevalence of Cybercrime

The rapid digitalisation of society has made daily life more convenient and expanded opportunities for cybercrime (Phillips et al., 2022). This trend is evident worldwide, with countries such as France (Petrosyan, 2024a), Canada (Petrosyan, 2024b), the United States (U.S.) (Petrosyan, 2024c), and the United Kingdom (U.K.) (Petrosyan, 2023); experiencing a rising number of cyber incidents and financial losses. In France, economic damages from cybercrime increased from USD5.1 billion in 2016 to USD93 billion in 2023 (Petrosyan, 2024a). In Canada, cybercrime reports increased by 387% from 2014 to 2022 (Petrosyan, 2024b), while 60% of U.S. citizens have experienced credit card fraud (Petrosyan, 2024c).

In the U.K., about eight in ten internet users have encountered scams; though many hesitate to report them, often due to doubts about their helpfulness or uncertainty about where to report (Petrosyan, 2023). This rise in cybercrime may reflect a shift of traditional property crimes—such as theft, burglaries, and vandalism—onto online platforms, according to dark figure research from victimisation surveys (Burssens, 2023). This digital transformation of crime indicates how online platforms have enabled criminal activities, making it more difficult to accurately measure and address their true scope.

Globally, cybercrime is projected to cost up to USD15.63 trillion by 2029 (Petrosyan, 2024d). In Malaysia, 5,917 incidents were reported to Cyber999 in 2023, with phishing, impersonation and spoofing being the most common types of fraud (Malaysia Computer Emergency Response Team [MyCERT], 2024a). This high number of reported incidents raises concerns about how easily cybercriminals can exploit internet users in a society with a 97.4% internet penetration rate (Kemp, 2024), resulting in financial, psychological, and data losses for victims. These incidents underscore the risks that come with widespread digital integration, including an increased risk of cybercrime victimisation.

1.1.2 Unreported Cybercrime in Malaysia

Crime statistics are essential for shaping effective policies, directing resources, and facilitating the arrest of offenders by identifying underlying issues (van de Weijer, Leukfeldt & van der Zee, 2020). However, when crimes remain unreported, the validity of these statistics is compromised (Buil-Gil, Moretti & Langton, 2022). This creates “dark figures” of crime, leading to a skewed understanding of crime trends and

victim behaviours (Asiama & Zhong, 2022), limiting victims' access to necessary support services. These dark figures reduce the number of criminals entering the criminal justice system and distort the effectiveness of public safety policies (Asiama & Zhong, 2022; Buil-Gil, Moretti & Langton, 2022).

In the case of cybercrime, both the seriousness of the offence and the anonymity of offenders are predictors of higher reporting rates (van de Weijer, Leukfeldt & van der Zee, 2020). However, given the prevalence of minor cybercrimes like phishing (MyCERT, 2024a), it is highly likely that substantial cybercrime go unreported. In Malaysia, a 2022 survey of Malaysian internet users (n = 2,401) revealed that around 40% of respondents had experienced cybercrime victimisation (Siddharta, 2023a). From that percentage of victims, 38.6% of respondents took no further action after being targeted by cybercriminals, while only 18.9% of victims reported the cybercrime incidents to authorities (Siddharta, 2023b). These statistics raise questions regarding the dark figures of cybercrime in Malaysia.

1.1.3 Challenges in Cybercrime-Reporting System

In Malaysia, cybercrime victims have access to online platforms for reporting incidents to the relevant authorities, including hotlines (Central Bank of Malaysia [BNM], 2024; MyCERT, 2024c; National Scam Response Centre [NSRC], 2024), website portals (Malaysian Communications and Multimedia Commission [MCMC], 2024a; MyCERT, 2024c; The Royal Malaysian Police [RMP], 2024), and mobile applications (MyCERT, 2024c). These reporting platforms cover a wide range of cybercrime from online financial fraud (NSRC, 2024) to technical threats like phishing and malware (MyCERT, 2024c). Despite the availability of these reporting options, still, the most

critical step for initiating an official investigation is to lodge a police report at the nearest station. Unfortunately, online reporting to the police is restricted to complaints pertaining to cases of lost personal documents or items that do not relate to crime (RMP, 2024).

