University of Strathclyde

Department of Computer and Information Science

The Disconnect Between Cyber Knowledge and Cyber Behaviour by Malaysian Youngsters'

Siti Suraya Binti Mohamad

A thesis presented in partial fulfilment of the requirements for the degree of Doctor of Philosophy

2026

Declaration of Authenticity and Author's Rights

This thesis is the result of the authors' original research, except where otherwise acknowledged. It has been composed by the author and submitted to the University of Strathclyde for the degree of Doctor of Philosophy. This thesis has not been previously submitted for the award/higher degree to any other university or institution.

Signed:  Date: 09/02/2026

Dedication

This thesis is dedicated to my parents and my children

&

To the experiences we never expected,

And the paths that were redirected,

To the friends and family, we found along the way.

Acknowledgement

In the name of Allah the most gracious and the most merciful

I wish to express my deepest gratitude to my supervisor, Dr. Karen Renaud, for her invaluable guidance, expertise, and unwavering support throughout this research endeavour. Her steadfast belief in my abilities sustained me through the most challenging phases of this work.

My profound thanks go to my parents, Mok and Abah, whose lifelong support and encouragement have been the foundation of my achievements. To my children, Iman and Ivaa, I thank Allah every day for the privilege of having you by my side, you are my greatest inspiration. My siblings, Kakak, Ya, and Amel, thank you for always standing beside me.

I am deeply grateful to MARA for the financial support provided through the Graduate Excellence Program (GrEP). This funding was instrumental in enabling the successful completion of this research. I extend my appreciation to my CISO, Chelsea Siew, I witnessed firsthand how a great leader empowers their team.

To my family and friends, both near and far, your love, patience, and encouragement have meant more than words can express. Maa, Wea, Salwani, Kak Hani, Dr. Hawa, Dr. Malihah, thank you for your unwavering support through all the ups and downs.

Finally, I thank my fellow researchers at the University of Strathclyde's Computer and Information Science Department and the StrathCyber community. Your intellectual camaraderie, collaborative spirit, and moral support have made this academic journey both enlightening and rewarding.

Thank you all for being a part of this remarkable chapter in my life.

Zaini Ahmad, thank you for the memories.

Abstract

The pervasive and escalating threat landscape in cyberspace has underscored the critical role of human factors as the most significant vulnerability in cybersecurity defences. While technical solutions advance, a persistent gap between cybersecurity knowledge and protective behaviours remains a central challenge, particularly among digitally native but often overconfident youngsters. This research addresses a critical lacuna in the literature by moving beyond a generalised view of cybersecurity awareness to investigate how specific domains of knowledge and behavioural components interact to influence the cyber hygiene of young adults in Malaysia, a nation with one of the highest cybercrime rates in Southeast Asia.

A sequential, multimethod design was employed. First, a large-scale survey (N=765) assessed five distinct domains of cybersecurity knowledge: password, software/system, human, organisational, and social security; and their relationship with behavioural determinants framed by the Theory of Planned Behaviour (TPB): attitudes, subjective norms, and perceived behavioural control. This quantitative phase was followed by a controlled phishing simulation experiment, where a stratified random sample of survey participants was targeted by one of three ethically-designed phishing emails. This innovative design allowed for a critical comparison between participants' perceived security intentions (measured in the survey) and their actual behavioural responses (observed in the simulation).

The findings reveal a critical paradox. While survey results indicated a moderately positive self-assessment of cybersecurity knowledge and strong behavioural intentions, the phishing simulation demonstrated a significant vulnerability, with a substantial portion of participants succumbing to the attacks. Quantitative analysis identified that knowledge domains related to human security (e.g., recognising suspicious emails and websites) and organisational security were the most significant predictors of secure behavioural intentions. However, the

experimental phase crucially demonstrated that these intentions did not reliably translate into behaviour. Furthermore, demographic analysis revealed that educational level, rather than age or gender, was the most significant moderator, with higher education correlating with both greater knowledge and, paradoxically, in some cases, a higher susceptibility to certain types of phishing attempts in real-world contexts, suggesting potential overconfidence among more educated individuals. It is important to note that the phishing simulations used in this study were designed to be recognisable to vigilant users; the finding regarding education and susceptibility is discussed as a potential trend requiring further investigation rather than a definitive conclusion based solely on the simulation results.

The thesis makes three primary contributions. First, it provides empirical evidence for a domain-specific understanding of cybersecurity knowledge, moving the field beyond monolithic constructs. Second, it critically demonstrates the stark discrepancy between perceived and actual cybersecurity behaviour within a youngster cohort, challenging the efficacy of awareness measures that rely solely on self-reporting. Third, it validates the application of the TPB in a cybersecurity context while highlighting its limitations in predicting actual behaviour without observational data. The study concludes that effective cybersecurity interventions for youngsters must not only disseminate knowledge but also actively address the behavioural biases and overconfidence that contribute to the knowledge-behaviour gap, recommending a shift towards experiential, simulation-based training integrated into educational curricula. This research offers a robust methodological framework and substantive findings for policymakers, educators, and security professionals aiming to build a more resilient digital society.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

2FA	Two-Factor Authentication
AOL	America On-Line
ARPANET	Advanced Research Projects Agency Network
AVG	Anti-Virus Guard
C.I. A	Confidentiality. Integrity. Accessibility
CDOC	Cyber Defence Operation Centre
CISA	Cybersecurity And Infrastructure Security Agency
CISO	Chief Information Security Officer
CNII	Critical National Infrastructure
CyberSAFE	Cyber Security Awareness for Everyone
DFTZ	Digital Free Trade Zone
EFA	Exploratory Factor Analysis
GITN	Government Integrated Telecommunications Network
ICT	Information And Communication Technology
ISO	International Organisation for Standardisation
LLM	Large Language Models
MASSA	Mobile Assessment Security Scanning Application
MCMC	Malaysian Communications and Multimedia Commission
ML	Machine Learning
NASCA	National Cyber Security Agency
NC4	National Cyber Coordination and Command Centre
NCCMP	National Cyber Crisis Management Plan
NCCMP	National Cyber Crisis Management Plan
NCII	National Critical Information Infrastructure
NCSP	National Cyber Security Policy
NFCP	National Fiberisation and Connectivity Plan
NSC	National Security Council
SOC	Security Operation Centres
TPB	Theory Of Planned Behaviour
TRA	Theory Of Reasoned Action
TTS	Text-To-Speech

CHAPTER 1 INTRODUCTION

The genesis of the contemporary internet lies in the late 1960s with the U.S. Department of Defence's development of ARPANET, a network designed to interconnect research institutions and facilitate resource sharing (Advanced Research Projects Agency Network) (Tronco, 2010). As the foundational architecture of the modern internet, ARPANET's expansion introduced transformative digital infrastructures and protocols. This evolution has precipitated a profound societal transformation, enabling unprecedented global connectivity and novel domains like e-commerce and social networking. Consequently, while the internet has fundamentally reconfigured modern life, it has also concomitantly produced a critical and expanding frontier of cybersecurity challenges.

The foundational technologies that enable global connectivity and digital convenience inherently introduce systemic vulnerabilities, giving rise to a spectrum of cyber threats. The ontology of these threats can be traced to the late 1960s, with early instances such as the illicit use of computers for telecommunications fraud presaging future risks, perhaps. While initially characterised in the 1980s and 1990s as acts of minor dissent or mischief, the evolution of cyber-attacks has mirrored the internet's integration into critical societal functions. Today, they constitute deliberate and malicious operations designed to compromise digital assets, steal sensitive information, and disrupt essential services.

