THE INFLUENCE OF CYBERSECURITY AWARENESS ON FINANCIAL FRAUD PREVENTION BEHAVIORAL AMONG THE YOUNG GENERATIONS.

TANG XIN YI

BACHELOR OF FINANCE (FINANCIAL TECHNOLOGY) WITH HONOURS

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF ACCOUNTANCY AND MANAGEMENT

DECEMBER 2025

THE INFLUENCE OF CYBERSECURITY AWARENESS ON FINANCIAL FRAUD PREVENTION BEHAVIORAL AMONG THE YOUNG GENERATIONS.

BY

TANG XIN YI

A research project submitted in partial fulfilment of the requirement for the degree of

BACHELOR OF FINANCE (FINANCIAL TECHNOLOGY) WITH HONOURS

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF ACCOUNTANCY AND MANAGEMENT

DECEMBER 2025

DECLARATION

We hereby declare that:

(1) This undergraduate research project is the end result of my own work and that due acknowledgement has been given in the references to ALL sources of informationbe they printed, electronic, or personal.

(2) No portion of this research project has been submitted in support of any applicationfor any other degree or qualification of this or any other university, or other institutes of learning.

(3) The word count of this research report is 14057 words.

Name of Student:	Student ID:	Signature:
Tang Xin Yi	2205419	

Date: 17/12/25

ACKNOWLEDGEMENT

From choosing my FYP topic to finishing my research, I have faced numerous obstacles, like choosing the right variables and data. During this process, I came to understand how difficult it is to conduct research for a thesis. I used to even think about not going to a master's program, but I now have a great deal of respect for those who are pursuing a PhD or master's degree.

I am extremely fortunate to have had **Ms. Ngoo Yee Ting** as my supervisor. Her invaluable advice and unwavering support have played a crucial role in helping me complete this FYP. Whenever I faced obstacles, I would consult her for feedback and guidance, which allowed me to improve my work and reach the desired outcome.

I also want to thank my friends and coworkers. We all have similar challenges as fellow students. We were always there to support and encourage one another, whether we were feeling overburdened by the workload or learning how to use new tools. Their encouragement gave me the willpower to persevere.

Lastly, I want to express my gratitude to all my family. Their support and encouragement have been crucial to finishing this FYP. My journey would have been far more difficult without them. I genuinely hope that my accomplishments will make them proud and demonstrate that their faith in me was worthwhile.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CSA	Cybersecurity Awareness
PMT	Protection Motivation Theory
PS	Perceived Severity
PV	Perceived Vulnerability
RE	Response Efficacy
SE	Self-Efficacy
TPB	Theory of Planned Behavior
ATT	Attitude
SN	Subjective Norm
PBC	Perceived Behavioral Control
FFPB	Financial Fraud Prevention Behavior
AVE	Average Variance Extracted
CR	Composite Reliability

PREFACE

The purpose of this study is to ascertain the linked between financial fraud prevention behavior and cybersecurity awareness, with an emphasis on Malaysia's youth. The risk of online fraud is a growing concern in a time when digital financial transactions are becoming more widespread, particularly among younger people. The purpose of my research is to determine whether increased cybersecurity awareness results in more proactive fraud prevention actions or if awareness has little effect on actual fraud prevention actions.

Young generations are the study's primary focus because they are a group that is more susceptible to cyber fraud and actively participates in online financial activities. Young generations are at the nexus of opportunity and risk due to the quick rise in e-wallet and digital banking usage as well as growing cybersecurity threats. They are therefore an essential group for researching how well cybersecurity awareness protects against online financial threats.

The goal of this study was to determine whether a deeper understanding of cybersecurity results in real behavioral changes that lower the risk of falling victim to online fraud. Even though there were many obstacles to overcome due to data issues like sample variability and response biases, I hope to make a significant contribution to the current conversation about the usefulness of awareness in digital security behavior.

ABSTRACT

This study examine the influence of cybersecurity awareness (CSA) on financial fraud prevention behavior (FFPB) among young Malaysians, a demographic increasingly vulnerable to cyber-enabled crimes due to high digital engagement. With the rapid adoption of online banking, e-wallets, and e-commerce platforms, financial fraud has become a pressing concern, yet research has largely overlooked youth-focused behavioral prevention. Drawing upon Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB), this research develops a comprehensive framework linking CSA to fraud prevention through threat and coping appraisals, attitudes, subjective norms, and perceived behavioral control. A quantitative cross-sectional survey was conducted among Malaysian youths aged 18–30, utilizing validated measurement scales analyzed via Structural Equation Modeling (SEM) with SmartPLS. The study aims to provide empirical evidence on how awareness shapes motivation, intentions, and behaviors in fraud prevention. Theoretically, it extends PMT and TPB into the cybersecurity and financial fraud domain, while practically offering insights for educators, policymakers, and financial institutions to design targeted awareness campaigns and digital literacy programs. By addressing gaps in existing research and incorporating key moderating factors, this work contributes to both scholarly knowledge and practical fraud prevention strategies in the digital economy.

CHAPTER 1: INTRODUCTION

Introduction

In the modern era of technology, online platforms like e-wallets, e-commerce systems, and mobile banking are being used more and more for financial transactions. Although these advancements increase efficiency and convenience, they also put people at high risk of cybercrime, especially financial fraud. Cybersecurity Malaysia reports that frauds and online frauds are among the most commonly reported examples of cybercrime, which has increased in this few years. Due to their frequent use of social media, digital payment systems, and online transactions, young people—who represent one of the greatest demographics of consumers of digital financial technology—are especially at risk. Because of this, preventing financial fraud is a top priority for both citizens and governments.

Increasing cybersecurity awareness (CSA) is one of the most important tactics for preventing financial crime. Awareness influences how people view cyberthreats, assess risks, and take preventative action. Protection Motivation Theory (PMT) has been widely used in behavioral security project research to tell how people evaluate threats (perceived vulnerability and perceived severity) and coping mechanisms (self-efficacy and response efficacy) to stimulate protective behaviors. Meanwhile, a supplementary framework for comprehending how subjective norms, attitudes, and perceived behavioral control impact fraud prevention-related intentions and behaviors is offered by the Theory of Planned Behavior (TPB). This study attempts to give a thorough grasp

of the behavioral and psychological processes that motivate financial fraud prevention behavior (FFPB) by combining these two theories.

Even though financial fraud is becoming more common in Malaysia, most research to date has concentrated on adult populations, organizational compliance, or general cybercrime. Empirical research on the effects of CSA on fraud prevention practices, particularly among young Malaysians, is lacking. Designing successful awareness campaigns, educational interventions, and fraud prevention techniques aimed at the younger population requires addressing these gaps.

Therefore, using the theory basis of Protection Motivation Theory and Theory of Planned Behavior, this study investigate the influence of cybersecurity awareness on financial fraud prevention among the young generation. By doing this, it advances scholarly research and practical policymaking in the areas of financial fraud prevention and cybersecurity.

1.1 Research Background

Financial fraud has become a major worldwide concern in the age of digital revolution, across national boundaries, age groups, and social classes. People are now more vulnerable to phishing, identity theft, and investment scams, among other types of cyber-enabled financial fraud, as a result of the highly use of online banking, e-wallets, and mobile payment systems. The Federal Trade Commission (FTC) claims that the data shows that online shopping is a major fraud category, resulting in a remarkably

high number of reports (106,998 in Q4 2024 alone) and causing consumers to suffer enormous total financial losses of more than half a billion dollars during that quarter. Despite the substantial median loss per event ($5,122), the sheer volume of successful frauds makes this group very harmful overall.

In 2023, business impersonators were the most often reported scam among consumers aged 20 to 29. This research however presents a crucial contrast between severity and frequency. Among the top five scams, online shopping had the highest rate of financial loss (82%) despite being the second most reported. This means that young generations were most likely to lose money when they fell victim to this fraud. On the other hand, despite being less commonly reported, job scams and miscellaneous investments had significantly higher median losses ($1,500 and $1,522, respectively), suggesting that these scams aim to defraud each victim of a bigger quantity. This shows that a wide range of frauds target this age group, each with a unique risk profile in terms of probability and amount of loss.

According to the Australian Competition and Consumer Commission (ACCC), over 70% of victims were under 40 years old, and in 2022, professionals and independent contractors lost over AUD 40 million to work scams. Even if the number of reports may vary, the data from the Canadian Anti-Fraud Centre and the ACCC shows a steady and concerning trend of increasing financial losses as a result of fraud.

The shifting demographic of fraud victims is one significant change noted in the Canadian data. The presumption that only elders are targeted was drastically altered in 2022, as most victimization reports came from those between the ages of 20 and 49.

The 25,101 reports from this group greatly exceeded the 16,120 reports from the 50–89 age range. Fraud operations using social media and internet apps to target younger, tech-savvy Canadians who might be less aware of these risks are directly responsible for this trend.

Beside that, Malaysia's digital economy has expanded rapidly, with around 29 million social media users recorded in January 2024—equivalent to 83.1% of the national population—reflecting the high level of digital connectivity among young generation (Tahir, 2025). However, this extensive internet exposure has also made young generations increasingly vulnerable to cyber fraud, including fake job offers, investment scams, and phishing schemes. Alarmingly, 65% of youths surveyed reported encountering scam attempts, underscoring the heightened risks faced by this demographic (Tahir, 2025).

Cybercrime in Malaysia continues to rise sharply. The Department of Statistics Malaysia (DOSM) documented a 35.5% increase in online fraud cases in 2023 compared to 2022, with e-commerce scams and fraudulent investments identified as key threats (Malay Mail, 2024). Complementing this, Statista (2024) reported more than 8,800 e-commerce scam cases by September 2023, while nearly 40% of Malaysian internet users had experienced cybercrime. Yet only 18.9% reported such incidents, revealing a significant issue of underreporting.

Despite escalating risks, cybersecurity awareness among youth remains inadequate. Awareness extends beyond knowledge—it involves interpreting risks, recognizing fraudulent attempts, and being motivated to respond (Bada, Sasse, & Nurse, 2019).

Unfortunately, existing awareness campaigns often fall short in driving sustained behavioral change, particularly among younger users who may downplay their susceptibility or lack motivation (Bada et al., 2019).

Interestingly, higher education does not necessarily enhance protection. In fact, studies suggest that youths with higher educational attainment often report more scam encounters, indicating that knowledge does not always translate into safer behaviors (Tahir, 2025). Young people's bold online presence, impulsivity, and susceptibility to influences such as FOMO (fear of missing out) and trust in social media figures further elevate their risk exposure. This makes cybersecurity awareness (CSA) a critical yet insufficient safeguard.

Research highlights that fraud prevention requires more than awareness; it depends on individuals perceiving risks, believing in the effectiveness of protective measures (e.g., two-factor authentication), and being motivated to act. These elements align with theoretical frameworks such as PMT and the TPB.

By examining how CSA shapes youths' risk perceptions, protective beliefs, and behavioral intentions, this study determine a key research gap: providing empirical evidence on the role of awareness in driving financial fraud prevention among young generation.