The NSRC, a collaboration between the National Anti-Financial Crime Centre (NFCC), BNM, RMP, MCMC, and telecom providers; offers a 997 hotline for rapid response to online financial fraud that operates from 8 a.m. to 8 p.m. (NSRC, 2024). Incidents that happen outside of those hours will require the victim to contact their banks' 24/7 hotline (BNM, 2024; NSRC, 2024). However, even after contacting the NSRC or the bank's hotline, victims still need to lodge a police report for a formal investigation to proceed (BNM, 2024; NSRC, 2024). Similarly, technical incidents such as phishing, spam or malware can be reported to Cyber999; while cases of cyber-harassment can be filed at the MCMC online portal, but these reports also require follow-up at a police station (MyCERT, 2024c; MCMC, 2024a).

Although there are a range of reporting platforms available, it is an overall complex and fragmented process. The victims are required to go through multiple platforms and file in-person reports, which can be burdensome and confusing. These multiple steps raise concerns about whether the current system meets the victims' needs in terms of accessibility and efficiency (Wiredu et al., 2024).

1.2 Problem Statements

Three problem statements underlie the need for this FYP. The first is the unclear role of personality traits in cybercrime victimisation. The second is the unknown prevalence and reasons for non-reporting amongst cybercrime victims. The third is the difficulties in the cybercrime-reporting system.

1.2.1 The Unclear Role of Personality Traits in Cybercrime Victimisation

Despite the prevalence of cybercrime, contemporary literature (Koning, Junger & Veldkamp, 2023; Nzeakor, Ede & Nwoke, 2024; Stiff & Reeves, 2024; Partin et al., 2021) that examines the association between personality traits and different types of cybercrime victimisation remains limited. Past research suggests that human factors significantly contribute to cybercrime, with victims often deceived through social engineering tactics and perceived cues of urgency or authority, rather than by the exploitation of technological vulnerabilities (Curtis & Oxburgh, 2023; Nzeakor, Ede & Nwoke, 2024). The variation in individuals' victimisation risk, raises questions about why some fall victim to cybercrime, while others do not (Nzeakor, Ede & Nwoke, 2024). Stiff and Reeves (2024) suggested that focusing on victims' characteristics could better address the high prevalence of cybercrime, as these individuals are motivated to reduce their own vulnerability. This reveals a research gap in understanding how personality traits relate to vulnerability and different types of cybercrime.

1.2.2 Unknown Prevalence and Reasons for Non-Reporting Amongst Cybercrime Victims

Unreported cybercrime remains a critical issue globally, leading to significant dark figures of crime (Asiama & Zhong, 2022; United Nations Office on Drugs and Crime

[UNODC], 2019). A 2017 study in the Netherlands showed that only 13% of cybercrime victims reported their experiences to the police (van de Weijer, Leukfeldt & van der Zee, 2020). In the Netherlands, common reasons for non-reporting include perceptions that the police will not act (32.3%, *n* = 112) and a preference for solving the issue by themselves (29.1%, *n* = 101) (van de Weijer, Leukfeldt & van der Zee, 2020). In Malaysia, a survey (*n* = 2,401) revealed that a significant number of respondents who experienced cybercrime do not report their victimisation to the authorities as described in the previous section (Siddharta, 2023a, 2023b). Currently, most research on cybercrime-reporting behaviour is largely based on studies conducted in European countries like Belgium and the Netherlands (De Kimpe et al., 2021; van de Weijer, Leukfeldt & Bernasco, 2018; van de Weijer, Leukfeldt & van der Zee, 2020), while the reasons behind what discourages reporting of cybercrime in Malaysia remains unclear.

1.2.3 Difficulties in the Cybercrime-Reporting System

Despite the digital nature of cybercrimes, victims are still required to physically visit a police station to file a report for an official investigation to be initiated. This requirement is particularly inconvenient for victims living in remote areas or those with mobility difficulties (Wiredu et al., 2024). Victims of minor cybercrimes may also be deterred from reporting if they perceive the process as overly troublesome (10.4%, *n* = 36, van de Weijer, Leukfeldt & van der Zee, 2020). While various online platforms (BNM, 2024; MCMC, 2024a; MyCERT, 2024c, NSRC, 2024) exist to address specific types of cybercrime in Malaysia, the current reporting system that combines online and in-person processes can overwhelm victims, especially those

already experiencing distress. Public awareness regarding Malaysia's reporting system remains largely unexplored.