The contemporary threat landscape is distinguished by its severe and multifaceted consequences. Cyber-attacks precipitate substantial economic damage, as illustrated by logistics disruptions incurring costs of millions (Weaver et al., 2022), and pose direct threats to national security, with the SolarWinds and WannaCry incidents for instance (Kushner, 2013; Walker, 2018; Wolff et al., 2021). Furthermore, they engender a critical erosion of privacy through large-scale data breaches, such as the Equiax leak impacting 800 million individuals

(Novak & Vilceanu, 2019), and are weaponised to manipulate public discourse and jeopardise political stability (Neyazi, 2020; Santini, 2021; Schafer, 2020). These objectives are typically realised through the exploitation of technical vulnerabilities or via social engineering, a persistent threat vector demonstrated by recent successful attacks on major corporations like MGM Resorts, Fujifilm, and Canva (Fujifilm, 2021; Jackson, 2023; Welsh, 2020), underscoring the enduring challenge of securing complex digital infrastructures.

This research is situated within the distinctive socio-technological context of Malaysia, a nation that has undergone rapid digital transformation. This evolution into a diversified, export-oriented economy, supported by significant investment in information and communication technology (ICT) infrastructure (Felker, 2025), has concurrently amplified the national cybersecurity risk profile. Globally, Malaysia confronts a severe threat landscape, ranking as the eighth most breached country worldwide (Azmin & Serota, 2024) and leading Southeast Asia in malware exposure. This elevated ranking can be attributed to several factors: a significant cybersecurity talent gap, with only 15,248 active professionals against a required 27,000, outdated or unpatched devices that attackers exploit (Leskin, 2025), with Malaysia ranks first in Asia for data breaches, with 98% of phone numbers and 89% of names exposed, enabling sophisticated impersonation scams (Fam, 2025). While youngsters constitute approximately 46% of the total population (Mahidin, 2021) and represent the largest proportion of internet users in the country (see Figure *2*, pg. 7). At the national level, cybercrime now constitutes approximately 70% of all crimes reported to the Royal Malaysia Police (Ariffin & Letchumanan, 2020), with phishing established as the most prevalent fraud vector and a cause of substantial financial losses.

In response, Malaysia has enacted a robust institutional cybersecurity framework encompassing policies, a national strategy, and initiatives designed to protect critical infrastructure (Malaysian National Security Council, 2020). Despite this strategic focus, a

critical gap persists: the national approach predominantly emphasises institutional and infrastructural security, thereby neglecting the human element; specifically, the cybersecurity vulnerabilities of the public. This oversight is particularly acute, given Malaysia's substantial demographic of young adults aged 18-26 years-olds, conceptualised here as "youngsters". This digitally-native cohort exhibits high online engagement yet demonstrates a pronounced disconnect between their stated cybersecurity knowledge and intentions, and their actual protective behaviours a phenomenon termed the "knowledge and intention-behaviour gap". Consequently, this research investigates this specific gap as it manifests in Malaysian youngsters, a public-facing vulnerability that seemingly remains unaddressed within the current national cybersecurity efforts.

Prevailing awareness campaigns often operate in a superficial manner, failing to cultivate a foundational cyber knowledge domain, or a structured understanding of core threats, principles, and consequences which builds the essential cognitive foundation upon which genuine protective intention can be formulated and, subsequently, upon which consistent secure behaviour can be built. Without progressing individuals from a state of being passively unaware to actively formulating an intention and acting, interventions will not bridge the knowledge-intention-behaviour gap.

Therefore, this research argues that addressing the human element in a national cybersecurity strategy requires moving beyond the isolated measurement of knowledge (know-how). While establishing a baseline of youngsters understanding of key cyber-security domains is necessary, the true foundation for effective intervention necessitates an investigation into knowledge and psychological drivers behind the resistance to deception gap between what they know and how they act in threat scenarios. This study focuses explicitly on closing this knowledge-behaviour gap. It takes phishing as a central case, as resisting such attempts depends not merely on factual knowledge but also on the youngster’s capacity to detect

deceptive cues, dark patterns and apply understanding under pressure (Mathur et al., 2019; Oh et al., 2025). Accordingly, the selected knowledge domains are designed to measure comprehension of principles that directly aid in identifying phishing tactics, for instance recognising suspicious URLs, understanding authentication mechanisms, and assessing communication legitimacy. By targeting these root cognitive and behavioural factors of vulnerability, the research aims to shift from outdated awareness metrics towards strategies that address the specific behavioural risks within the Malaysian youngsters demographic.

Five cybersecurity knowledge domains: password security, software and system security, human security, organisational security, and social security; were selected to align methodically to address the knowledge-behaviour gap among Malaysian youngsters aged 18–26. The selection of that age group represents an age group that transitionally entering higher education, starting careers, or joining the workforce (Rehman & Manickam, 2023). The research included organisational security as part of the domain, where we have seen studies which capture the increase of apprenticeship career paths which are critical as youngsters increasingly engage with professional environments (Fabian et al., 2023; Smith et al., 2020). This domain allows the research to assess whether an organisational security domain initiatively allows research to effectively assess individual improved cybersecurity practices, thereby bridging the gap between institutional efforts and personal behaviour. Furthermore, social security was included as it acknowledges the role of internet access such as social media and peer interactions in shaping cybersecurity behaviours, a key aspect for the most digitally active users (Al-Hodiany, 2023).

Thesis statement is: *Knowledge on its own is insufficient to improve phish detection and thereby prevent Malaysian youngsters from falling victim to attacks.*

1.1. Research Motivation

The motivation for this research is rooted in the author's professional experience in the cybersecurity industry. Prior to undertaking this PhD, the author spent seven years working in cybersecurity roles, including experience analysing phishing campaigns deployed within large organisations. This industry exposure revealed a critical gap: while technical defences were advanced, employees, digitally native staff, remained vulnerable to phishing attacks despite having received cybersecurity awareness training. This observation raised a fundamental question: why does knowledge not translate into behaviour? This question became the raison d'être of this thesis: to move beyond measuring awareness to understanding the psychological and behavioural mechanisms underlying the knowledge-behaviour gap, specifically among Malaysian youngsters.

The strategic focus on youngsters is dictated by Malaysia’s unique demographic divergence. Unlike nations such as the United Kingdom and the United States of America with aging populations, Malaysia has significant youngster-dominant population structure (see Figure 1 pg. 6).

This digitally active cohort represents both the future of the nation's digital economy and a primary target for cybercriminals. Consequently, the youngster bulge expands the national attack surface, making Malaysia more vulnerable to phishing, social engineering, and malware attacks that disproportionately target younger, digitally active youngsters. This group exhibits extensive use of social media, online gaming, e-commerce, and mobile applications, yet lacks commensurate cybersecurity awareness or safe digital practices. Existing research on this group in the Malaysian context is limited, particularly with respect to studies that dissect cybersecurity into specific knowledge domains and link the knowledge to actual behaviour.