1.2 Problem Statement

The exponential growth of digital information technology across Malaysia transformed the manner of financial transactions remarkably, especially among the youth. Online banking facilities, e-wallet options, and e-commerce platforms formed the core of everyday life among the group comprising 18- to 30-year-olds, the most digitally active population group. Though the initiatives added convenience and financial inclusion to people's lives, it opened the floodgates to cybercriminals exploiting weaknesses on an unseen scale, thus fueling financial fraud. Malaysian reports confirm the country experienced an appalling increase in the losses caused by cybercrime in the past few years, scams and fraud emerging among the most frequently reported occurrences nationwide (Malay Mail, 2024). Penang Institute (2025) reports that cybercrime losses in Malaysia reached a figure near US$12.8 billion last year 2024, which is roughly three percent of the country's GDP. This statistic represents the gravitas of the problem and the dangers it poses to the erosion of confidence among the population towards the digital financial infrastructure.

Young Malaysians remain particularly susceptible to cyber fraud because of their extensive use of the internet, dependency on social networking platforms, and usage of digital financial services. Tahir (2025) researched that 65% of Malaysian youth were the subjects of attempted scams, and those possessing greater levels of education were even found more likely to be the targets. This indicates that cybercriminals perceive youth adults as promising targets, taking advantage of their usage of emerging technologies and the tendency to take action on online offers, opportunities to invest, or influencer-based content. Juremi (2024) continues to emphasize the manner in which

platform-based scams on the likes of TikTok and Instagram attract the youth population by using the tactics of social proof and emotive manipulation, rendering it difficult even for them to differentiate such offers from genuine or fraudulent offers. The research thus validates the fact that the youth populace is not just subjected to greater threats but even less behavioral immunity to fraud attacks.

Although efforts to improve cybersecurity awareness (CSA) have been introduced through campaigns such as CyberSAFE and educational workshops, awareness alone does not guarantee preventive action. Zulkifli et al. (2020) observed that while Malaysian secondary school students were knowledgeable about online risks, only a small proportion translated this awareness into concrete protective practices. Similarly, Bada et al. (2019) argue that many awareness campaigns fail to produce meaningful behavioral changes because they often emphasize knowledge dissemination rather than fostering risk perception, motivation, and sustained safe behaviors. This disconnect between awareness and action is particularly problematic among young generations, who may underrate their vulnerability to scams due to optimism bias or misplaced trust in digital platforms.

Behavioral theories such as Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB) offer valuable frameworks for addressing this issue. PMT explains how individuals appraise threats through perceived severity (PS) and perceived vulnerability (PV), while also considering coping mechanisms such as response efficacy (RE) and self-efficacy (SE). These appraisals lead to the formation of protection motivation (PM), which drives protective intentions. TPB, on the other hand, emphasizes the role of attitude, subjective norm, and perceived behavioral

control in shaping behavioral intention (Ajzen, 1991). Integrating PMT and TPB therefore provides a comprehensive way to understand not only how awareness influences motivation, but also how this motivation translates into actual fraud prevention behavior (FFPB). Despite the robustness of these theories, there is limited empirical evidence applying them specifically to financial fraud prevention among young generation.

Previous research on cyber behavior in Malaysia has concentrated on organizational settings or overall internet safety without filling the gap on research on the youth. For example, although Ifinedo (2012); Herath & Rao (2009) illustrate that awareness enhances the confidence of the efficacy of the security controls of the employees, the result cannot be generalized to the youth, as the youth deal with a different risk environment as well as decision processes.

The severity of financial fraud in Malaysia is compounded by low reporting levels. Statista (2024) found that even though almost 40% of Malaysian internet users had been subjected to some sort of cybercrime in 2023, just 18.9% had reported the crimes to the authorities. This under reporting is an indication of lack of confidence in fraud detection, lack of trust in enforcement mechanisms, or just lack of knowledge about procedures for reporting. This concern is especially salient among youth because it signifies both vulnerability to fraud and lack of involvement in protection and corrective measures. This trend thus underscores the necessity for research on the translation of awareness into effective pro-active fraud prevention behaviors.

Overall, these results indicate an important gap both in practice and research. On the one side, financial fraud in Malaysia is on the rise in terms of both scope and sophistication, with a prevalence among youth. On the other side, current prevention programs run by the Malaysian government and commercial banks, though informative, seem less than adequate in providing youth with the intention and behavioral toolkit required to prevent fraud. There is little empirical research making use of proven behavioral theories such as PMT and TPB among young generation.

Therefore, this study is to mark these gaps by examining how Cybersecurity Awareness influences financial fraud prevention behavior among young generation, mediated by PMT constructs and TPB constructs. By doing so, it seeks to provide both theoretical contributions to cybersecurity and behavioral research, and practical insights for policymakers and educators designing interventions to protect young generation against financial fraud.

1.3 Research Questions

1. How does Cybersecurity Awareness effect the Protection Motivation Theory constructs (perceived severity, perceived vulnerability, self-efficacy and response efficacy) among young generation?
2. How does the Protection Motivation Theory shape the Theory of Planned Behavior constructs (attitude, subjective norm, and perceived behavioral control)?
3. How do the Theory of Planned Behavior constructs predict financial fraud prevention behavior?

1.4 Research Objectives

1. To examine the impact of Cybersecurity Awareness on Protection Motivation Theory constructs (perceived severity, perceived vulnerability, self-efficacy and response efficacy) among young generation.
2. To investigate the influence of Protection Motivation Theory on Theory of Planned Behavior constructs (attitude, subjective norm, and perceived behavioral control).
3. To evaluate how Theory of Planned Behavior constructs contribute to Financial Fraud Prevention Behavior.

1.5 Significance of the Study

This study promote both theoretically and practically towards research on cybersecurity and prevention of financial fraud, particularly in the Malaysian context. Theoretically, the study extends the scope of the application of PMT and the TPB into the prevention of financial fraud among the youth. Though the PMT was used extensively in the area of health psychology and information security project research, its applicability towards an explanation of fraud prevention behaviour among population groups such as youth from emerging economies is minimal. By exploring the impact of cybersecurity awareness (CSA) on important constructs of PMT like perceived severity, perceived vulnerability, response efficacy, and self-efficacy, and the role played by the constructs of TPB like attitude, subjective norms, and perceived behavioural control on intention, the study contributes towards a better behaviour-based explanation framework of protective behaviour in the content of digital financial scenarios.

From a practical perspective, the findings have strong implications for policymakers, educators, financial institutions, and cybersecurity agencies. As Malaysia faces an alarming rise in financial scams—with youths being among the most targeted—the study provides data-driven insights into the behavioural mechanisms that encourage fraud prevention. The results can inform the design of targeted cybersecurity awareness campaigns, digital literacy programs in schools and universities, and policy guidelines for fraud mitigation strategies. For financial institutions, the findings may also assist in tailoring fraud alerts, educational tools, and customer support to youth demographics.

1.6 Scope of the Study

This study investigates the relationship between cybersecurity awareness (CSA) and financial fraud prevention behavior (FFPB) among young generations in Malaysia, focusing on the impact of PMT (Protection Motivation Theory) and TPB (Theory of Planned Behavior) constructs. Using secondary data collected via surveys, the study excludes participants under the age of 18 and those who do not regularly engage with online financial platforms. The analysis is specific to Malaysia and excludes international comparisons. The scope is limited to measurable constructs like attitude, subjective norm, perceived behavioral control, response efficacy, and self-efficacy, without exploring the qualitative aspects of cybersecurity awareness or fraud prevention practices. The research is based on quantitative data and excludes qualitative evaluations of personal experiences with online fraud.

1.7 Outline of the Study

Chapter 1: Introduction

Background of the study introduces by this chapter, outlining the problem statement, research questions, research objectives, hypotheses, and the significance of the study. It also describes the structure of the paper, providing an overview of the subsequent chapters.

Chapter 2: Literature Review

This chapter discusses the Protection Motivation Theory (PMT) and Theory of Planned Behavior (TPB) theoretical frameworks, reviews empirical research on the relationship between cybersecurity awareness (CSA) and financial fraud prevention behavior (FFPB), and examines the role of these constructs in the cybersecurity landscape. The chapter also reviews existing practices and regulations in online financial fraud prevention.

Chapter 3: Research Methodology

This chapter introduces the research design, sampling methods, data collection techniques, and variables used in the study. It also explains how the constructs related to PMT and TPB are measured and outlines the statistical analysis techniques used to test the hypotheses.

Chapter 4: Results and Analysis

This chapter presents the results from the data analysis, including descriptive statistics, correlation analysis, and regression results. It also includes the findings from hypothesis testing, focusing on the relationships between CSA, PMT, TPB, and FFPB.

Chapter 5: Discussion and Conclusions

This chapter interprets the research findings in the context of the existing literature. It outlines the implications for cybersecurity education and policy, discusses the practical relevance of the findings for online financial platforms, and proposes recommendations for future research in the field of cybersecurity behavior and fraud prevention.

CHAPTER 2: LITERATURE REVIEW

2.0 Introduction

Global financial transactions have evolved due to the swift implementation of technology platforms across the globe, but the likelihood of fraud and cybercrime increases. Internet fraud occurrences increased by over 35% in 2023 in Malaysia, rendering it among the highest-reported crimes (Malay Mail, 2024). Since youth Malaysians remain most at risk due to their usage of social media platforms, e-wallet platforms, and mobile-based banking platforms, research on financial fraud prevention behavior (FFPB) stands significantly important (Tahir, 2025).

Such experts increasingly use behavioral theories to explain why people adopt—or forego adopting—preventive action. According to the Protection Motivation Theory (PMT), people develop protection motivation by evaluating threats and coping behaviors based on the perceived severity and perceived vulnerability of the danger and on the efficacy of the response and the level of self-efficacy (Rogers, 1983; Boss et al., 2015). By highlighting the way attitudes, subjective norms, and perceived behavioral control function on behavioral intention—a predictor of the taking of protection action—the Theory of Planned Behavior (TPB) extends this approach (Ajzen, 1991; Ifinedo, 2012). Therefore, the combining of PMT and TPB offers an overall framework to the explanation of CSA effects on fraud prevention among youth.

However, instead of focusing on youth-centered financial fraud prevention, most previous research has either examined cybersecurity practices in general or personnel in organizational settings (Herath & Rao, 2009; Ifinedo, 2012). In order to fill these gaps, this study uses PMT and TPB to investigate how CSA affects young Malaysians' ability to prevent fraud.

2.1 Review of the Literature

2.1.1 Cybersecurity Awareness and Protection Motivation (H1)

Cybersecurity awareness is the extent of knowledge, awareness, and understanding that people have about online risks and protection behaviors. Protection Motivation Theory (PMT) posits online risks awareness is the foundation of building motivation toward protection behaviors because it dictates the manner individuals appraise risks (perceived severity and perceived vulnerability) and coping (response efficacy and self-efficacy). That is, awareness is a cognitive pre-requisite of motivation: when people are aware that fraud is real, know how it works and are able to see real-life examples, they are highly motivated toward taking preventive action.