1.3 Study Rationales

Three study rationales are identified in this FYP study. First, there is a need to better understand the personality traits of cybercrime victims. Second, there is a need to understand the barriers to cybercrime-reporting behaviour. Third, there is a need to understand public awareness regarding the current cybercrime-reporting system in Malaysia.

1.3.1 Understanding Personality Traits of Cybercrime Victims

Given the prevalence of cybercrime and the suggestion that personality traits may contribute to cybercrime victimisation, there is a need to better understand the personality traits of cybercrime victims. This understanding is important, as it seeks to study why some people become easy targets while others do not (Nzeakor, Ede & Nwoke, 2024). This FYP research aims to address this gap, providing a more comprehensive understanding of the personality traits associated with different types of cybercrime victimisation.

1.3.2 Understanding Barriers of Cybercrime-Reporting Behaviour

The prevalence of unreported cybercrime and the non-reporting amongst cybercrime victims in Malaysia underscores a need for research to understand the barriers deterring cybercrime-reporting behaviour. A lack of understanding about what deters the victim from reporting can lead to a distortion of the true extent of cybercrime statistics, masking the severity of the issue (Asiama & Zhong, 2022; Buil-Gil, Moretti, & Langton, 2022).

This FYP research aims to understand the barriers to non-reporting behaviours amongst cybercrime victims in Malaysia.

1.3.3 Understanding Public Awareness of the Cybercrime-Reporting System

The challenges and difficulties in Malaysia's cybercrime-reporting system address a need to understand public awareness regarding this system. According to van de Weijer, Leukfeldt, and van der Zee (2020), victims of less serious cybercrime may choose not to report if they believe that the police will not take action (32.3%, n = 112), prefer to handle the issue independently (29.1%, n = 101), find the overall process particularly inconvenient (10.4%, n = 36), or feel it is unimportant (9.5%, n = 33). This FYP research aims to comprehend the public awareness of the current cybercrime-reporting system in Malaysia.

1.4 Research Questions

This FYP study aims to address four research questions. The research questions correspond to the objectives stated in the next section. Below are the four research questions for this FYP.

1. How do the personality traits of victims differ across different types of cybercrime in Malaysia?
2. How do the personality traits of cybercrime victims compare to those of non-victims in Malaysia?
3. Are there associations in reporting behaviour across different types of cybercrime victimisation in Malaysia?
4. What are the common barriers influencing cybercrime-reporting amongst victims in Malaysia?

1.5 Research Objectives

This FYP study has one general objective and four specific objectives. The general objective is to determine the relationship between personality traits, types of cybercrime victimisation, and cybercrime-reporting behaviour amongst victims and non-victims in Malaysia; emphasising the barriers and awareness of the current reporting system.

The four specific objectives are outlined below.

1. To examine the differences in personality traits amongst victims of different types of cybercrime in Malaysia.
2. To compare the personality traits of cybercrime victims with those of non-victims in Malaysia.
3. To determine the associations in cybercrime-reporting behaviour across different types of cybercrime victimisation in Malaysia.
4. To determine the common barriers influencing cybercrime reporting amongst victims in Malaysia.

1.6 Hypotheses

Based on the problem statements and study rationales stated in the previous sections, four hypotheses were developed. The four hypotheses are listed below, with H_O indicating the null hypothesis, and H_A indicating the alternative hypothesis.

H_{O1}: There is no difference in the personality traits amongst victims of different types of cybercrime in Malaysia.

H_{A1}: There is a difference in the personality traits amongst victims of different

types of cybercrime in Malaysia.

H_{O2}: There is no difference in the personality traits of cybercrime victims compared to non-victims in Malaysia.

H_{A2}: There is a difference in the personality traits of cybercrime victims compared to non-victims in Malaysia.

H_{O3}: There are no associations in cybercrime-reporting behaviour across different types of cybercrime in Malaysia.