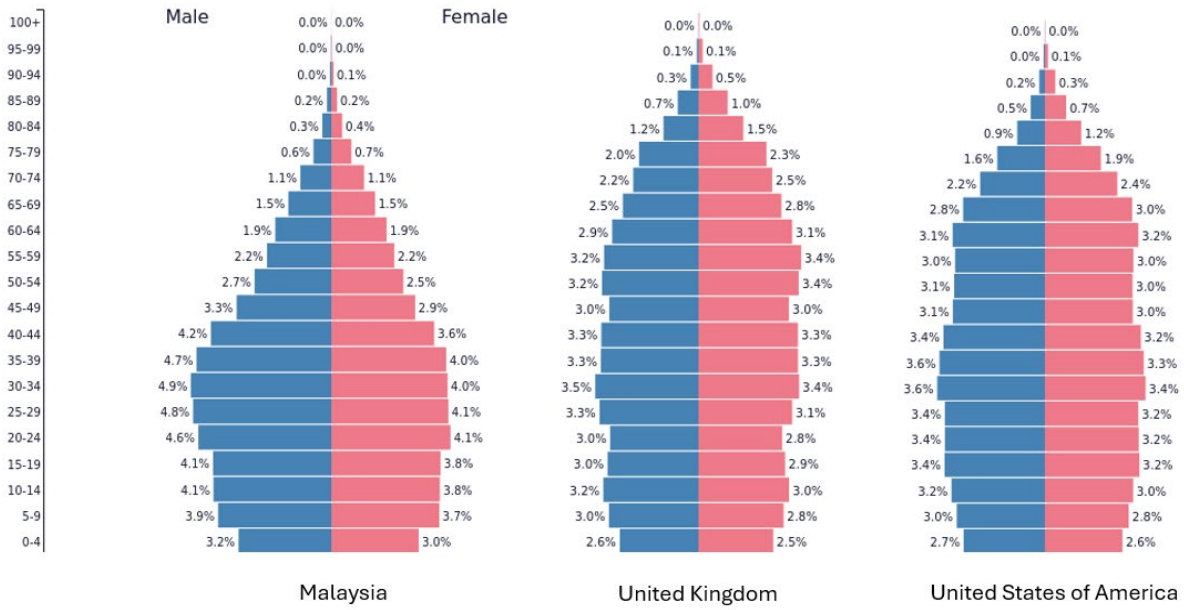


Figure 1 Comparison of population in Malaysia, United Kingdom and United States of America (PopulationPyramid.net, 2025)

Empirically, the behavioural patterns of this demographic reveal an operational dependence on always-on digital connectivity for quotidian routines (Tila, 2020), from mobility (e-payment for transportation) and sustenance (food procurement via apps) to educational access, professional development, and the maintenance of socio-cultural identity through social media platforms. Youngsters between ages 18–26 were selected for this research, as this demographic segment represents the largest proportion of internet users in Malaysia, constituting nearly half of the total user base, according to 2020 national statistics (see Figure 2 pg. 7).

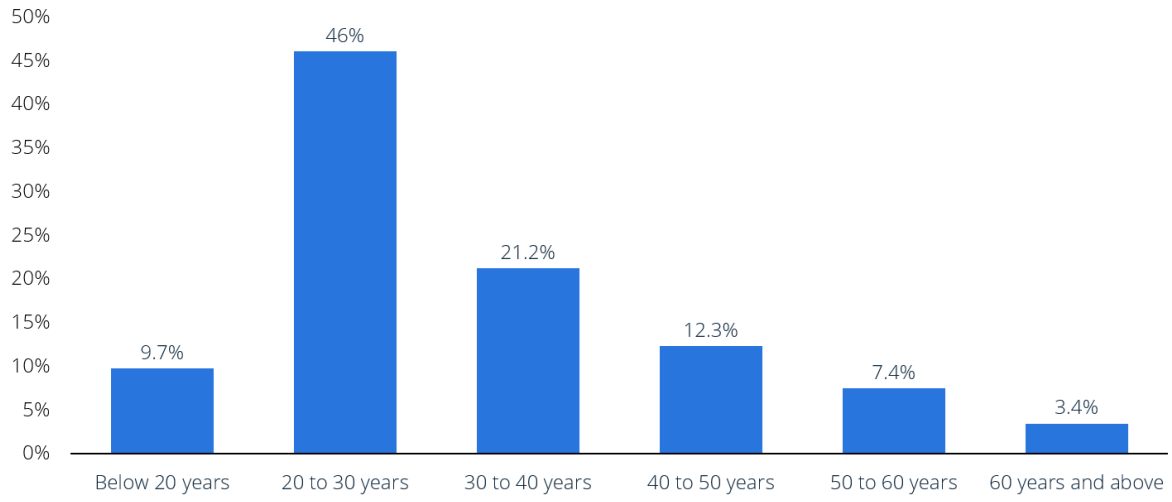


Figure 2 Age group distribution of internet users in Malaysia in 2020 (Tila, 2020)

As illustrated in Figure 3, cybersecurity awareness forms the foundational layer of the cybersecurity learning continuum, where youngsters are competently identified and mitigate threats such as phishing. This model progresses from raising basic awareness among the public environment, to delivering practical training for IT and organisational personnel, and culminates in formal education for specialists with deep expertise, such as cybersecurity practitioners (Gardner, 2014). In general, it focuses on making people understand cybersecurity risks, and how their actions directly contribute towards secure cyber practices.

Figure 3 Cybersecurity learning Continuum

Current efforts to build cybersecurity awareness, however, are often ineffective in reaching the general public, and particularly youngsters. Whether the extent to which cyber hygiene practices effectively protect the organisation (Uberti, 2020), lack of cyber preparation (Bareja, 2021) insufficient depth of the talent pipeline (Barela et al., 2019) or obsolete strategic resources (Nagyfejeo & von Solms, 2020). These fundamental limitations are complicated by the core challenge of measurement, which must be gained from a basic and actionable understanding of cybersecurity. Participating in cybersecurity awareness training is insufficient, as effective self-defence requires a foundational knowledge of what to protect in cyberspace and how to protect it (Ariffin & Letchumanan, 2020). Youngsters must, therefore, move beyond superficial awareness to develop a stable knowledge base that actively informs their own defensive behaviours thereby bridging the gap between intention and actual protective behaviour. This directly applicable knowledge is essential for taking preventative measures to safeguard themselves against incidents, rather than solely focusing on risks posed to others.

1.2. Research Questions

The primary objective of the survey is to address research questions as below:

- **RQ1**: How do different cybersecurity knowledge domains (password, software/system, human, organisational, and social security) predict Malaysian Youngsters' self-reported cybersecurity behavioural intentions?
- **RQ2**: To what extent do the Theory of Planned Behaviour constructs (Attitude, Surrounding Pressure, and Perceived Control) mediate the relationship between cybersecurity knowledge domains and behavioural intentions among Malaysian youngsters?
- **RQ3**: How do demographic factors (gender, age, education level) and cybersecurity knowledge domains influence actual cybersecurity behaviour, as measured by susceptibility to phishing simulations?
- **RQ4:** What discrepancies exist between Malaysian youngsters' self-reported cybersecurity intentions and their actual behaviour when faced with a simulated phishing attack?

1.3. Aim and Objective

This research aims to address these gaps through a two-phase empirical study investigating the cybersecurity practices of Malaysian youngsters. The overarching objective is to determine how cybersecurity knowledge and behavioural factors predict resilience to cyber-attacks, and how these relationships are moderated by demographics.

- **Phase 1:** A quantitative survey will be administered to a large sample to measure cybersecurity knowledge, behavioural intentions, self-reported practices, and demographic variables and directly address research questions 1 and 2.
- **Phase 2:** Building on the Phase 1 analysis, and to directly address research questions 3 and 4, a subset of volunteering participants will be targeted by a simulated phishing attack. This phase provides an objective behavioural measure to complement and validate the self-reported data from the survey.
  The integrated findings from both phases will provide a comprehensive model of the factors influencing the cybersecurity practices of the study population.