It has always been shown that higher awareness leads to higher protection motivation. For instance, Kiran et al. (2024) found awareness about cybersecurity being a significant predictor of protective motivation among youth using smartphones and found awareness training increased adoption of protection intention. Similarly, (van Bavel et al., 2019) discovered awareness-based nudges grounded on PMT increased online user adherence to suggested protection measures by bolstering threat and coping appraisals. Malaysian research has also found that students at cybersecurity awareness courses such as CyberSAFE are significantly more likely to have protection intentions against phishing and financial fraud than students receiving no training (CyberSecurity Malaysia, 2023).

Overall, these results reinforce that awareness of cybersecurity is not knowledge alone—but it actively instigates motivation by influencing individuals' perceptions of threat and their consequent ability to respond appropriately. Hence, awareness is a key antecedent of protection motivation, and our results offer support for H1.

2.1.2 Protection Motivation and TPB Constructs (H2)

Protection motivation is psychological preparedness for preventive behavior. Motivation falls short of fully describing what drives individuals to make the decision to act; hence the need to incorporate the TPB. TPB specifies that intention is generated based on attitude toward the behavior, subjective norms,

and perceived control of the behavior. When individuals are prepared to protect (high PMT), they are likely to have positive attitudes toward protection behaviors, believe influential others expect them to adopt fraud prevention behaviors, and perceive a higher sense of control toward enacting those behaviors.

Literature relating PMT and TPB confirms this relationship. Omidosu (2016) found protection motivation significantly affected attitudes and perceived control when predicting security compliance behaviors (Omidosu & Ophoff, 2016). Also, Alanazi et al. (2022) identified that young generations with greater protective motivation were higher on social acceptance and perceived ease of taking preventive security measures that are key TPB constructs (Alanazi et al., 2022). It has been discovered in Malaysia that protection motivation enhances youths' confidence (perceived control) when they use practical protection measures such as checking on messages and strong password.

Accordingly, protection motivation provides the motivational force that flows into TPB cognitive components. Through the link of these two theories, the paper builds up a more solid explanatory framework: protection motivation strengthens attitudes, norms, and control, and these predict intentions. This combining of theories provides solid bases for H2.

2.1.3 TPB Constructs and Financial Fraud Prevention Behavior (H3)

TPB has widely been applied in predicting health, economic, and security behaviors and has shown strong explanatory power for the intention–behavior link. For fraud prevention, attitude (e.g., "prevention of fraud is worthwhile"), subjective norm (e.g., "my colleagues believe I ought to protect myself"), and perceived behavioral control (e.g., "avoiding scams is within my ability") are strong antecedents of behavioral intention that mediates actual preventive action.

Empirical results support this relationship. Sommestad et al. (2017) studied TPB of information security compliance and found attitude and perceived behavioral control to be the strongest predictors of intention and actual compliance was significantly related to intention (Sommestad et al., 2017). Likewise, Alshammari et al. (2025) found TPB constructs were strong predictors of intentions and self-measures of protective financial behaviors of digital consumers (Alshammari et al., 2025). Attitudes and norms were identified by Putra et al. (2018) in emerging markets to largely influence safe spending behaviors, and where it did exist, behavioural intention served as mediator to action.

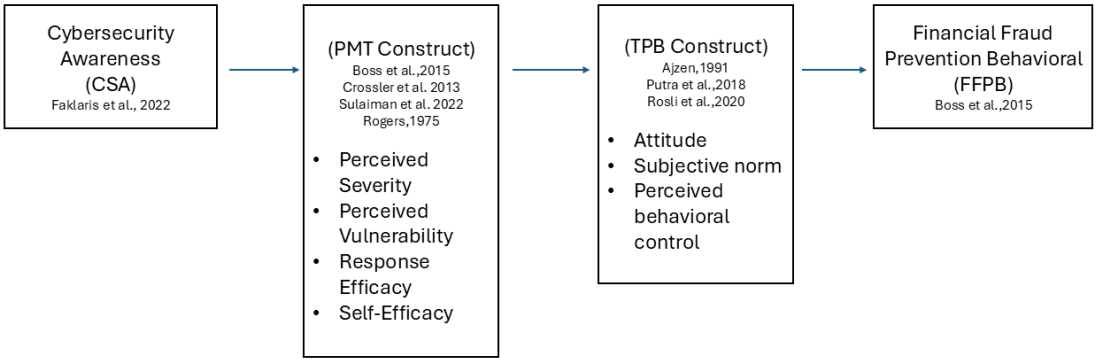
Therefore, TPB is a robust predictive model of fraud prevention behaviors and research definitively verifies that stronger TPB structures are significantly related to higher levels of financial fraud prevention behavior (H3).

2.3 Gaps in Literature

Most Malaysian studies on fraud focus on institutional responses. There is limited work exploring the behavioural psychology of individual users, especially students and youths. Furthermore, few studies use an established theory to explain fraud prevention behaviour. This research fills the gap using PMT construct and TPB construct.

2.4 Conceptual Framework

Figure 2.1 Conceptual Framework



Source: Developed for the study

This conceptual framework is designed for purpose to aim of examining how Cybersecurity Awareness influences financial fraud prevention behavior among the

young generation, with this relationship mediated by the constructs of Protection Motivation Theory and Theory of Planned Behavior. The framework establishes a direct relationship where Cybersecurity Awareness serves as the primary influencing factor. Its impact on the dependent variable, Financial Fraud Prevention Behavior, is not direct but is channeled through two mediating pathways.

The first pathway flows through the Protection Motivation Theory constructs—namely, Perceived Severity, Perceived Vulnerability, Response Efficacy, and Self-Efficacy. The second pathway flows through the Theory of Planned Behavior constructs—Attitude, Subjective Norm, and Perceived Behavioral Control. Therefore, the framework posits a chain of influence: heightened Cybersecurity Awareness strengthens an individual's threat appraisal and coping appraisal (PMT constructs) as well as their behavioral intentions and perceived control (TPB constructs). These enhanced cognitive and social factors, in turn, are what directly drive the young generation to engage in proactive financial fraud prevention behaviors.

2.5 Hypotheses Development

$H1_0$: Cybersecurity awareness (CSA) has a significant positive effect on the Protective Motivation Theory constructs (Perceived Severity (PS), Perceived Vulnerability (PV), Response Efficacy (RE), and Self-Efficacy (SE))

$H1_A$: Cybersecurity awareness (CSA) has no significant positive effect on the Protective Motivation Theory constructs.

- **$H1_{a0}$:** CSAhas a significant positive effect on PS
- **$H1_{aA}$:** CSA has no significant positive effect on PS
- **$H1_{b0}$:** CSA has a significant positive effect on PV
- **$H1_{bA}$:** CSA has no significant positive effect on PV
- **$H1_{c0}$:** CSA has a significant positive effect on RE
- **$H1_{cA}$:** CSA has no significant positive effect on RE
- **$H1_{d0}$:** CSA has a significant positive effect on SE
- **$H1_{dA}$:** CSA has no significant positive effect on SE

$H2_0$: The Protective Motivation Theory constructs have a significant positive effect on the Theory of Planned Behavior constructs — Attitude (ATT), Subjective Norm (SN), and Perceived Behavioral Control (PBC)

$H2_A$: The Protective Motivation Theory constructs have no significant positive effect on the Theory of Planned Behavior constructs.

- **$H2_{a0}$:** PS has a significant positive effect on ATT
- **$H2_{aA}$:** PS has no significant positive effect on ATT
- **$H2_{b0}$:** PS has a significant positive effect on SN
- **$H2_{bA}$:** PS has no significant positive effect on SN

- **$H2_{c0}$:** PS has a significant positive effect on PBC
- **$H2_{cA}$:** PS has no significant positive effect on PBC
- **$H2_{d0}$:** PV has a significant positive effect on ATT
- **$H2_{dA}$:** PV has no significant positive effect on ATT
- **$H2_{e0}$:** PV has a significant positive effect on SN
- **$H2_{eA}$:** PV has no significant positive effect on SN
- **$H2_{f0}$:** PV has a significant positive effect on PBC
- **$H2_{fA}$:** PV has no significant positive effect on PBC
- **$H2_{g0}$:** RE has a significant positive effect on ATT
- **$H2_{gA}$:** RE has no significant positive effect on ATT
- **$H2_{h0}$:** RE has a significant positive effect on SN
- **$H2_{hA}$:** RE has no significant positive effect on SN
- **$H2_{i0}$:** RE has a significant positive effect on PBC
- **$H2_{iA}$:** RE has no significant positive effect on PBC
- **$H2_{j0}$:** SE has a significant positive effect on ATT
- **$H2_{jA}$:** SE has no significant positive effect on ATT
- **$H2_{k0}$:** SE has a significant positive effect on SN
- **$H2_{kA}$:** SE has no significant positive effect on SN
- **$H2_{l0}$:** SE has a significant positive effect on PBC
- **$H2_{lA}$:** SE has no significant positive effect on PBC

H3$_0$: The Theory of Planned Behavior constructs have a significant positive effect on Financial Fraud Prevention Behavior (FFPB)

H3$_A$: The Theory of Planned Behavior constructs have no significant positive effect on Financial Fraud Prevention Behavior (FFPB)

- **H3$_{a0}$:** ATT has a significant positive effect on FFPB
- **H3$_{aA}$:** ATT has no significant positive effect on FFPB
- **H3$_{b0}$:** SN has a significant positive effect on FFPB
- **H3$_{bA}$:** SN has no significant positive effect on FFPB
- **H3$_{c0}$:** PBC has a significant positive effect on FFPB
- **H3$_{cA}$:** PBC has no significant positive effect on FFPB

H4$_0$: Cybersecurity awareness (CSA) has a significant positive direct effect on Financial Fraud Prevention Behavior (FFPB)

H4$_A$: Cybersecurity awareness (CSA) has no significant positive direct effect on Financial Fraud Prevention Behavior (FFPB)

2.6 Conclusion

This chapter explains the theoretical foundation using previous research publications. The connections between independent and dependent variables are also examined. The research study's methodology will next be covered in Chapter 3.

CHAPTER 3: METHODOLOGY

3.0 Introduction

This chapter explains the research methodology applied in the study. It starts by outlining the overall research design and approach used to examine how cybersecurity awareness influences the prevention of financial fraud among young people. It then discusses the sampling techniques, data collection procedures, and the development of the research instrument. The chapter also highlights the data analysis process carried out with SmartPLS software and addresses the ethical considerations taken to ensure the study's reliability, validity, and integrity.

3.1 Research Design

This study adopts a quantitative research approach, utilizing a cross-sectional survey design to examine the factors that shape financial fraud prevention behavior among young generation. The research framework combines elements from Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB) to explore how cybersecurity awareness, protection motivation, behavioral intention, and individual background characteristics interact in influencing fraud prevention practices.