H_{A3}: There are associations in cybercrime-reporting behaviour across different types of cybercrime in Malaysia.

H_{O4}: There are no differences in the barriers influencing cybercrime-reporting amongst victims in Malaysia.

H_{A4}: There are differences in the barriers influencing cybercrime-reporting amongst victims in Malaysia.

1.7 Operational Definitions and Terms

This section describes the definition of the key terms and concepts used in this FYP study. The terms defined herein are “cybercrime”, “victim”, and “personality trait”.

1.7.1 Cybercrime

Cybercrime is an umbrella term for illegal activities facilitated or committed using digital technology, though a universally accepted definition is lacking (Phillips et al., 2022; UNODC, 2021). According to the UNODC (2021), cybercrime involves

unlawful activities conducted through information and communication technology (ICT), either by directly attacking networks, systems, data, and websites, or by using technology to aid in committing a crime; whereas the Budapest Convention focuses on protecting the confidentiality, integrity, and availability of information systems (Phillips et al., 2022; Sarkar & Shukla, 2023). Despite these definitions, the complexity and impact of cybercrime remain challenging to be fully captured.

Based on a review of 23 sources, Sarkar and Shukla (2023: p. 5) provide a broader perspective, defining cybercrime as "actions occurring within the realm of cyberspace that are deemed unlawful within the jurisdiction in which they occur, consequently leading to socio-economic and psychosocial harm for affected individuals". This suggests that cybercrime includes any illegal online activity that causes financial or psychological harm to individuals, though what is deemed "unlawful" varies by jurisdiction. Hence, it is essential to define cybercrime according to Malaysian law, as not all cyber incidents constitute as an offence under Malaysian legal provisions, even when it is considered as a crime elsewhere. ***Table 1.1*** includes categories of incidents reported via Cyber999, however some incidents are not considered crimes, such as intrusion attempts and vulnerability reports.

Table 1.1: *Sub-categories of the reported cyber incidents (MyCERT, 2024a)*

CATEGORIES OF INCIDENTS	
1. Content-related	**5. Intrusion attempt**
Data breach	Login brute force
2. Denial of Service (DoS)	Port scanning
DoS/DDoS	Vulnerability probes
3. Fraud	**6. Malicious codes**
Bogus email	Botnet C&C
Business email compromise (BEC)	Bots
Fraud site	Malware
Impersonation & spoofing	Malware hosting
Job scam	**7. Spam**

Lottery scam	Spam
Love/Parcel scam	Spam relay
Phishing	**8. Vulnerabilities report**
4. Intrusion	Misconfiguration disclosure
Account compromise	System
Defacement	Web

Currently, “cybercrime” lacks an exact definition in Malaysian law. However, related terminology like “computer crime” (Phillips et al., 2022) and similar offences are addressed across various legal provisions. This section outlines several laws that address common types of cybercrime in Malaysia.

1.7.1(a) Computer Crimes Act 1997 (Act 563)

This act falls within the jurisdiction of the Commercial Crime Investigation Department (CCID) of the RMP (MCMC, 2024b). Act 563 covers offences related to computer misuse. Hacking, regardless of intent to commit further crimes, is classified as “unauthorised access to computer material” under Section 3. This aligns with MyCERT’s (2024b) definition of intrusion as unauthorised or illegal access to a system or network, often leading to account compromise, web defacement, or the installation of malicious programs.

MyCERT (2024b) defines malicious codes as any software or script designed to cause harm, breaches, or damage to a system without the owner’s consent. Section 5, Act 563 addresses “unauthorised modification of computer contents,” such as the spread of computer viruses. Examples of malicious codes include attack scripts, viruses, worms, Trojan horses, backdoors, and malware. Act 563 also covers denial-of-service (DoS) attacks, which deprive users of the resources they would normally expect (MyCERT, 2024b).