1.4. Research Hypotheses

To provide clarity for the reader, Table 1 below maps each research question to the corresponding hypotheses tested in this study

Table 1 Mapping research question to hypotheses

Research Question	Corresponding Hypotheses
RQ1: How do different cybersecurity knowledge domains predict self-reported behavioural intentions?	H6a-H6e, H7a-H7e, H8a-H8e (knowledge domains → Attitude, Subjective Norms, Perceived Control)
RQ2: To what extent do TPB constructs mediate the relationship between knowledge domains and behavioural intentions?	H1, H2, H3 (Attitude, Subjective Norms, Perceived Control → Intention)
RQ3: How do demographic factors and knowledge domains influence actual behaviour (phishing susceptibility)?	H4, H5, H9 (Perceived Control → Behaviour; Intention → Behaviour; Demographics → Behaviour)
RQ4: What discrepancies exist between self-reported intentions and actual behaviour?	H5 (Intention → Behaviour) – tested via comparison of survey and simulation results

Table 1 above shows the diagram of Research Question mapping onto Hypotheses. RQ1 is addressed by H6-H8 (examining the influence of the five knowledge domains on the three TPB constructs). RQ2 is addressed by H1-H3 (examining the influence of TPB constructs on intention). RQ3 is addressed by H4, H5, and H9 (examining direct paths to behaviour and demographic moderation). RQ4 is addressed by H5, interpreted through the comparison of survey intentions (Phase 1) with actual simulation behaviour (Phase 2). Hypothesis diagram in Figure 4, page 11.

1.4.1. Intention

Attitude is a key driver of behavioural intention. The investigation of this specific relationship to RQ2.

H_1: Youngsters who hold a more positive attitude toward cybersecurity practices will demonstrate stronger intention to engage in secure online behaviour.

Social norms often act more indirectly in digital-behaviour studies.

H_2: Higher perceived social pressure from family, peers, educators, and surrounding influences will positively influence youngsters' intention to adopt safe cybersecurity behaviours.

Confidence to update systems, avoid suspicious links, and adjust behaviour, strongly predicts intention, aligning with TPB.

H_3: Youngsters with stronger perceived control (confidence in performing secure behaviour) will show stronger intention to engage in cybersecurity-safe practices.

This reflects TPB's pathway where perceived control may influence behaviour directly.

H_4: Youngsters who perceive higher levels of behavioural control are more likely to demonstrate safer observable cybersecurity behaviour.

1.4.2. Behaviour

Behaviour was used as one of the components that came from the Theory of Planned Behaviour (TPB) model and complement RQ4.

H_5: Stronger cybersecurity intentions will lead to safer actual cybersecurity behaviours.

1.4.3. Cyber Knowledge Domain

These hypotheses examine how the collective cyber knowledge domain in RQ1 (password security, software & system security, human security, organisational security, social security) influences the three constructs in the TPB model.

H_6: Cyber Knowledge Domains → Youngsters' Attitude

H_{6a}: Password Security has a significant positive influence on Youngsters' Attitude toward cybersecurity.

H_{6b}: Software & System Security has a significant positive influence on Attitude.

H_{6c}: Human Security has a significant positive influence on Attitude.

H_{6d}: Organisational Security has a significant positive influence on Attitude.

H_{6e}: Social Security has a significant positive influence on Attitude.

H_7: Cyber Knowledge Domains → Youngsters' Social Pressure (Subjective Norms)

H_{7a}: Password Security has a significant positive influence on Social Pressure.

H_{7b}: Software & System Security has a significant positive influence on Social Pressure.

H_{7c}: Human Security has a significant positive influence on Social Pressure.

H_{7d}: Organisational Security has a significant positive influence on Social Pressure.

H_{7e}: Social Security has a significant positive influence on Social Pressure.

H_8: Cyber Knowledge Domains → Youngsters' Perceived Behavioural Control

H_{8a}: Password Security has a significant positive influence Perceived Control.

H_{8b}: Software & System Security has a significant positive influence on Perceived Control.

H_{8c}: Human Security has a significant positive influence on Perceived Control.

H_{8d}: Organisational Security has a significant positive influence on Perceived Control.

H_{8e}: Social Security has a significant positive influence on Perceived Control.

1.4.4. Demographic Characteristics

This assumption forms the basis for the analysis within RQ3. As age and education rise, and among females, risky behaviour decreases. Thus, demographics meaningfully moderate cybersecurity behaviour.

H_9: Higher demographic will reduce risky cybersecurity behaviour

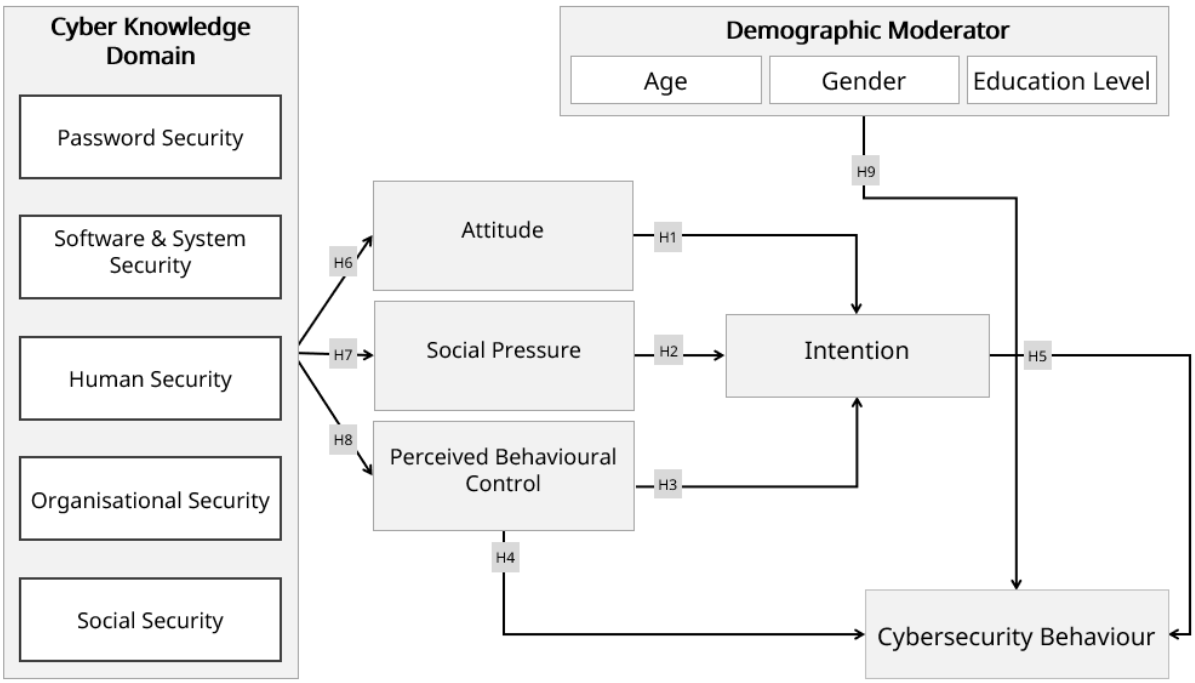


Figure 4: Research Hypothesis for Studies into Youngsters' Cybersecurity Knowledge, Intention and Active Behaviours

Figure 4 above illustrates the hypothesised relationships in this study. The five cybersecurity knowledge domains (Password Security, Software/System Security, Human Security, Organisation Security, and Social Security) were derived from a synthesis of the literature in Sections 2.6.1(I)-2.6.1(V) and represent distinct areas of cybersecurity competency. The three 'control' constructs refer to the Theory of Planned Behaviour (TPB) components: Attitude, Subjective Norms (labelled 'Surrounding Pressure'), and Perceived Behavioural Control. These TPB constructs mediate the relationship between knowledge domains and behavioural intentions. The model also includes direct paths from Perceived Control to Behaviour and from Intention to Behaviour, as well as demographic moderation.