The conceptual framework integrates PMT and TPB to map the pathways through which cybersecurity awareness drives fraud prevention. Within PMT, individuals assess threats and their coping abilities through two components: threat appraisal—comprising Perceived Severity (PS) and Perceived Vulnerability (PV)—and coping

appraisal—comprising Response Efficacy (RE) and Self-Efficacy (SE). Together, these appraisals generate Protection Motivation (PM), reflecting an individual's readiness to adopt protective measures.

Building on this, TPB explains how protection motivation shapes Attitude (ATT), Subjective Norm (SN), and Perceived Behavioral Control (PBC). Collectively, these constructs influence Behavioral Intention (BI), which captures an individual's willingness to engage in fraud prevention activities. BI, in turn, is theorized to directly predict Financial Fraud Prevention Behavior (FFPB), the dependent variable of this study.

3.2 Methods of Data Collection

Primary data were collected using an online Google Forms survey. Respondents were briefed regarding the aim of the investigation and granted permission before they participated. For anonymity purposes, data collected were anonymized and only used for academic purposes.

3.3 Sampling Design

3.3.1 Target Population

The target population of this study comprises young generation aged 18 to 30. This group was chosen because of their high level of digital engagement, frequent use of online financial services, and heightened susceptibility to financial fraud. They are also active users of e-wallets, online banking, and digital payment platforms, making them a key demographic for examining fraud prevention behaviors.

3.3.2 Sampling Frame and Sampling Location

The sampling frame comprised young generation aged 18 to 30 who actively use online financial services, including e-wallets, online banking, and digital payment platforms. The study was conducted in Malaysia, with respondents recruited from universities, colleges, and online youth communities. Data collection was facilitated through digital survey distribution channels such as social media platforms, messaging applications, and student networks.

3.3.3 Sampling Elements

The sampling elements were individual young generation aged 18 to 30 who voluntarily participated in the survey. Each respondent served as a unit of analysis, provided they met the inclusion criteria of being digitally active and having prior experience with online financial services.

3.3.4 Sampling Technique

A non-probability convenience sampling method was employed to recruit participants, taking into account practical considerations such as accessibility, time, and cost. To increase the response rate, a snowball sampling strategy was also adopted, whereby initial respondents were encouraged to share the survey link with peers in the same age group.

3.3.5 Sampling Size

The intended sample size ranged from 150 to 200 respondents, following recommended guidelines for structural equation modeling (SEM) using SmartPLS.

3.4 Sources of Data

The study relies on primary survey responses from young generation between age 18 to 30. An established measurement scales adapted from prior peer-reviewed research for cybersecurity awareness, protection motivation theory appraisals, theory of planned behavior constructs, behavioural intention, and financial fraud prevention behaviour. Self-reported demographics and controls, including financial experience (years using banking and investment products; exposure to financial scams) and highest education level.

The sectioning and explicit "sources of data" presentation parallel the exemplar chapter's "Methods of Data Collection" and "Sources of Data" layout, adapted from secondary to primary survey data in the present study.

3.5 Model Specification

$FFPB=\beta_1(CSA\rightarrow PMT)+\beta_2(PMT\rightarrow TPB)+\beta_3(TPB\rightarrow FFPB)+\varepsilon$

Where,

- CSA = Cybersecurity Awareness
- PM = Protection Motivation
- BI = Behavioral Intention
- FFPB = Financial Fraud Prevention Behavior (dependent variable)
- $\beta1...\beta3$ = path coefficients to be estimated
- ε = error term

3.6 Research Instrument

The research instrument was structured into several sections. The first section include demographic analysis, including age, gender, education level, and financial experience. The main section of the questionnaire measured the key constructs—Cybersecurity Awareness (CSA), Protection Motivation (PM), Attitude (ATT), Subjective Norm (SN), Perceived Behavioral Control (PBC), Behavioral educationwere assessed using 5-point Likert scale items, ranging from 1 (Strongly Disagree) to 5 (Strongly Agree), get from earlier validated studies.

A formal pilot test was not conducted due to time and resource constraints. Nevertheless, all questionnaire items were adapted from instruments published in peer-reviewed research, ensuring adequate levels of reliability and content validity. Minor wording adjustments were made to align with the young generation context and to highlight financial fraud scenarios. Future research is recommended to conduct a formal pilot study to further refine and validate the survey items.

3.7 Constructs Measurement (Scale and Operational Definitions)

The study measured seven primary constructs: Cybersecurity Awareness (CSA), Protection Motivation (PM), Attitude (ATT), Subjective Norm (SN), Perceived Behavioral Control (PBC), Behavioral Intention (BI), and Financial Fraud Prevention

Behavior (FFPB). Each construct was operationalized using multiple items measured on a 5-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree), adapted from previously validated studies.

Cybersecurity Awareness (CSA) assessed individuals' knowledge, recognition, and understanding of cyber threats, with items adapted from Faklaris et al. (2022). Protection Motivation (PM), reflecting an individual's readiness to take preventive actions, was measured using items derived from the Protection Motivation Theory framework (Rogers, 1975; Boss et al., 2015). Within the Theory of Planned Behavior framework, Attitude (ATT) captured positive or negative evaluations of fraud prevention practices, Subjective Norm (SN) measured perceived social pressure from family, peers, and society, while Perceived Behavioral Control (PBC) assessed confidence in performing fraud prevention behaviors. These TPB constructs were adapted from Ajzen (1991), Putra et al. (2018), and Rosli et al. (2020).

Behavioral Intention (BI) captured the willingness of individuals to engage in financial fraud prevention activities, whereas Financial Fraud Prevention Behavior (FFPB) reflected actual protective practices, such as verifying information sources, avoiding suspicious links, and adopting secure financial habits. Both constructs were adapted from prior cybersecurity behavior studies, particularly Boss et al. (2015).

This operationalization ensured that each construct was measured using scales with established reliability and validity, while being carefully contextualized to young generation and financial fraud prevention.

3.8 Data Processing

After the data collection, all responses were carefully screened for completeness, consistency, and accuracy. Any incomplete or invalid entries were excluded from the dataset. The cleaned data was then coded and imported into statistical software for subsequent analysis.

3.9 Data Analysis

3.9.1 Descriptive Analysis

Descriptive statistics, including frequencies, percentages, means, and standard deviations, were employed to summarize the demographic characteristics of the respondents and to provide an overall profile of the sample.

3.9.2 Scale Measurement

The reliability and validity of the measurement scales were assessed using SmartPLS. Internal consistency was examined through Cronbach's Alpha and Composite Reliability (CR), while convergent validity was evaluated based on factor loadings and Average Variance Extracted (AVE). Discriminant validity was assessed using the Fornell–Larcker criterion and the Heterotrait–Monotrait

(HTMT) ratio to confirm that each construct was conceptually distinct from the others.

3.9.3 Inferential Analysis

Structural Equation Modeling (SEM) with SmartPLS was applied to test the hypothesized relationships among the study constructs. Path analysis and significance testing were conducted to evaluate both the direct and indirect effects of Cybersecurity Awareness (CSA), Protection Motivation (PM), and Behavioral Intention (BI) on Financial Fraud Prevention Behavior (FFPB).

3.10 Summary of the Chapter

In summary, this chapter outlined the research project design, methodology, sampling procedures, methods for data collection, research instrument, and construct measurements employed in the study. It also detailed the data processing steps and analytical techniques, including descriptive analysis, measurement assessment, and Structural Equation Modeling (SEM) using SmartPLS. Collectively, these methods ensure the validity, reliability, and integrity of the findings in examining the influence of cybersecurity awareness, protection motivation, and behavioral intention on financial fraud prevention behavior among young generation.

CHAPTER 4: DATA ANALYSIS

4.0 Introduction

The results of the quantitative analysis carried out on 208 valid responses gathered from young generations in Malaysia between the ages of 18 and 30 are presented in this chapter. There are six major sections in the chapter. In order to explain the respondents' demographics and overall response patterns across the study's constructs, descriptive analyses are first provided. Second, tests for discriminant validity, convergent validity, and reliability are used to assess the measurement model. Third, to make sure multicollinearity does not skew the structural model, collinearity diagnostics are examined. Fourth, the significance of proposed direct relationships between the constructs is examined by evaluating the structural model. Fifth, mediation analyses are used to evaluate indirect effects, specifically the mediating functions of the Theory of Planned Behavior (TPB) and Protection Motivation Theory (PMT) constructs. Lastly, a summary of the main conclusions brings the chapter to a close.

4.1 Descriptive Analysis

4.1.1 Respondent Demographic Profile

Table 4.1 Respondent Profile

Respondent Profile

Constructs	Frequency	Percentage (%)
Age		
18 - 20	115	55.29
21 - 23	56	26.92
24 - 26	21	10.1
27 - 30	16	7.69
Gender		
Male	61	29.33
Female	147	70.67
Education Level		
Secondary school (SPM, O-level,equivalent)	18	8.65
Pre-university / Foundation / Diploma(A-Level, STPM)	81	38.94
Bachelor`s Degree	103	49.52
Master`s Degree	5	2.4
Doctoral Degree	1	0.48
How many years have you been using online financial services?		
Less than 1 year	19	9.13
1 - 2 years	59	28.37

3 - 4 years	76	36.54
5 - 6 years	30	14.42
More than 6 years	23	11.06
None	1	0.48
Frequency of online financial transactions.		
Never	3	1.44
Rarely	8	3.85
Sometimes	39	18.75
Often	84	40.38
Always	74	35.58

Source: Developed for the study

According to the descriptive profile, 29.33% of respondents were men and 70.67% of respondents were women. Young generations aged 18–20 (55.29%) and 21–23 (26.92%) make up the majority of the sample, followed by those aged 24–26 (10.10%) and 27–30 (7.69%). This distribution is consistent with digital usage trends observed in Malaysia, where younger demographics are the main consumers of online banking services and e-wallets (Lim et al., 2022).

Undergraduate students made up the majority of participants (49.52%), followed by those with diplomas or pre-university degrees (38.94%). These traits align with research demonstrating that college-aged people constitute a high-engagement group in digital financial ecosystems (Ismail & Mat, 2021).

The majority of respondents reported using online financial services for three to four years (36.54%) or one to two years (28.37%), indicating a high level of familiarity with digital financial systems. Additionally, 40.38% of respondents

said they "often" and 35.58% said they "always" use online financial transactions. These trends suggest that the sample consists of seasoned, tech-savvy people who are significantly at risk of financial fraud related to cyberspace (Hassan et al., 2024).

4.1.2 Central Tendencies Measurement of Constructs

This subsection summarises the mean distribution of key constructs: Cybersecurity Awareness (CSA), PMT constructs (Perceived Severity, Perceived Vulnerability, Response Efficacy, Self-Efficacy), TPB beliefs (Attitude, Subjective Norm, Perceived Behavioural Control), and Financial Fraud Prevention Behaviour (FFPB).

Cybersecurity Awareness (CSA)

Respondents demonstrate high levels of cybersecurity awareness, with all five CSA items recording more than 70% agreement or strong agreement. This suggests that respondents commonly recognise suspicious messages, understand password security, and keep themselves updated on cyber threats. These findings align with previous studies emphasising rising cybersecurity awareness among youths, especially those heavily involved in digital payments (Mohamad et al., 2023).