Additionally, Act 563 holds hackers accountable for unlawful communication, such as sharing unauthorised access credentials, codes, or passwords of another person's computer system. For the purpose of this FYP study, the term “hacking” (MCMC, 2024b) is used to cover the meanings of intrusion that lead to subsequent account compromise, web defacement, and the installation of malicious codes, as it is a term more commonly used to describe these events that can be easily understood by a layperson. Since DoS attacks are more focused on organisational-level victims rather than victims at the individual level, and there are lesser prevalence of DoS attacks recorded (MyCERT, 2024a), it is excluded in this study.

1.7.1(b) Penal Code (Act 574)

This act falls within the jurisdiction of the RMP (MCMC, 2024b). Under the fraud category of reported cyber incidents, phishing and impersonation & spoofing are the most and second most common types of fraud, respectively (MyCERT, 2024a). MyCERT (2024b) defines phishing as a method where attackers fraudulently obtain personal information, such as passwords or credit card numbers, by pretending to be trustworthy entities through electronic communications like emails or instant messages.

Whereas, impersonation and spoofing involve creating emails that appear legitimate to deceive targets or falsifying a person’s or program’s data to gain an illegitimate advantage (MyCERT, 2024b). Currently, there is no specific provision in Malaysia addressing these crimes (MCMC, 2024b). Instead, Section 416 of the Penal Code (Act 574) covers “cheating by personation,” which applies to cases where someone pretends to be another person, whether real or imaginary, with the intent to cheat, as below:

> *"A person is said to "cheat by personation", if he cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is."*

For the purpose of this FYP study, phishing and impersonation can be combined into a single category as they bring similar meaning under the provision of Act 574 regardless of the different tactics used to deceive the victim. In addition, Section 509 of Act 574 also addresses cyber-harassment, including cyberbullying, cyberstalking, and online sexual harassment, indicating that individual(s) committed an offence when they insult a person verbally, by certain actions or display of objects with the intention to gain the victim's attention. It states:

> *"Whoever intending to insult the modesty of any person, utters any word, makes any gestures or exhibits any object, intending that such words or sound shall be heard, or that such gestures or objects shall be seen by such person shall be punished with imprisonment for a term which may extend to five years or with fine, or with both."*

1.7.1(c) Communications and Multimedia Act 1998 (Act 588)

This act falls within the jurisdiction of the Malaysian Communications and Multimedia Commission (MCMC, 2024b). Act 588 includes provisions under Sections 231, 232, 234, and 235 to address hacking, communication interception, and tampering with network facilities or Wi-Fi. Section 236 covers the possession of devices or software used to commit cybercrimes. Section 233(1)(*a*) of Act 588 offers a more comprehensive definition of cyber-harassment, specifically targeting offensive statements made online that are obscene, indecent, false, menacing, or offensive in character, with the intent to annoy, abuse, threaten, or harass another person. Section 211 also prohibits offensive content made using content applications service.

Additionally, Section 233(1)(*b*) addresses spam. MyCERT (2024b) defines spam as unsolicited, often commercial emails sent indiscriminately to multiple recipients, commonly known as junk email. Section 233(1)(*b*) prohibits the following:

> *"initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address…"*

For the purpose of this FYP study, cyber-harassment is included as a part of this study to capture the variety of cybercrimes such as cyberbullying, cyberstalking, and online sexual harassment. Spam is not included in this study as the illegality of such events is difficult to determine, particularly the intention of the sender to annoy, threaten or harass the recipient of the spam message (MCMC, 2024c).

1.7.1(d) Classification of Cybercrime

Phillips et al. (2022) suggested that categorisation is more suitable to define the variety of cybercrime, as attempts to define the term "cybercrime" often limit its ability to convey a comprehensive understanding. Given that an overlap of jurisdiction towards several crimes was observed in several legal provisions, this section intends to offer a more detailed classification of cybercrime as described previously.

One of the dominant classifications divides cybercrime into "cyber-dependent" (targeting ICT systems) and "cyber-enabled" crimes (traditional crimes using ICT). However, Phillips et al. (2022) argued that a three-category system, albeit less popular, is more advantageous over the two-category system, as it better captures the range of behaviours under "cyber-enabled" crimes by distinguishing between crimes against

property and crimes against people. This three-category system divides cybercrimes as follows (Wall, 2017, as cited in Phillips et al., 2022):

1. "Crimes against the Machine" (CAtM) includes computer integrity crimes.
2. "Crimes using the Machine" (CUtM) includes computer-assisted crimes.
3. "Crimes in the Machine" (CItM) includes computer content crimes.