1.5. Research Contribution and Significance of the study

This research makes three distinct and significant contributions to the field of cybersecurity:

- **Theoretical Contribution**: The study provides a novel theoretical advancement by deconstructing the monolithic concept of cybersecurity awareness into five specific, measurable knowledge domains. It then empirically establishes the differential influence of these domains on the behavioural components of the Theory of Planned Behaviour (TPB), thereby offering a more nuanced understanding of the psychological mechanisms that underpin the knowledge-behaviour gap.
- **Methodological Contribution**: Methodologically, this research introduces and validates a robust sequential multi-method design, integrating a large-scale survey with a controlled phishing simulation. This approach directly addresses a critical validity gap in the literature by triangulating self-reported intentions with observed behavioural data, yielding a more authentic and reliable analysis of cybersecurity practices

- **Practical and Policy Contribution**: The findings deliver actionable, evidence-based insights for key cyber stakeholders in Malaysia. For policymakers and educators, the results provide a clear framework for moving beyond generic awareness campaigns towards developing targeted interventions that address specific behavioural triggers and knowledge deficiencies identified in the youngster demographic, thereby enhancing the efficacy of national cybersecurity initiatives.

1.6. Thesis Chapters

Introduction in chapter 1, establishes the foundation by presenting the background of cybersecurity, highlighting the critical role of the human factor, the significance of the study and stated the research questions, along with the research hypothesis the study and explains the thesis structure.

Chapter 2, the Literature Review, establishes the human element as the principal vulnerability within cybersecurity, foregrounding its analysis on pervasive threats such as phishing and social engineering. It systematically operationalises cybersecurity competency by delineating five critical knowledge domains. Employing the Theory of Planned Behaviour as its theoretical framework. Contextualising this within Malaysia, it synthesis culminates in the identification of a critical and persistent knowledge-intention-behaviour gap among Malaysian youngsters, thereby defining the core problem this research investigates.

Chapter 3 details the pragmatic, multi-method approach that was adopted, meticulously describing the two sequential phases: a large-scale survey that measured knowledge and behavioural intentions, followed by a controlled phishing simulation experiment that observed actual behaviour, with thorough explanations of sampling strategies, instrument development, data collection procedures, and ethical considerations.

The presentation and analysis of the empirical findings are reported in Chapter 4, Data Analysis and Results, which covers data preparation, descriptive statistics of the demographics and key constructs, tests for validity and reliability, and the results of both the survey analysis and the phishing simulation, including hypothesis testing.

Chapter 5 interprets these results by critically analysing them in relation to the research questions, exploring the paradox between high self-reported knowledge and actual phishing susceptibility, and linking the findings back to the research literature in Chapter 2 and Chapter

3 which culminated in practical recommendations for education, policy, and awareness initiatives.

Finally, Chapter 6 synthesises the entire study by summarizing the key findings, explicitly outlining the original contributions to knowledge, acknowledging the research's limitations, and proposing concrete avenues for future work, followed by a personal reflection on the academic journey undertaken to complete the thesis. The structure of this thesis is in Figure 5.

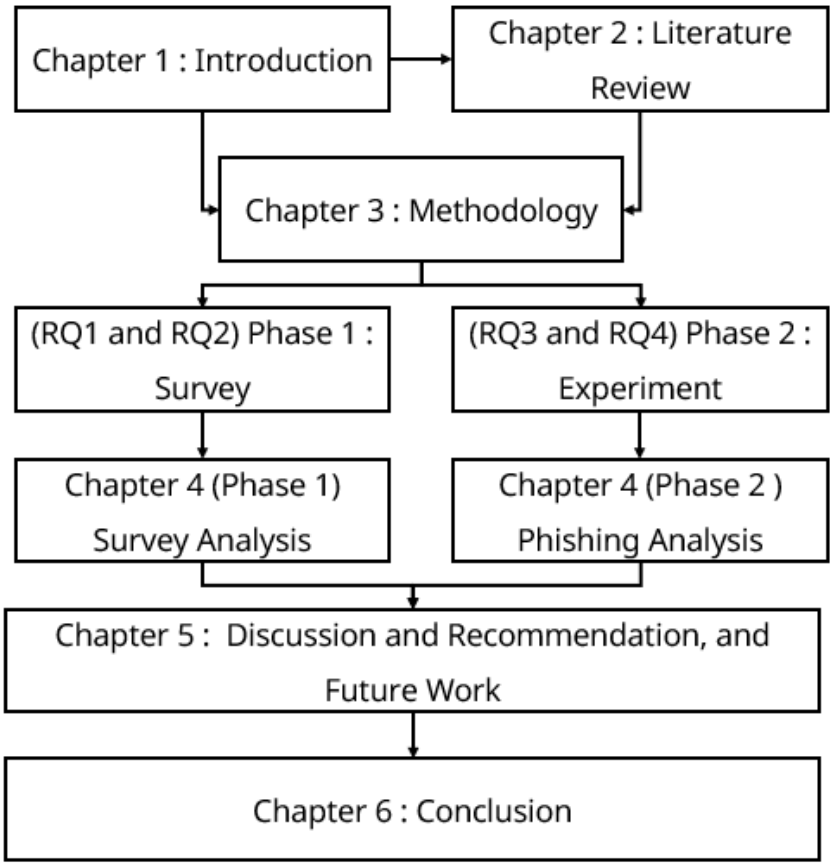


Figure 5: PhD Dissertation Structure

CHAPTER 2 LITERATURE REVIEW

2.1. Introduction

This chapter presents a comprehensive review of the literature concerning the relationship between cybersecurity knowledge and behaviour among Malaysian youngsters. The review is structured to build a foundational understanding before narrowing the focus to the specific context of Malaysia and the behavioural theories relevant to this study.

The chapter begins with Section 2.2, which scopes the field of cybersecurity to establish a consistent definition for this research and explores the critical role of human factors as a primary vulnerability. Section 2.3 builds on this by examining the human element, shifting the perspective from the "weakest link" to the primary attack surface. Building on the foundation in Section 2.3, Section 2.4 analyses the types of attacks targeting users, detailing essential countermeasures, while Section 2.5 explores the social engineering arsenal, categorising attacks by medium of delivery, deception techniques, and intended goals.

Section 2.6 investigates the prevention of phishing success through various knowledge domains, including password, software, human, organisational, and social security. This section also introduces the Theory of Planned Behaviour (TPB) as the framework for understanding user's behaviour. Finally, Section 2.7 then synthesises these discussions within the Malaysian context, outlining the nation's cybersecurity challenges, key legislative measures, and public-private collaboration initiatives. Collectively, these sections highlight the critical youngsters' cybersecurity knowledge–behaviour gap, establishing the core problem this research addresses.

By integrating insights from global cybersecurity research with specific findings from Malaysia, this chapter identifies the persistent disconnect between what youngsters know and how they act online. It concludes by validating the necessity of this research and lays the

groundwork for developing a targeted framework to bridge this knowledge-behaviour gap among Malaysian youngsters.

The term 'youngster' was deliberately chosen for this study to move beyond a rigid, classical definition of youth. Drawing from Lakoff (1987) is prototype theory, which posits that categories often have radial structures with central and extended members, we conceptualise 'youngster' as a fluid category representing the journey into adulthood. Consequently, the term serves as a placeholder for a demographic character marked by a specific life-stage transition and broad individual differences, rather than being limited to a fixed age bracket.

2.2. Scoping Cyber Security: From Technical Walls to the Human Firewall

The International Telecommunication Union (ITU) defined comprehensive definition of cybersecurity referred to ITU-T X.1205 as:

> *"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organisation and user's assets. Organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organisation and user's assets against relevant security risks in the cyber environment. The general security objectives comprise availability integrity, which may include authenticity and non-repudiation confidentiality",* (International Telecommunication Union, 2008).

A consistent definition of cybersecurity has been in debate be it in the academic (Cains et al., 2022; Schatz, Bashroush, & Wall, 2017; Wang, Sun, & Zhu, 2020), government and private sectors (CISA, 2014; International Telecommunication Union, 2008; Luiijf, Besseling, & de Graaf, 2013) or even considered from non-expert perspectives (Neil et al., 2023). However, they remain inconsistent. This research is concerned that the inconsistencies might

come from heterogeneity of countries' regulations, acts and their cyber security initiatives. Maurer & Morgus (2014) compiled cybersecurity definitions covering a wide range of ideas from different countries and government bodies and concluded that while various sources present surface-level differences in how they describe the field, the fundamental definition of cybersecurity remains consistent across most contexts. These definitions converge on the protection of assets within cyberspace against unauthorised access and attacks, primarily to maintain the CIA triad (confidentiality, integrity, and availability).