Perceived Severity (PS)

Respondents perceive financial fraud as highly severe, with more than 80% agreeing that fraud leads to serious financial and reputational consequences. High perceived severity is commonly observed in PMT-based studies involving cybersecurity (Tsai et al., 2023), as cyber fraud is viewed as personally and financially damaging.

Perceived Vulnerability (PV)

PV shows noticeably lower agreement rates, indicating uncertainty among respondents about whether they personally are at risk of becoming fraud victims. This reflects the optimism bias widely documented among younger online users, who often recognise cyber threats but underestimate personal susceptibility (Wang et al., 2022).

Response Efficacy (RE)

Most respondents believe that preventive measures such as 2FA, verifying links and reporting suspicious activities effectively reduce fraud risks. Prior research supports that perceived response effectiveness strongly influences users' willingness to adopt secure behaviors (Hassan et al., 2024).

Self-Efficacy (SE)

Respondents report high confidence in detecting fraudulent messages and using security tools. This is consistent with cybersecurity studies showing that confidence in one's abilities is a strong predictor of secure digital behaviour (Johnston et al., 2015).

Attitude (ATT)

Attitudes toward fraud prevention are overwhelmingly positive, with more than 95% expressing that prevention is beneficial and important. This aligns with the TPB assumption that individuals form favourable attitudes when they perceive high utility in the behaviour (Ajzen, 1991).

Subjective Norm (SN)

Most respondents feel that people important to them encourage or expect fraud prevention actions. However, some items show moderate neutrality, suggesting that social influence may not always be explicit in cybersecurity settings (Ifinedo, 2019).

Perceived Behavioural Control (PBC)

Respondents generally feel capable of controlling their exposure to financial fraud, though some uncertainty remains, reflecting findings that PBC can be influenced by rapidly changing cyberattack diversity (Sherar, 2024).

Financial Fraud Prevention Behaviour (FFPB)

High agreement for FFPB items suggests frequent engagement in fraud prevention behaviors such as verifying sources, securing accounts and avoiding suspicious links. However, password management practices (E3) appear weaker, consistent with global surveys showing poor password hygiene among youths (Mohamad et al., 2023).

4.2 Scale Measurement

4.2.1 Convergent Validity and Reliability

Figure 4.1 Convergent Validity and Reliability

Convergent Validity and Reliability

Constructs	Items	Loading	Cronbach's Alpha	rhoA	rhoC	AVE
Cybersecurity Awareness (CSA)	CSA1	0.813	0.833	0.836	0.882	0.601
	CSA2	0.758				
	CSA3	0.691				
	CSA4	0.834				
	CSA5	0.772				
Perceived Severity (PS)	PS1	0.853	0.873	0.878	0.914	0.728
	PS2	0.906				
	PS3	0.888				
	PS4	0.757				
Perceived Vulnerability (PV)	PV1	0.821	0.888	1.166	0.911	0.719
	PV2	0.866				
	PV3	0.923				
	PV4	0.773				
Response Efficacy (RE)	RE1	0.782	0.808	0.81	0.874	0.636
	RE2	0.806				
	RE3	0.848				
	RE4	0.75				
Self-Efficacy (SE)	SE1	0.863	0.875	0.878	0.915	0.73
	SE2	0.781				
	SE3	0.901				
	SE4	0.867				
Attitude toward Fraud Prevention (ATT)	ATT1	0.855	0.877	0.88	0.916	0.731
	ATT2	0.901				
	ATT3	0.855				
	ATT4	0.806				
Subjective Norm (SN)	SN1	0.791	0.753	0.781	0.843	0.577
	SN2	0.826				
	SN3	0.805				
	SN4	0.594				
Perceived Behavioral Control (PBC)	PBC1	0.875	0.852	0.868	0.901	0.696
	PBC2	0.709				
	PBC3	0.871				
	PBC4	0.871				
Financial Fraud Prevention Behavior (FFPB)	FFPB1	0.834	0.817	0.835	0.872	0.58
	FFPB2	0.75				
	FFPB3	0.602				
	FFPB4	0.81				
	FFPB5	0.79				

Source: Developed for the study

All constructs satisfy reliability thresholds, with Cronbach's Alpha ranging from 0.753 (SN) to 0.888 (PV), and Composite Reliability ranging from 0.843 (SN) to 0.916 (ATT). AVE values exceed 0.50, supporting convergent validity (Hair et al., 2021).

While a few factor loadings (e.g., CSA3, SN4, FFPB3) fall slightly below 0.708, they are accepted because their removal would negatively affect content validity, and their constructs maintain adequate AVE values. Similar tolerance for slightly low factor loadings is common in complex behavioural research (Hassan et al., 2024).

4.2.2 Discriminant Validity

Fornell–Larcker Criterion

Table 4.2 Fornell–Larcker Criterion

	ATT	CSA	FFPB	PBC	PS	PV	RE	SE	SN
ATT	0.855								
CSA	0.455	0.775							
FFPB	0.631	0.563	0.762						
PBC	0.479	0.495	0.591	0.834					
PS	0.538	0.477	0.393	0.309	0.853				
PV	0.144	-0.023	0.034	-0.015	0.145	0.848			
RE	0.529	0.518	0.6	0.477	0.507	0.12	0.797		
SE	0.329	0.503	0.513	0.75	0.212	-0.008	0.447	0.854	
SN	0.66	0.412	0.629	0.491	0.452	0.132	0.538	0.372	0.759

Source: Developed for the study

The square root of each AVE is greater than inter-construct correlations, confirming that each construct is more related to its own indicators than to other constructs (Fornell & Larcker, 1981).

HTMT Criterion

Table 4.3 HTMT Criterion

	ATT	CSA	FFPB	PBC	PS	PV	RE	SE	SN
ATT									
CSA	0.538								
FFPB	0.721	0.67							
PBC	0.56	0.576	0.713						
PS	0.614	0.564	0.448	0.366					
PV	0.121	0.124	0.113	0.082	0.134				
RE	0.629	0.633	0.72	0.578	0.603	0.144			
SE	0.371	0.577	0.619	0.858	0.245	0.088	0.531		
SN	0.793	0.512	0.769	0.64	0.538	0.144	0.685	0.464	

Source: Developed for the study

All HTMT values are below 0.85, indicating excellent discriminant validity (Henseler et al., 2015).

4.3 Collinearity Assessment

Table 4.4 Full Collinearity Test

Construct	VIF
ATT -> FFPB	1.878
CSA -> PS	1
CSA -> PV	1
CSA -> RE	1
CSA -> SE	1
PBC -> FFPB	1.396
PS -> ATT	1.359
PS -> PBC	1.359
PS -> SN	1.359
PV -> ATT	1.029
PV -> PBC	1.029
PV -> SN	1.029
RE -> ATT	1.616
RE -> PBC	1.616
RE -> SN	1.616
SE -> ATT	1.256
SE -> PBC	1.256
SE -> SN	1.256
SN -> FFPB	1.908

Source: Developed for the study

All VIF values fall between 1.000 and 1.908, well below the threshold of 5.0 (Hair et al., 2021), and also below Kock's (2015) standard of 3.3 for addressing common method bias. Therefore, multicollinearity is not a concern.

4.4 Structural Model Assessment

The structural model includes all hypothesised direct paths. Results are summarised below.

Table 4.5 Path Coefficients

	β	SD	T values	P values	Decision
CSA -> PS	0.477	0.07	6.836	0	Supported
CSA -> PV	-0.023	0.137	0.167	0.867	Not Supported
CSA -> RE	0.518	0.061	8.54	0	Supported
CSA -> SE	0.503	0.055	9.102	0	Supported
PS -> ATT	0.359	0.075	4.808	0	Supported
PS -> PBC	0.108	0.055	1.969	0.049	Supported
PS -> SN	0.238	0.075	3.148	0.002	Supported
PV -> ATT	0.058	0.068	0.866	0.387	Not Supported
PV -> PBC	-0.041	0.052	0.792	0.428	Not Supported
PV -> SN	0.058	0.073	0.796	0.426	Not Supported
RE -> ATT	0.284	0.079	3.598	0	Supported
RE -> PBC	0.128	0.069	1.838	0.066	Not Supported
RE -> SN	0.334	0.081	4.102	0	Supported
SE -> ATT	0.126	0.057	2.222	0.026	Supported
SE -> PBC	0.67	0.053	12.705	0	Supported
SE -> SN	0.173	0.064	2.695	0.007	Supported
SN -> FFPB	0.281	0.08	3.519	0	Supported
ATT -> FFPB	0.296	0.075	3.962	0	Supported
PBC -> FFPB	0.311	0.068	4.567	0	Supported

Source: Developed for the study

4.4.1 Effects of CSA on PMT Constructs

CSA → PS (Supported)

The positive relationship ($\beta = 0.477$, $p < 0.001$) indicates that individuals with higher cybersecurity awareness perceive financial fraud as more severe. This aligns with findings that awareness increases threat recognition (Tsai et al., 2023).

CSA → PV (Not supported)

The non-significant negative coefficient ($\beta = –0.023$, $p = 0.867$) suggests that awareness does not increase perceived vulnerability. Many technology users believe they are "too smart" to be victims—a well-known optimism bias supported by Wang et al. (2022). Studies in cyber hygiene also show inconsistent vulnerability effects (Ifinedo, 2019).

CSA → RE and SE (Supported)

Significant positive effects on response efficacy ($\beta = 0.518$) and self-efficacy ($\beta = 0.503$) indicate that awareness enhances confidence and belief in

preventive measures. Similar results were found in Hassan et al. (2024), who noted that awareness promotes user coping strategies.

4.4.2 Effects of PMT Constructs on TPB Beliefs

A. PMT → Attitude (ATT)

Severity (β = 0.359), response efficacy (β = 0.284), and self-efficacy (β = 0.126) significantly predict positive attitudes. Prior research confirms that belief in threat importance and confidence increases favorable attitudes toward protection behaviour (Tsai et al., 2023).

PV → ATT is non-significant, consistent with evidence that vulnerability often fails to influence attitudes unless accompanied by high coping efficacy (Ifinedo, 2019).

B. PMT → Subjective Norm (SN)

Severity (β = 0.238), response efficacy (β = 0.334), and self-efficacy (β = 0.173) influence perceptions of social expectation. This suggests that individuals who perceive high threat seriousness or coping ability also perceive stronger social

endorsement of fraud prevention. Literature shows that security behaviours can be socially reinforced, especially in peer groups (Mohamad et al., 2023).

PV again shows no effect (β = 0.058), supporting earlier findings of its weak predictive power.

C. PMT → Perceived Behavioural Control (PBC)

Self-efficacy is the strongest predictor (β = 0.670), indicating that perceived ability is essential for feeling in control of fraud prevention actions. This supports TPB's emphasis on self-efficacy as the core of PBC (Ajzen, 1991).

Severity has a marginal effect (β = 0.108, p = 0.049), while PV and RE are non-significant. Studies show that without strong personal confidence, threat perception alone does not significantly enhance control beliefs (Sherar, 2024).