Based on the classification as described above, the selected cybercrime provisioned by the Malaysian law are grouped accordingly, as indicated in ***Table 1.2***. The information was presented in such a way to indicate the overlap of jurisdiction between Act 574 and Act 588 for cyber-harassment.

Table 1.2: *A summary of the classification of the selected cybercrime*

No.	Classification	Jurisdiction	Law	Selected Cybercrime
1.	CAtM	RMP	Act 563	**Hacking** -Intrusion/Malicious codes (account compromise, web defacement, and malicious codes installation)
2.	CUtM		Act 574	Section 416 **Phishing and impersonation**
3.	CItM			Section 509;
		MCMC	Act 588	Section 211 & 233 **Cyber-harassment** (cyberbullying, cyberstalking, and online sexual harassment)

It is mentioned here that information in ***Table 1.2*** is applied in the survey battery and in testing hypotheses. As such, when utilising any of the classifications in ***Table 1.2***, the selected cybercrimes are referred to **Appendix F** and **Section 1.6**.

1.7.2 Victim

Currently, Malaysia lacks a unified legal definition of "victim" that applies across all crime types. Despite Nasimah's (2011) concerns over a decade ago about the punitive,

retributive, and offender-focused nature of Malaysia's criminal justice system, no broad "victim" definition exists. The Domestic Violence Act 1994 (Act 521) defines "victim" specifically for domestic violence cases, yet this definition does not extend to other crimes. The Criminal Procedure Code (Act 593), however, acknowledges certain victims' rights, including restitution and compensation under certain conditions. Section 183A Act 593 allows victims to give impact statements and share how the offence has affected them or their families, including trauma, harm, damages, and economic losses.

According to Nasimah (2011), victims are individuals or groups who have experienced harm—such as physical or mental injury, emotional suffering, economic loss, or rights violations—due to acts or omissions that breach criminal laws. This term also includes the immediate family or dependents of direct victims, as well as those harmed while assisting the victims or preventing victimisation (Nasimah, 2011). Such definitions align with the UN Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power, where "victim" was defined as "victims of crime" (General Assembly Resolution 40/34, 1985), as follows:

> *"1. 'Victims' means persons who, individually or collectively, have suffered harm, including physical or mental injury, emotional suffering, economic loss or substantial impairment of their fundamental rights, through acts or omissions that are in violation of criminal laws operative within Member States, including those laws proscribing criminal abuse of power.*
>
> *"2. A person may be considered a victim, under this Declaration, regardless of whether the perpetrator is identified, apprehended, prosecuted or convicted and regardless of the familial relationship between the perpetrator and the victim. The term "victim" also includes, where appropriate, the immediate family or dependants of the direct victim and persons who have suffered harm in intervening to assist victims in distress or to prevent victimization.*
>
> *"3. The provisions contained herein shall be applicable to all, without distinction of any kind, such as race, colour, sex, age, language, religion, nationality, political or other opinion, cultural beliefs or practices, property, birth or family status, ethnic or social origin, and disability."*

For this FYP, victims are defined as individuals who have been victimised by the selected cybercrime described in the previous section. This excludes victimisation that occurred at an organisational, national, or international level. This definition also excludes other forms of cybercrime not investigated herein.

1.7.3 Personality Trait

A personality trait refers to "differences among individuals in a typical tendency to behave, think, or feel in some conceptually related ways, across a variety of relevant situations and over some fairly long period of time" (Ashton, 2022: pp. 31–33). This implies that personality traits are useful for comparing individuals directly or indirectly, by reflecting a person's relatively strong predisposition to certain behaviours, thoughts, or emotions (Ashton, 2022). These traits are characterised by recurring psychological patterns, expressed across various situations over time, indicating stable and consistent behaviour rather than temporary reactions (Ashton, 2022). Siegel (2016) earlier suggested that certain personality traits, such as depression, anxiety, impulsivity, and low self-control, may increase a person's vulnerability to victimisation, making them appear as easier targets unlikely to resist. For instance, impulsive individuals in particular, tend to take risks and avoid precautions, putting them in dangerous situations where they are more likely to be victimised (Siegel, 2016).