This research identifies six core contexts of cybersecurity, derived from an analysis of definitions provided by the Oxford English Dictionary, national agencies, and prominent scholars. (Balzacq & Cavelty, 2016; Bullock, Haddow, & Coppola, 2018; CISA, 2014; International Telecommunication Union, 2008; Muller, 2024; Oxford English Dictionary, 2025):

1. **Measures**: Implementation of strategies, policies and tools to ensure safeguarding of cyberspace. The measure can also be in the aspect of technical controls or a non-technical control.
2. **Protection**: Guarding the assets (Infrastructure, data and application or the people) against destructions, disruption, unauthorised access.
3. **Cyberspace**: Internet and interconnected with the digital environments. Where cyber activities occur.
4. **Attack**: Objects that shape cyberspace environment such as malware (Balzacq & Cavelty, 2016), attempts to breach the security in IT/OT.
5. **Unauthorised access**: Access to the system data by individuals who do not have permission to access and breach the confidentiality.
6. **CIA triad**: Confidentiality, integrity, and availability, a foundation in cybersecurity.

It is crucial to distinguish cybersecurity, which focuses on securing networks and systems within digital environments, from the broader field of information security, which protects data in both physical and digital forms (Alexei & Alexei, 2023). Historically, cybersecurity strategies emphasised technical measures to secure these digital layers (Devasis et al., 2022). However, the contemporary threat landscape has undergone a significant shift which mandates a shift in strategy.

We have seen a rapid increase in social engineering attacks rather than technical attacks such as malware attacks (Kamarudin et al., 2018), DoS/DDoS attack (Li et al., 2018), SQL injection (Paul, Sharma, & Olukoya, 2024), or cross-site scripting (XSS) attacks (Krombholz et al., 2015). Albeit technical mitigation is taken against cyber threats, prioritising technical strengthening of the system, network, or application architecture alone is insufficient. This deceptive practice such as impersonating, Quid Pro Quo, pretexting, or replication may appear in many forms, but it most often relies on psychological manipulation tactics that take advantage of human trust.

For organisations, for instance, it is widely acknowledged that the advanced technological infrastructure within large organisations, while essential for productivity, offers no absolute defence; the threat of cyber-attacks continues to loom despite these substantial investments. It is crucial to understand the human's perspective in term of cybersecurity to improve employee cyber hygiene practices. In general, the world is witnessing a rapid increase in attacks that bypass technical controls by targeting the user directly.

2.3. The Pivotal Human Factor: From “Weakest Link” to Primary Attack Defender

This shift in focus is not incidental. Robust technical defences, while essential, offer no absolute guarantee (Murtaza, Pak, & Siddiqi, 2022). A common and disconcerting thread runs through modern security breaches: the human factor. Human error, influenced by cognitive factors like stress, workload, and expertise, remains a leading and persistent vulnerability (Joisten et al., 2022; Montañez, Golob, & Xu, 2020; Rahim, Hamid, & Kiah, 2019; Safa et al., 2015). This was a significant cybersecurity threat, particularly evident during the COVID-19 pandemic when remote working and e-learning, surged (Guitton, 2020). Researchers consistently conclude that internet users are a primary threat vector, with human behaviour being a core factor influencing cybersecurity outcomes (Aigbefo, Blount, & Marrone, 2022; Anderson & Agarwal, 2010; Burns & Roberts, 2013; Lahcen et al., 2020; Shah & Agarwal, 2020).

High-profile incidents illustrate this vulnerability. For example, in May 2025, the UK retailer Marks & Spencer disclosed a cyber-attack resulting from 'human error' rather than technical failure. An employee was tricked by a phishing email into revealing credentials, leading to unauthorised access to customer data. The incident cost the company an estimated £300 million (Saker-Clark, 2025). Similarly, NHS Scotland experienced a disruption due to a cyber-attack (ANSecurity, 2025), and major email providers have reported credential theft attacks (Cloud&More, 2025). These examples highlight that the greatest threat is often not sophisticated malware, but the exploitation of human psychology through social engineering. Social engineering, is the root cause of many modern breaches (Saulsbery, 2021). It is defined as:

> *“Social engineering is the process of someone or something (e.g., email, malware, programme) fraudulently and maliciously masquerading as someone or something else*

to acquire unauthorised information or to create a desired action that is contrary to the victims or their organisation's self-interests. Simply put, it's a "con" with malicious intent. It is often done in person, using mailed advertisements, using email, in messaging apps, or over the phone". (Roger, 2021, p. 259).

Whilst social engineering is not novel as it was first introduced in the early 1970 (Pound, 1969), it capitalised on gaps in knowledge and exploited psychological tendencies such as trust, urgency, offering rewards, invoking identity threats, ensuring contextual fit, and curiosity, mainly to alter decision-making and prompting specific actions (Chapagain et al., 2024; Gallegos-Segovia et al., 2017; Longtchi & Xu, 2025). This vulnerability has been noted for decades (Kraemer, Carayon, & Clem, 2009; Schultz, 2005; Tam, Glassman, & Vandenwauver, 2010) and remains critically relevant today (Corradini & Nardelli, 2020; Inho, 2021; Renaud, van der Schyff, & MacDonald, 2023; Wulandari, Adnan, & Wicaksono, 2022). Human factors represent aspects beyond the predictive capacity of secure technology, making informed "actions, knowledge, and attitude" the most efficacious personal security measure (Reynolds, 2021). Therefore, the paradigm must evolve from viewing the human as the "weakest link" to recognising them as the primary attack surface requiring dedicated defence (Onwuegbuche et al., 2025).

2.4. Attacks Targeting Users

Phishing attacks have become the largest and most rapidly growing cybercrime vector. As common as social engineering is nowadays, people remain vulnerable to these tactics. Receiving emails claiming exciting news or warning of financial trouble, pretending to be a friend, or exploiting tragic events to stir sympathy and encourage donations, and using emotions such as curiosity, fear, and empathy are ways of manipulating to deceive people in phishing scams.

Figure 6 shows both the two main ways phishing attacks are carried out are by convincing a victim to click a malicious link, leading to a fake website, or to open a corrupted attachment, which can deploy harmful software also provision of information. Ultimately, both techniques function by using social engineering to manipulate human decision-making. Phishing stands apart from other social engineering tactics because of the industrialises deception, combining unique adaptability with low-cost, highly scalable operations within the digital environment. Its continuous evolution enables it to grow increasingly complex, challenging both human resilience and traditional security defences (Subbulakshmi et al., 2025).