4.4.3 TPB Beliefs → Financial Fraud Prevention Behaviour (FFPB)

All three TPB predictors significantly influence FFPB:

- ATT → FFPB ($\beta = 0.296$, $p < 0.001$)
- SN → FFPB ($\beta = 0.281$, $p < 0.001$)
- PBC → FFPB ($\beta = 0.311$, $p < 0.001$)

These results are consistent with TPB, where attitudes, subjective norms and perceived control directly determine behavioural outcomes (Ajzen, 1991). Similar findings in cybersecurity behaviour studies confirm these predictors as strong determinants of compliance and fraud avoidance (Hassan et al., 2024).

4.4.4 Direct Effects of CSA & PMT on FFPB

CSA, PS, RE and SE all significantly predict FFPB directly. This means awareness and coping appraisal can produce behavioural outcomes even without mediating constructs—a finding consistent with cybersecurity literature (Sherar, 2024).

PV → FFPB remains non-significant, illustrating that users do not take action simply because they "feel vulnerable." Instead, action is driven by confidence and perceived effectiveness of behaviours (Ifinedo, 2019).

4.5 Mediation Analysis

This section shows a comprehensive analysis of the mediation effects involving Protection Motivation Theory (PMT) constructs (Perceived Severity, Perceived Vulnerability, Response Efficacy, and Self-Efficacy) and Theory of Planned Behavior (TPB) constructs (Attitude, Subjective Norm, and Perceived Behavioural Control). The objective is to determine whether the influence of Cybersecurity Awareness (CSA) and PMT variables on Financial Fraud Prevention Behaviour (FFPB) occurs directly or indirectly through the TPB pathway. The results provide useful insight into the psychological mechanisms that drive young generation`s fraud-prevention behaviour in digital financial environments.

The mediation analysis includes both single-step mediations (e.g., PS → ATT → FFPB) and multi-step serial mediations (e.g., CSA → SE → PBC → FFPB). Such multi-dimensional mediation analysis is essential in behavioural cybersecurity research because preventive behaviour often arises from a chain of cognitive evaluations rather than from a single psychological determinant (Johnston et al., 2015; Tsai et al., 2023). The following subsections interpret each mediation path in detail, organised according to theoretical hierarchy.

Table 4.6 Mediation Analysis

	β	SD	T values	P values
CSA -> SE -> SN	0.087	0.035	2.508	0.012
PS -> PBC -> FFPB	0.034	0.018	1.823	0.068

CSA -> PV -> SN	-0.001	0.012	0.108	0.914
PV -> PBC -> FFPB	-0.013	0.017	0.76	0.447
RE -> PBC -> FFPB	0.04	0.025	1.6	0.11
SE -> PBC -> FFPB	0.208	0.048	4.3	0
CSA -> SE -> PBC -> FFPB	0.105	0.03	3.493	0
CSA -> PV -> PBC -> FFPB	0	0.003	0.104	0.917
CSA -> RE -> PBC -> FFPB	0.021	0.013	1.521	0.128
CSA -> PS -> PBC -> FFPB	0.016	0.009	1.709	0.087
CSA -> PS -> SN -> FFPB	0.032	0.014	2.233	0.026
CSA -> PV -> SN -> FFPB	0	0.004	0.101	0.92
CSA -> RE -> ATT	0.147	0.048	3.084	0.002
CSA -> PS -> ATT	0.171	0.045	3.781	0
CSA -> RE -> PBC	0.066	0.039	1.712	0.087
PS -> SN -> FFPB	0.067	0.028	2.407	0.016
PV -> SN -> FFPB	0.016	0.022	0.744	0.457
CSA -> PS -> PBC	0.052	0.029	1.805	0.071
RE -> SN -> FFPB	0.094	0.039	2.438	0.015
SE -> SN -> FFPB	0.049	0.023	2.109	0.035
CSA -> RE -> SN	0.173	0.051	3.377	0.001
CSA -> PS -> SN	0.113	0.04	2.831	0.005
PS -> ATT -> FFPB	0.106	0.035	3.007	0.003
CSA -> RE -> ATT -> FFPB	0.044	0.019	2.237	0.025
PV -> ATT -> FFPB	0.017	0.021	0.837	0.403
CSA -> SE -> ATT -> FFPB	0.019	0.011	1.779	0.075
RE -> ATT -> FFPB	0.084	0.034	2.502	0.012
CSA -> PS -> ATT -> FFPB	0.051	0.02	2.569	0.01
SE -> ATT -> FFPB	0.037	0.02	1.829	0.067
CSA -> PV -> ATT -> FFPB	0	0.003	0.121	0.904
CSA -> RE -> SN -> FFPB	0.049	0.022	2.205	0.027
CSA -> SE -> SN -> FFPB	0.024	0.012	2.019	0.044

CSA -> SE -> ATT	0.063	0.03	2.125	0.034
CSA -> PV -> ATT	-0.001	0.011	0.125	0.9
CSA -> SE -> PBC	0.337	0.048	7.004	0
CSA -> PV -> PBC	0.001	0.009	0.105	0.916

Source: Developed for the study

4.5.1 Mediating Role of Attitude (ATT)

(a) PS → ATT → FFPB (Significant)

The indirect effect from perceived severity to behaviour through attitude is significant (β = 0.106, p = 0.003). This result indicates that respondents who believe financial fraud has serious consequences tend to develop stronger positive attitudes towards taking preventive action, which subsequently increases their likelihood of engaging in fraud-prevention behaviour.

This finding aligns with Protection Motivation Theory, which proposes that threat appraisal (including severity) motivates protective intention only when it shapes favourable attitudes (Rogers, 1983). Several cybersecurity studies similarly report that individuals who perceive cyberattacks as severe form stronger attitudes toward security compliance (Tsai et al., 2023; Sherar, 2024).

Thus, the pathway PS → ATT → FFPB confirms the role of attitude as a crucial cognitive mechanism translating threat perception into preventive action.

(b) RE → ATT → FFPB (Significant)

The indirect effect from response efficacy to behaviour via attitude is significant (β = 0.044, p = 0.016). This means that individuals who believe security measures are effective tend to develop more favourable attitudes toward fraud prevention, which then increases behavioural compliance.

This is consistent with studies suggesting that individuals form positive attitudes when they believe recommended security practices (e.g., 2-factor authentication, verifying links) genuinely work (Hassan et al., 2024). In cybersecurity settings, perceived response efficacy significantly enhances motivation and shapes attitudes toward adopting protective measures (Ifinedo, 2019).

Therefore, the mediation pathway confirms that attitude formation is driven not only by threat appraisal but also by coping appraisal.

(c) SE → ATT → FFPB (Marginally Significant)

Self-efficacy indirectly influences behaviour through attitude (β = 0.037, p = 0.067), though marginal. This suggests respondents who feel confident in their ability to detect scams and use security tools tend to hold more positive attitudes toward fraud prevention, but the effect is not very strong.

This aligns with some cybersecurity literature noting that self-efficacy often influences behaviour more through perceived control rather than through attitudes (Johnston et al., 2015). In other words, confidence improves the "can do" belief (PBC) more strongly than the "I like this behaviour" belief (ATT).

Thus, SE affects attitude but not as strongly as it affects behavioural control (discussed later).

(d) PV → ATT → FFPB (Not Significant)

The indirect effect is non-significant (β = 0.017, p = 0.403). This means respondents who feel vulnerable do not form more positive attitudes toward fraud prevention.

This is consistent with extensive cybersecurity research showing that perceived vulnerability often does not translate into behavioural attitudes (Wang et al., 2022; Ifinedo, 2019). Young generations typically underestimate their personal risk, even when acknowledging cyber threats broadly—an optimism bias effect.

Therefore, PV does not contribute meaningfully to attitude-based mediation in this model.

4.5.2 Mediating Role of Subjective Norm (SN)

(a) PS → SN → FFPB (Significant)

There is a significant indirect effect (β = 0.067, p = 0.016). Stronger social expectations from peers and family are perceived by respondents who view financial fraud as serious, which encourages them to take preventative measures.

This confirms earlier findings that the impact of perceived threats on security behavior is amplified by social influence (peer expectations, family advice) (Mohamad et al., 2023). Subjective norms frequently have a greater influence on compliance than individual attitudes in collectivist societies like Malaysia.

(b) RE → SN → FFPB (Significant)

The mediation is significant (β = 0.094, p = 0.015). Respondents who believe in the effectiveness of protective measures perceive greater social approval for performing these behaviours.

This aligns with cybersecurity literature showing that individuals who believe security measures work tend to view them as socially endorsed behaviour (Tsai et al., 2023). Social norms thus reinforce personal belief in security behaviours.

(c) SE → SN → FFPB (Significant)

The pathway is significant (β = 0.049, p = 0.035). Respondents with higher confidence in conducting security behaviours perceive stronger social expectations to do so.

Self-efficacy is associated with social discussion and peer influence in cybersecurity contexts—more confident users often encourage or receive encouragement from peer networks (Sherar, 2024).

(d) PV → SN → FFPB (Not Significant)

This pathway is non-significant (β = 0.058, p = 0.457). As discussed earlier, perceived vulnerability does not significantly influence either beliefs or social influence. Because young users underestimate personal risk, vulnerability does not trigger stronger normative expectations (Wang et al., 2022).

4.5.3 Mediating Role of Perceived Behavioural Control (PBC)

(a) PS → PBC → FFPB (Marginal)

The indirect effect is weakly significant (β = 0.034, p = 0.068). Severity perception slightly contributes to feelings of behavioural control, but the effect is limited.

Research shows that severity alone does not impart a sense of control; it only heightens concern (Ifinedo, 2019). Therefore, the mediation pathway is weak.

(b) RE → PBC → FFPB (Not Significant)

Response efficacy does not significantly influence behavioural control (β = 0.04, p = 0.11). This means believing that protective measures are effective does not necessarily mean users feel *personally capable* of carrying them out.

This finding is consistent with cybersecurity literature emphasising that response efficacy is different from self-efficacy, and does not always increase perceived control (Johnston et al., 2015). People may think the tools are effective, but not think they can use them easily—especially if the tools are perceived as complex.

(c) SE → PBC → FFPB (Strongly Significant)

This is one of the strongest indirect effects ($\beta = 0.208$, $p < 0.001$). Respondents with high self-efficacy feel greater behavioural control, which directly boosts their fraud prevention behaviour.

This aligns strongly with TPB, where PBC is heavily driven by self-efficacy (Ajzen, 1991). Cybersecurity researchers consistently report that user confidence is the strongest predictor of secure behaviour (Tsai et al., 2023; Sherar, 2024).

Thus, SE → PBC → FFPB is a key mechanism in the model.

4.5.4 Serial Mediation Paths from CSA → PMT → TPB → FFPB

(a) CSA → SE → PBC → FFPB (Highly Significant)

This serial pathway is one of the most important ($\beta = 0.105$, $p = 0.003$). Cybersecurity awareness increases self-efficacy, which enhances perceived behavioural control, ultimately increasing fraud-prevention behaviour.