In the context of this FYP, personality traits refer to individual differences of the participants in this study. These differences are measurable by the questions shown in **Appendix F**, adapted from the sources listed in ***Table 3.1***. Based on the scoring key in ***Table 3.1***, the scores of each trait form an overarching theme, known as domain. Based on the theoretical framework outlined in **Section 2.5**, domains included Impulsivity,

Risk-Taking Attitude, Greed, and Lack of Genuineness. As such, whenever personality traits are mentioned in this FYP thesis, they refer to the selected personality traits stated in **Section 2.5**.

1.8 Significance of Study

This section describes the significance of study corresponding to the background issues and study rationales previously described. This research is significant to provide insights into the development of effective prevention strategies. The second significance includes suggestions for an improved cybercrime-reporting system. The third significance includes the enhancement of public awareness of the cybercrime-reporting system in Malaysia.

1.8.1 Suggestion for the Development of Effective Prevention Strategies

This FYP study aims to provide insights into how personality traits are associated with cybercrime victimisation. This understanding provides information regarding the profile of cybercrime victims in Malaysia, thus helping the identification of vulnerable populations. It can contribute to the field of criminology by informing the importance of addressing personality traits in cybercrime prevention efforts. Subsequently, tailored prevention strategies and educational programmes could be developed to protect and enhance resilience among vulnerable individuals (Nzeakor, Ede & Nwoke, 2024).

1.8.2 Suggestion for an Improved Cybercrime-Reporting System

By addressing the challenges of cybercrime-reporting and understanding the barriers influencing non-reporting behaviour, this FYP study seeks to address the need for a

more user-friendly reporting system. An online crime-reporting system improves accessibility by enabling citizens to report crimes at any time, potentially increasing reporting rates by up to 25% (Wilson, 2020, as cited in Wiredu et al., 2024). Hence, this informs relevant authorities about the necessity to develop an online-crime reporting system.

1.8.3 Public Awareness of the Cybercrime-Reporting System

This FYP study aims to improve public understanding of the cybercrime-reporting system in Malaysia, thereby increasing awareness of available resources. By informing potential victims about these reporting options, this study promotes greater utilisation of the system, which may help address the issue of unreported cybercrime. Additionally, the survey battery used in this study may offer participating victims a sense of closure by providing an opportunity for them to express their distress, potentially motivating them to make a report (Geshina A. M. S., personal communication, October 27, 2024).

1.9 Outline of the Thesis

This dissertation is divided into six chapters. **CHAPTER 1** includes the introduction to this study. It describes the study background, problem statements, study rationales, research questions, research objectives, hypotheses, operational definition of terms and the significance of the study.

Next, **CHAPTER 2** includes the literature review of this FYP study. Available theories and gaps in knowledge were discussed in this chapter. This forms the theoretical framework, which is the basis of this study.

In **CHAPTER 3**, the methodology used in this research is explained. This chapter was divided into two main parts—the pilot and validation study, as well as the main study. Research design, research subjects, research tool, research procedures, and the translation and validation process were covered. **CHAPTER 4** includes the study findings according to the hypotheses.

CHAPTER 5 discussed the research findings based on the analysis results. Such discussions are related to the proposed theoretical framework and previous studies. The final chapter—**CHAPTER 6**, concludes this FYP study. Research implications as well as several suggestions and recommendations for future research were also covered in this chapter. At the end of the thesis, the references and appendices were included.

CHAPTER 2: LITERATURE REVIEW

2.0 Introduction

This chapter consists of a brief literature review for the basis of this FYP research. In this chapter, literature sources from the search engine Google Scholar were reviewed. Materials reviewed included journal articles, surveys, and statistical reports. The focus was on literature related to personality traits, cybercrime victimisation, cybercrime-reporting behaviour, and relevant theories.

The relationship between personality traits and cybercrime victimisation is discussed in **Section 2.1**. The determinants of cybercrime-reporting behaviour are described in **Section 2.2**. In **Section 2.3**, the gaps in knowledge are identified. **Section 2.4** includes the theories relevant to this FYP study, forming the foundation of this study—the theoretical framework, as depicted in **Section 2.5**.