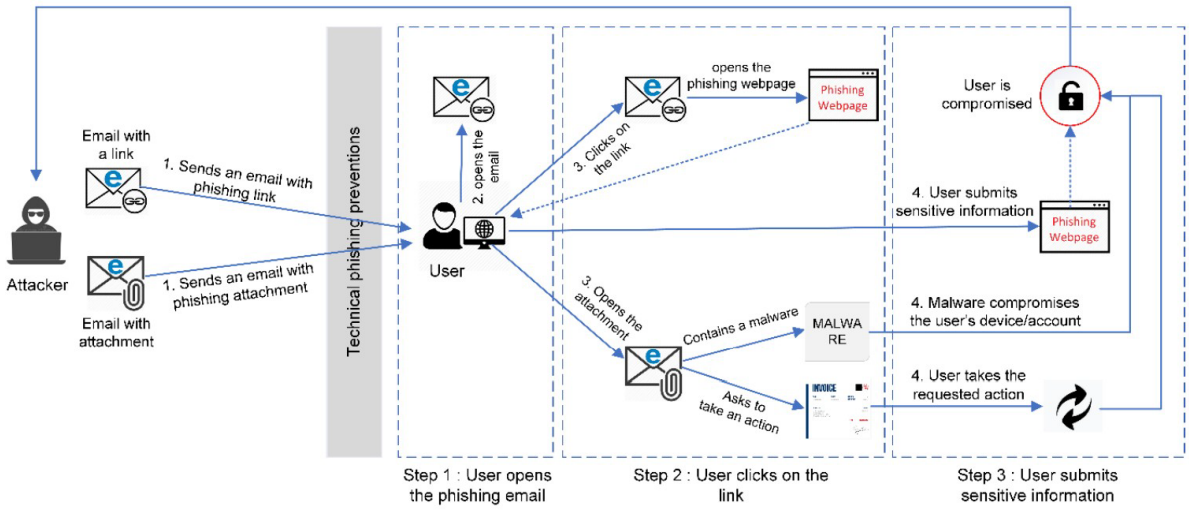


Figure 6 Implementation of Phishing Attacks (Abroshan et al., 2021, p. 44929)

Users' lack of knowledge of their own behavioural vulnerabilities increases potential consequences to phishing attacks, although there are many other factors that contributed to phishing attacks, this research acknowledged the factor of specific domain in cyber knowledge with behaviour as one of the main contribution, which is explained in detail in Section 2.4 and Section 2.5 below (Desolda et al., 2022).

The integration of Artificial Intelligence has fundamentally escalated the phishing threat landscape by acting as a force multiplier that enhances the scale, precision, and evasiveness of attacks across all vectors (Rajeswari & Rajeeth, 2025; Salahdine & Kaabouch, 2019). AI automates the labour-intensive process of reconnaissance and content creation, enabling hyper-personalised spear phishing at scale and generating linguistically flawless emails that erase traditional detection cues like poor grammar (Emanuela, Cristina, & Luminiţa, 2024). Furthermore, it empowers new levels of sophistication through dynamic attacks, such as AI-driven voice cloning for vishing (Blancaflor et al., 2025), interactive chatbots for smishing (Shibli, Pritom, & Gupta, 2024), and algorithmically generated domains and landing pages for quishing (Keerthi et al., 2025). These paradigm shifts have effectively democratised advanced social engineering, lowering the skill barrier for attackers while simultaneously creating a more pervasive and credible threats that challenges both human vigilance and conventional, static security filters

2.4.1. Phishing countermeasures

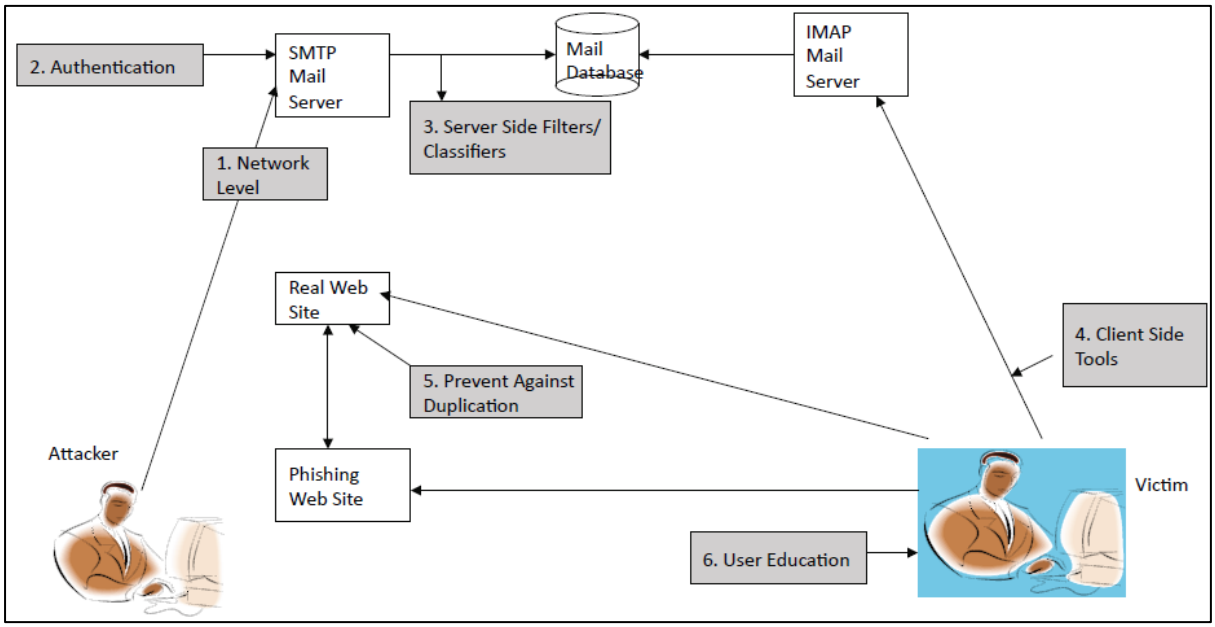


Figure 7: Protection techniques as part of phishing countermeasures (Ramanathan & Wechsler, 2012, p. 3)

Based on Figure 7 by Ramanathan & Wechsler (2012), despite their shared focus on proactive phishing prevention, network and client-side approaches have distinct challenges. Network-based defences remain inherently reactive, as their efficacy relies on constant demand and updates and targets the client-side of the security architecture, though this approach is uniquely dependent on consistent user engagement and the fallibility of human judgment. A holistic security strategy integrates technological solutions with ongoing user awareness programmes which can strengthen defence, ensuring that both automated systems and human behaviour work together to reduce phishing attack success.

An awareness programme is crucial, in that it is the vehicle for disseminating information to all users. Cyber security awareness ensure that individuals comprehend their personal role in securing information and systems (Wilson & Hash, 2003). Based on the NIST Special Publication 800-50, awareness is described as:

> *"...The purpose of awareness presentations is simply to focus attention on security... Awareness relies on reaching broad audiences with attractive packaging techniques..." (Merritt et al., 2024, pp. 8-9)*

Machine learning also is one of a comprehensive set of tools for enhancing online security through, and prevention of, phishing attacks. The application of XGBoost and Random Forest demonstrated over 97% accuracy in distinguishing between legitimate and phishing emails (Divakarla & Chandrasekaran, 2023). In PhishBlock, a system combining Blockchain and Machine Learning, Pitre, Joshi, and Das (2023) proposed a system to counter the rising threat of phishing attacks. Gradient Boost and SVM machine learning algorithms were integrated to improve the system's detection and prevention capabilities, while Blockchain technology was employed to enhance the system's security and reliability (Abadla et al., 2023;

Lakshmi, Skandarsini, & Ida, 2023; Mittapalli, Ojha, & T, 2021; Prasad et al., 2024). AI tools such as Natural Language Processing (NLP) have become a critical tool for boosting phishing detection with successful rate of 90-95% of sophisticated spear-phishing emails detected (Mohamed, Taherdoost, & Khashan, 2025). Other AI tools such as VeriActor, DNN with a Lasso-based feature, Named entity recognition (NER), and Atrous Spatial Pyramid Pooling (ASPP) shows an accuracy of above 80 percent of AI phishing detection (Pan et al., 2025).