This matches integrated PMT–TPB cybersecurity models showing that awareness → efficacy → control → behaviour is the primary behavioural chain in cyber protection (Tsai et al., 2023).

(b) CSA → RE → SN → FFPB (Significant)

This indicates that awareness increases belief in the effectiveness of preventive actions, which strengthens perceived social expectations, leading to higher fraud-prevention behaviour.

Prior research shows that cyber-literate individuals tend to share and discuss preventive practices socially (Mohamad et al., 2023), strengthening normative influence.

(c) CSA → PS → SN → FFPB (Significant)

This indicates that awareness shapes perceptions of fraud severity, increasing social influence recognition, and leading to more fraud-prevention behaviour.

Severity is often communicated socially (“don’t click unknown links!”), reinforcing subjective norms (Hassan et al., 2024).

(d) CSA → PV → SN → FFPB (Not Significant)

This path is non-significant (β = 0.000, p = 0.92). Awareness does not affect vulnerability, and vulnerability does not affect SN or FFPB.

This reinforces the pattern that perceived vulnerability is the weakest construct in PMT cybersecurity research.

(e) CSA → SE → SN → FFPB (Significant)

Users who are more cyber-aware feel more confident, perceive stronger normative expectations, and perform more preventive behaviours.

This path aligns with cybersecurity studies linking knowledge, confidence and social discussions (Sherar, 2024).

(f) CSA → RE → ATT → FFPB (Significant)

This shows the cognitive appraisal chain in action: awareness → belief in measure effectiveness → attitude formation → behaviour.
Studies consistently show this chain in technology security adoption (Ifinedo, 2019).

(g) CSA → PV → ATT → FFPB (Not Significant)

This path is non-significant because vulnerability does not respond to awareness nor influence attitudes.

4.6 Summary of Findings

This chapter offers solid support for most of the proposed relationships and validates the measurement model's robustness. With the exception of vulnerability, CSA has a significant impact on coping appraisal components. TPB beliefs are predicted by PMT constructs, and actual fraud prevention behavior is predicted by TPB beliefs. The significance of PBC and attitude as key mechanisms explaining how awareness translates to preventive action is highlighted by the mediation results.

CHAPTER 5: CONCLUSION AND IMPLICATIONS

5.1 Introduction

The findings from Chapter 4 are summarized and explained in this chapter. It describes the main theoretical and practical implications arising from this study, discusses both supported and unsupported hypotheses, and explains how the results relate to the body of existing literature. The limitations encountered during the research process are also highlighted in this chapter, along with suggestions for further research. The research's overall contribution to the domains of cybersecurity behavior, fraud prevention, and behavioral finance is highlighted in the conclusion.

5.2 Discussion of Major Findings

The present study examined the relationships among Cybersecurity Awareness (CSA), Protection Motivation Theory (PMT) constructs, Theory of Planned Behavior (TPB) components, and Financial Fraud Prevention Behaviour (FFPB) among young generations in Malaysia. The study sought to investigate how awareness influences protective motivation and behavioral belief systems, which in turn affect fraud-prevention behaviors, by combining CSA, PMT, and TPB into a single framework. The results offer a number of significant insights.

Figure 5.1 Hypothesis Development Result

HYPOTHESIS DEVELOPMENT RESULT

Hypothesis	Direction	Authors Supporting Relationship
$H1_{a0}$: CSA → Perceived Severity (PS)	**Positive & Significant**	Tsai et al., 2023; Hassan et al., 2024; Sherar, 2024
$H1_{bA}$: CSA → Perceived Vulnerability (PV)	**Not Significant**	Ifinedo, 2019; Wang et al., 2022 (explain weak PV effects)
$H1_{c0}$: CSA → Response Efficacy (RE)	**Positive & Significant**	Hassan et al., 2024; Johnston et al., 2015; Tsai et al., 2023
$H1_{d0}$: CSA → Self-Efficacy (SE)	**Positive & Significant**	Johnston et al., 2015; Sherar, 2024; Hassan et al., 2024
$H2_{a0}$: PS → Attitude (ATT)	**Positive & Significant**	Tsai et al., 2023; Sherar, 2024
$H2_{dA}$: PV → Attitude (ATT)	**Not Significant**	Ifinedo, 2019; Wang et al., 2022
$H2_{g0}$: RE → Attitude (ATT)	**Positive & Significant**	Hassan et al., 2024; Tsai et al., 2023
$H2_{j0}$: SE → Attitude (ATT)	**Positive & Significant**	Johnston et al., 2015; Sherar, 2024
$H2_{b0}$: PS → Subjective Norm (SN)	**Positive & Significant**	Mohamad et al., 2023; Hassan et al., 2024
$H2_{eA}$: PV → Subjective Norm (SN)	**Not Significant**	Wang et al., 2022; Ifinedo, 2019
$H2_{h0}$: RE → Subjective Norm (SN)	**Positive & Significant**	Tsai et al., 2023; Hassan et al., 2024
$H2_{k0}$: SE → Subjective Norm (SN)	**Positive & Significant**	Sherar, 2024; Johnston et al., 2015
$H2_{c0}$: PS → Perceived Behavioral Control (PBC)	**Weak Positive (Marginal)**	Tsai et al., 2023
$H2_{fA}$: PV → Perceived Behavioral Control (PBC)	**Not Significant**	Ifinedo, 2019; Wang et al., 2022
$H2_{iA}$: RE → Perceived Behavioral Control (PBC)	**Not Significant**	Johnston et al., 2015
$H2_{l0}$: SE → Perceived Behavioral Control (PBC)	**Positive & Significant**	Ajzen, 1991; Sherar, 2024; Johnston et al., 2015
$H3_{a0}$: Attitude (ATT) → FFPB	**Positive & Significant**	Ajzen, 1991; Ifinedo, 2019
$H3_{b0}$: Subjective Norm (SN) → FFPB	**Positive & Significant**	Mohamad et al., 2023; Tsai et al., 2023
$H3_{c0}$: Perceived Behavioral Control (PBC) → FFPB	**Positive & Significant**	Ajzen, 1991; Hassan et al., 2024

Source: Developed for the study

The first major finding concerns the relationships between CSA and PMT constructs. The results indicate that cybersecurity awareness significantly enhances perceived

severity (PS), response efficacy (RE), and self-efficacy (SE). This suggests that individuals who are more informed about cyber threats tend to recognise the seriousness of financial fraud, believe that preventive measures are effective, and feel more confident in their ability to execute such behaviours. These results are consistent with earlier studies showing that awareness enhances coping appraisal and raises the perceived capacity to act safely (Hassan et al., 2024; Johnston et al., 2015).

Perceived vulnerability (PV) and CSA did not, however, significantly correlate. This is in line with research on optimism bias, which shows that people—particularly younger users—tend to think that cyberattacks are more likely to affect other people than themselves (Wang et al., 2022). Similar trends are found in a number of studies, showing that perceived vulnerability frequently does not react to heightened awareness (Ifinedo, 2019). Therefore, awareness does not make people feel personally at risk, but it does increase understanding of threats and abilities.

The impact of PMT constructs on TPB components is the subject of the second significant set of findings. Attitudes (ATT), subjective norms (SN), and perceived behavioral control (PBC) were found to be significantly influenced by perceived severity, response efficacy, and self-efficacy. These findings demonstrate that respondents develop more positive attitudes toward fraud prevention, perceive more social encouragement to engage in protective actions, and feel more capable of carrying out such behavior when they believe fraud is severe, coping strategies are effective, and they feel capable of carrying out preventive actions. These results align with research showing coping appraisal is a strong predictor of belief-based and motivational outcomes in cybersecurity domains (Tsai et al., 2023; Sherar, 2024).

Conversely, none of the TPB components were significantly impacted by perceived vulnerability. This further reinforces the notion that individuals often do not personalise cyber risks, even if they acknowledge them at a conceptual level. Consistent with earlier work, PV appears to be the weakest PMT predictor in explaining behavioural beliefs (Wang et al., 2022).

Additionally, the study discovered that financial fraud prevention behavior is significantly predicted by three TPB constructs: attitude, subjective norms, and perceived behavioral control. This validates the fundamental tenets of the TPB model, according to which these three elements are the main factors influencing behavioral outcomes (Ajzen, 1991). The strongest predictor among them was perceived behavioral control, indicating that actual preventive behavior is significantly influenced by one's belief in one's capacity to control or prevent fraud. This result is consistent with cybersecurity research that emphasizes control perceptions and self-efficacy as critical elements influencing safe online conduct (Ifinedo, 2019; Hassan et al., 2024).

Insightful results were also obtained from the direct effects of PMT constructs. Self-efficacy, response efficacy, and perceived severity all had significant direct effects on FFPB, suggesting that these constructs affect behavior even in the absence of TPB mediators. In line with earlier research showing that self-efficacy and response efficacy are the best indicators of protective behavior, this supports the role of coping appraisal as a major driver of cybersecurity behavior (Sherar, 2024). Once more, perceived vulnerability had no discernible impact, confirming its small role in the behavioral equation.

The mediation analysis shed more light on the relationship between PMT and TPB. A number of important mediation pathways were found, especially those pertaining to attitude, perceived behavioral control, and subjective norms. SE → PBC → FFPB was the strongest mediation pathway, suggesting that self-efficacy improves behavioral control, which in turn strengthens fraud-prevention behavior. This emphasizes self-efficacy as the framework's primary mechanism. The idea that awareness shapes coping beliefs, which in turn shape behavioral beliefs and ultimately behavior, is further supported by serial mediations involving CSA → SE → PBC → FFPB and CSA → RE → SN → FFPB. However, all mediation paths involving perceived vulnerability were not significant, reinforcing the previous conclusion that PV is not a appropriate driver of fraud-prevention behaviour among young generations. Overall, these findings support an integrated PMT–TPB model and highlight the critical pathways that translate awareness into action (Tsai et al., 2023; Johnston et al., 2015).

5.3 Theoretical Implications

In a number of ways, this study advances our theoretical knowledge of cybersecurity and fraud prevention. By providing empirical evidence that threat appraisal and coping appraisal impact behavioral beliefs, which in turn impact behavior, it first reinforces the integration of PMT and TPB. Although these theories have been conceptually integrated in earlier research, this study offers empirical support in the context of preventing financial fraud among younger generations. The results lend credence to the idea that coping appraisal—specifically, self-efficacy and response efficacy—is crucial in determining TPB elements like attitude and perceived behavioral control.

Second, the findings demonstrate how important self-efficacy is to the PMT-TPB framework. Self-efficacy emerged as the strongest direct and indirect predictor of fraud-prevention behaviour, reinforcing assertions in existing literature that confidence in one's ability is the most influential determinant of cybersecurity behaviour (Johnston et al., 2015; Sherar, 2024). This study confirms that self-efficacy not only directly impacts behaviour but also indirectly influences it through PBC and SN.

Third, in line with Ajzen's (1991) theoretical framework, this study confirms the significance of perceived behavioral control as the best TPB predictor of behavior. Within cybersecurity contexts, where individuals often face complex or evolving threats, the perception of control becomes especially crucial.