2.1 Personality Traits and Cybercrime Victimisation

According to Jaishankar (2020), some cybercrime victims had precipitated their own victimisation, often through greed or naivety. Phishing and money mule scams exploit those willing to take online risks, such as visiting unsafe sites or downloading unverified content, even if they are tech-savvy (Jaishankar, 2020). A study found that 80% of victims lacked genuineness, engaging in risky behaviours like viewing adult content (Norton, 2011, as cited in Jaishankar, 2020: pp. 9–10). In advance-fee fraud, some victims even sold their homes in hopes of receiving promised funds (Jaishankar, 2020). This raises questions about the victims' own roles in their victimisation, implying that certain personality traits may contribute to risky online behaviour that

increases their victimisation risk to cybercrime.

Studies (Koning, Junger & Veldkamp, 2023; Nzeakor, Ede & Nwoke, 2024; Stiff & Reeves, 2024; Partin et al., 2021; van de Weijer & Leukfeldt, 2017) examining the association between personality traits and different types of cybercrime victimisation are limited. Van de Weijer and Leukfeldt (2017) were the first to conduct a study in this area of research using Big Five personality traits (openness to experience, conscientiousness, extraversion, agreeableness, and emotional stability) with data from a large sample of Dutch individuals (n = 3,648). Their study (van de Weijer & Leukfeldt, 2017) found that individuals with higher scores on emotional stability (Odds Ratio [OR]: 0.959) and conscientiousness (OR: 0.981) were less likely to experience cybercrime victimisation, while higher scores in openness to experience (OR: 1.044) being significantly related to cybercrime victimisation—such as hacking, malware, phishing, identity theft, cyber romance scam, and online shopping fraud. In addition, van de Weijer and Leukfeldt (2017) also found that higher openness scores (OR: 1.044) were specifically linked to an increased risk of being a victim of cyber-dependent crime (hacking and malware). Although that study built a foundation for research in this area, its publication year in 2017 limits its relevance to contemporary cybercrime victimisation contexts, especially when contextualised to Malaysia.

In a cross-sectional study (n = 385), Partin et al. (2021) found that low self-control is strongly linked to 14 risky online behaviours, including downloading pirated content, purchasing from unsecured websites, and clicking unknown e-mail links; suggesting that impulsivity drives engagement in such behaviours. In a sequential process, these 14 risky online behaviours were significantly associated with 15 types

of self-reported cybercrime—such as cyber-harassment, Nigerian scams, malware, hacking, spam, card fraud, ransomware, and others—indicating that these behaviours increase their victimisation risks to cybercrime (Partin et al., 2021). The findings also showed an indirect relationship between low self-control and cybercrime victimisation, mediated by risky online behaviours, consistent with their theoretical framework (Partin et al., 2021). However, while the study included 15 types of cybercrime, it treated these crimes as a single category of cybercrime rather than analysing them individually, overlooking the differences in their natures.

Koning, Junger & Veldkamp (2023) identified several personality and behavioural factors that contribute to different stages—exposure, susceptibility, and victimisation—of online fraud victimisation. Notably, openness to experience was associated with phishing, spoofing, and purchase fraud victimisation, as this trait often drives curiosity and risk-taking with unknown links or attachments (Koning, Junger & Veldkamp, 2023). Lower self-control is linked to higher susceptibility across all fraud types—such as investment fraud, purchase fraud, job fraud, prize fraud, debt fraud, charity fraud, dating fraud, friend-in-need (WhatsApp) fraud, phishing, identity fraud, spoofing, and others—while higher internet usage, especially in online shopping and social media, correlates with increased exposure to fraud attempts (Koning, Junger & Veldkamp, 2023). Additionally, lower conscientiousness and high agreeableness also affect victimisation, though the influence varies by fraud context (Koning, Junger & Veldkamp, 2023). However, these results diverge from van de Weijer and Leukfeldt (2017) findings, who found no association between agreeableness and cybercrime victimisation, which initially suggested self-control overlaps with both agreeableness and conscientiousness traits.