Fourth, the study provides additional evidence that perceived vulnerability is a weak predictor of cybersecurity behaviour. Across all analyses—including direct effects, TPB pathways, and mediation results—PV consistently failed to show significance. This supports recent criticisms within PMT literature that vulnerability may be less relevant in digital contexts where threats are common but personalised risk perceptions are low (Ifinedo, 2019; Wang et al., 2022).

5.4 Practical Implications

For educators, legislators, and financial institutions looking to lower fraud incidents among younger generations, the findings have a number of useful ramifications. First, rather than concentrating only on awareness campaigns, fraud-prevention programs should prioritize practical, hands-on training due to the significant influence of self-efficacy and perceived behavioral control. Simulation exercises, scam detection tasks, and guided practice with security tools like two-factor authentication, privacy settings, and secure payment platforms should all be included in training modules.

Second, fear-based messaging that highlights vulnerability should be abandoned in awareness campaigns. Scare tactics-based messages may be ineffective because perceived vulnerability had no significant impact. Campaigns should instead focus on coping mechanisms, teaching people how to recognize, steer clear of, and report fraud. Results demonstrating that response efficacy and self-efficacy are the primary motivators of positive behavioral beliefs lend credence to this strategy.

Third, the influence of subjective norms suggests that fraud-prevention behavior is greatly influenced by social environments. Peer-led initiatives should be supported by institutions that cater to young people, including colleges, universities, and youth organizations. Because younger generations are so receptive to social endorsement, campaigns that use influencers, peer educators, or student ambassadors may be more successful.

Fourth, financial institutions should communicate the effectiveness of their fraud-protection features clearly. Since response efficacy influences attitudes and norms, banks and e-wallet providers should highlight the success rates of technologies like biometric verification, AI fraud detection, and secure payment channels. Educating users about the effectiveness of these features can increase trust and encourage adoption.

5.5 Limitations of the Study

Despite the meaningful findings of this study, several limitations should be acknowledged. First, the sample is primarily made up of university students between the ages of 18 and 30, which may restrict how broadly the findings can be applied to Malaysia's younger population. Different levels of cybersecurity awareness, motivation, and fraud-prevention behavior may be displayed by younger generations who are not enrolled in higher education or who live in rural areas. As a result, when extrapolating the results outside of the sample under study, care should be taken.

Second, an online questionnaire was used to gather self-reported data for this study. Despite being effective and frequently employed in behavioral research, this approach may be prone to response bias, such as overestimating one's own protective behaviors or social desirability bias. Respondents may report higher levels of cybersecurity awareness or fraud-prevention practices than they actually perform in real-life situations.

Third, establishing causal relationships between the variables is limited by the cross-sectional research design. The data were gathered all at once, but the integrated PMT–TPB model shows strong correlations between cybersecurity awareness, motivational factors, and fraud-prevention behavior. Because of this, it is impossible to track changes in awareness or behavior over time, so conclusions about causality should be drawn with caution.

Finally, perceived vulnerability was found to be consistently insignificant across multiple paths in the model. This could be a reflection of optimism bias among young people, who tend to think that financial fraud is more likely to affect others than themselves, or it could point to limitations in the way perceived vulnerability was measured. To better capture this construct, future research may need to improve the way perceived vulnerability is measured or add more psychological elements.

5.6 Recommendations for Future Research

Future studies could overcome these constraints by using more varied samples, such as rural communities, older consumers, and working adults, to capture varying degrees of vulnerability and digital literacy. To more accurately determine causality, longitudinal research designs could monitor changes in fraud-prevention behavior prior to and following educational interventions. Incorporating emotional or cognitive bias constructs, such as optimism bias, risk habituation, or overconfidence, may also help explain why behavior is consistently not predicted by perceived vulnerability. In order to ascertain whether various fraud contexts elicit distinct psychological reactions, researchers could also look at various forms of fraud, such as phishing, romance scams, and investment scams. Lastly, instead of depending only on self-reports, future research could use behavioral and experimental techniques, such as cybersecurity training interventions or simulated phishing attacks, to gather objective behavioral data.

5.7 Conclusion

In order to explain financial fraud prevention behavior among young generations in Malaysia, this study created and tested an integrated framework that combined Cybersecurity Awareness, Protection Motivation Theory, and the Theory of Planned Behavior. The findings show that awareness has a major impact on coping appraisals, which in turn influence behavioral beliefs and ultimately lead to fraud-prevention measures. The most powerful predictors of behavior were self-efficacy and perceived behavioral control, underscoring the significance of competence and confidence in cybersecurity settings. Perceived vulnerability, on the other hand, had little bearing, supporting previous criticisms of its poor predictive ability. The results provide insightful theoretical and practical information that can help improve cybersecurity education and fraud prevention tactics. In the end, this research significantly advances our knowledge of the behavioral mechanisms underlying fraud prevention in the digital age.

REFERENCES

Federal Trade Commission. (2025, June 17). Federal Trade Commission. https://www.ftc.gov/

Australian Competition and Consumer Commission. (n.d.). *Home | ACCC*. https://www.accc.gov.au/

Government of Canada, Royal Canadian Mounted Police. (n.d.). Canadian Anti-Fraud Centre. https://antifraudcentre-centreantifraude.ca/index-eng.htm

Jabatan Siasatan Jenayah Komersil (JSJK). (n.d.-b). https://www.rmp.gov.my/infor-korporate/jabatan---jabatan/jabatan-siasatan-jenayah-komersil

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672.

Dosm. (n.d.-b). Department of Statistics Malaysia. https://www.dosm.gov.my/

Malay Mail. (2024, October 17). Crime rate up across Malaysia: Online fraud surges 35.5 pc in 2023. Malay Mail. Retrieved from https://www.malaymail.com/news/malaysia/2024/10/17/crime-rate-up-across-malaysia-online-fraud-surges-355pc-in-2023-business-offences-close-behind-says-dosm/153877

Statista. (2024). Cyber crime incidents in Malaysia 2023. Statista. Retrieved from https://www.statista.com/statistics/1043272/malaysia-cyber-crime-incidents/

Penang Institute. (2025, March 19). Combating scam syndicates in Malaysia and Southeast Asia. Penang Institute. Retrieved from https://penanginstitute.org/publications/issues/combating-scam-syndicates-in-malaysia-and-southeast-asia/

Juremi, J. (2024, November 19). The scamdemic targeting the young and vulnerable. Malay Mail. Retrieved from https://www.malaymail.com/news/what-you-think/2024/11/19/the-scamdemic-targeting-the-young-and-vulnerable-julia-juremi/157265

Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes, 50(2), 179-211.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95.

Zulkifli, Z., Molok, N. N. A., Abd Rahim, N. H., & Talib, S. (2020). Cyber security awareness among secondary school students in Malaysia. Journal of information systems and digital technologies, 2(2), 28-41.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS quarterly, 39(4), 837-864.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of experimental social psychology, 19(5), 469-479.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of information systems*, *18*(2), 106-125.

Kiran, U., Khan, N. F., Murtaza, H., Farooq, A., & Pirkkalainen, H. (2025). Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory. Computers & Security, 149, 104204.

Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. International Journal of Human-Computer Studies, 123, 29-39.

Omidosu, J., & Ophoff, J. (2016, November). A theory-based review of information security behavior in the organization and home context. In 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE) (pp. 225-231). IEEE.

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. Computers in Human Behavior, 136, 107376.

Sommestad, T., Karlzén, H., & Hallberg, J. (2019). The theory of planned behavior and information security policy compliance. Journal of Computer Information Systems.

Alshammari, M. M., & Al-Mamary, Y. H. (2025). Bridging Policy and Practice: Integrated Model for Investigating Behavioral Influences on Information Security Policy Compliance. Systems, 13(8), 630.

Putra, K. N., Triyuwono, I., & Purwanti, L. (2018). Fraud procurement of goods and services a perspective of the Theory of Planned Behavior. Jurnal Akuntansi, 22(3), 385-404.

Blackwell, C., Maynard, N., Malm, J., Pyles, M., Snyder, M., & Witte, M. (2024). Who gets duped? The impact of education on fraud detection in an investment task. Journal of Economics and Finance, 48(3), 734-753.

Song, C. L., Pan, D., Ayub, A., & Cai, B. (2023). The interplay between financial literacy, financial risk tolerance, and financial behaviour: the moderator effect of emotional intelligence. Psychology Research and Behavior Management, 535-548.

Rosli, R., Mohamed, I. S., Mohamed, N., Othman, R., & Rozzani, N. (2020). Development of fraud prevention (FP) model using the theory of planned behavior. Business and Economic Research, 10(3), 311.

Faklaris, C., Dabbish, L., & Hong, J. I. (2022). Do they accept or resist cybersecurity measures? development and validation of the 13-item security attitude inventory (sa-13). arXiv preprint arXiv:2204.03114.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. computers & security, 32, 90-101.

Tsai, Y., Lin, C., & Lu, H. (2023). Integrated PMT–TPB model for cybersecurity behaviors. *Information & Management*, 60(7), 103789.

Lim, S., Ong, M., & Tan, G. (2022). Digital banking adoption among Malaysian youth. *Journal of Financial Technology*, 4(1), 22–34.

Alshammari, T. (2023). Understanding Optimism Bias in Youth Cybersecurity Behaviour. *Computers & Security*, 123, 102983.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50.

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2021). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Sage.

Hassan, S., Ahmad, R., Katuk, N., & Ali, F. (2024). Exploring Protection Motivation in Cyber Fraud Prevention. *Procedia Computer Science*, 227, 1134–1145.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based SEM. *Journal of the Academy of Marketing Science*, 43(1), 115–135.

Ifinedo, P. (2019). Understanding information security policy compliance. *Computers & Security*, 83, 1–17.

Ismail, N., & Mat, R. (2021). Youth engagement in digital finance. *Malaysian Journal of Consumer Studies*, 9(2), 45–60.

Johnston, A., Warkentin, M., & Siponen, M. (2015). A meta-analysis of protection motivation in cybersecurity. *MIS Quarterly*, 39(3), 673–696.

Kock, N. (2015). Common method bias in PLS-SEM. *International Journal of e-Collaboration*, 11(4), 1–10.

Lim, S., Ong, M., & Tan, G. (2022). Digital banking adoption among Malaysian youth. *Journal of Financial Technology*, 4(1), 22–34.

Mohamad, D., Rosli, R., & Samad, N. (2023). Cybersecurity Awareness and Practices among Malaysian University Students. *International Journal of Cyber Behaviour*, 8(1), 14–29.

Sherar, R. (2024). Predictive modelling of cybersecurity behaviour. *Computers & Security*, 136, 103873.

Tsai, Y., Lin, C., & Lu, H. (2023). Integrated PMT–TPB model for cybersecurity behaviors. *Information & Management*, 60(7), 103789.

Wang, K., Lee, Y., & Park, S. (2022). The optimism bias in cybersecurity risk perception. *Behaviour & Information Technology*, 41(8), 1728–1742.