Whilst most researchers highlight technical interventions, Nevin, Renaud, and Finney (2022) carried out a study to assess whether presenting participants with cues (encouraging thoughtful consideration) could enhance their skills in recognizing phishing attempts. Although the intervention did not lead to a substantial increase in detection rates overall, further examination indicated a potential positive correlation between the intervention and the better identification of emails that triggered feelings of urgency or stimulated greed and curiosity. Others implemented gamification (Adams & Makramalla, 2015; Baxter, 2016; Jalali, Siegel, & Madnick, 2019; Ortiz, Reinerman-Jones, & Matthews, 2016; Power, 2018; van Steen, 2021) and phishing simulation (Abdullah & Mohd, 2019; Bank, 2005; Chatchalermpun & Daengsi, 2021; Dodge, Carver, & Ferguson, 2007; Gordon et al., 2019; Rizzoni et al., 2022; Sparks, 2022; Sten et al., 2019) with a notable increase in threat detection rates among users.

2.5. The Social Engineering Arsenal

The exploitation of the human factor is operationalised through a diverse arsenal of social engineering attacks. To systematically categorise this threat landscape, this research employs the conceptual framework presented in Figure 8 in page 29, which deconstructs attacks into three core components: the Medium of Delivery, the Deception Technique, and the attacker’s goal.

Historically, the term change from ‘fishing’ to ‘phishing’ originated in 1996 during social engineering attacks targeting America On-Line (AOL) (Ribeiro, Guedes, & Cardoso, 2024) as a means for exploitation of social engineering to carry out crimes and the word phishing is in printed materials in 1997 (Rader & Rahman, 2015). Phishing has since become the most dominant social engineering vector due to its scalability and digital efficiency (Mouton et al., 2014). It stands apart by being highly adaptable, continually growing more complex, and spawning numerous specialised subtypes that populate the framework in Figure 8.

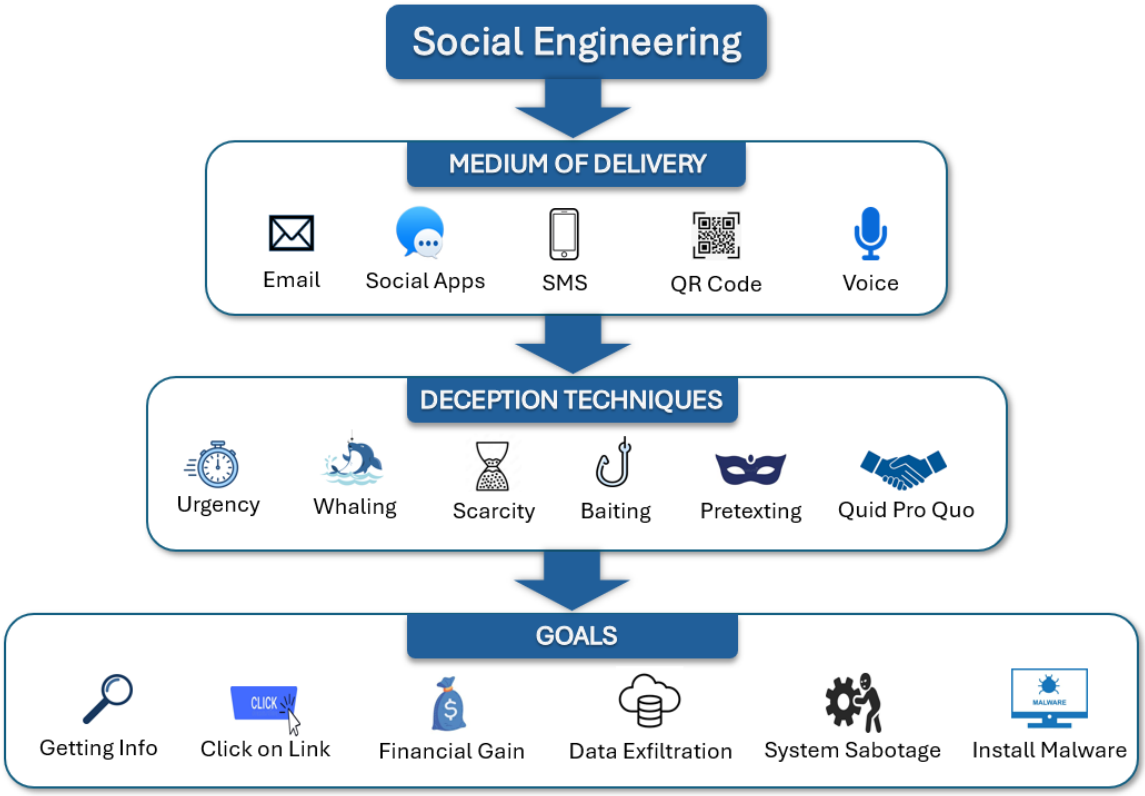


Figure 8. A Conceptual Framework of Social Engineering Attacks

The most dominant vectors for social engineering are the phishing attack (Desolda et al., 2022; Naqvi et al., 2023), *quid pro quo* (Vishal et al., 2025) or many other social engineering attacks. However it can also include tailgating, which is also one of social

engineering attacks which involve a physical social engineering attack vector (Akati & Conrad, 2021; Kamruzzaman et al., 2023).

Social engineering only involves minimal to no technical expertise for the attacker to bypass security measures to gain confidential information. For example, in a spear phishing attack, attackers only need to understand the victim's characteristic, and their behaviours (Albladi & Weir, 2020; Corradini & Nardelli, 2020). Considering that social engineering threats are evolving and diverse (Aldawood & Skinner, 2019), it is essential for the employee to remain vigilant with this threat. To mitigate social engineering, initiatives must necessitate from both the technical aspects and also an extensive understanding of its foundations (Hatfield, 2018) which is argued to be inconsistent due to the fact that it consisted of multiple phases (Z. Wang et al., 2020) and some contended the lack of technical aspect with psychological bias (Murtaza et al., 2022). The contention is that technical defences assume rational, rule-based behaviour, but humans are emotional, inconsistent, and easily manipulated. Until security starts treating psychology as seriously as it treats encryption, the human factor remains the weakest link.

2.5.1. Categorising Social Engineering Attacks by Medium of Delivery, Deception Techniques, and Goal.

2.5.1.1. Medium of Delivery

Email has emerged as a widely used communication tool on the internet, driven by its ability to support various communication features such as document attachments, embedded links, customisable design elements, ease of use, and underlying protocols (e.g., SMTP, IMAP, POP3) that enable reliable message delivery across different systems. The relevance of mentioning these protocols is that they are inherently vulnerable to spoofing and interception, attackers can exploit weaknesses in email protocols to forge sender addresses, bypass authentication, and make phishing emails appear legitimate. Because attackers continuously adapt to current technology, they have become increasingly sophisticated, employing the latest

tactics for the exploitation of victims. These attacks manifest through social engineering: the exploitation of human vulnerabilities by deploying sophisticated deceptive tactics, designed to dupe individuals into surrendering sensitive information, such as login credentials, financial data, or personal details. By diversifying their methods to maximise the success rate of such attacks, attackers utilise email as the primary attack vector for social engineering, accounting for 96% of cases (Tomičić, 2023). The remaining four percent comprise alternative vectors, including SMS (smishing) (Akande et al., 2023), or voice calls (vishing) (Alabdan, 2020), QR code (Mayer, Bekavac, & Strecker, 2024), WhatsApp, Snapchat, Skype and other social apps (Bello et al., 2025).

I. Vishing

Vishing, Vishing, or 'voice phishing', is a form of deception executed through phone calls. The term first appeared in security literature around 2006, as attackers began combining Voice over Internet Protocol (VoIP) technology with social engineering tactics. The word 'vishing' is a portmanteau of 'voice' and 'phishing' (Abu-Nimeh, 2009).Its tactics have evolved from simple fraudulent calls, as historically reported by the American Bankers Association, to now incorporate advanced technical algorithms. These include text-to-speech (TTS) systems, the misuse of generative AI, and large language models (LLMs) to enhance the scale and credibility of attacks, (Marchal et al., 2024; Toapanta et al., 2024; Triantafyllopoulos et al., 2025).

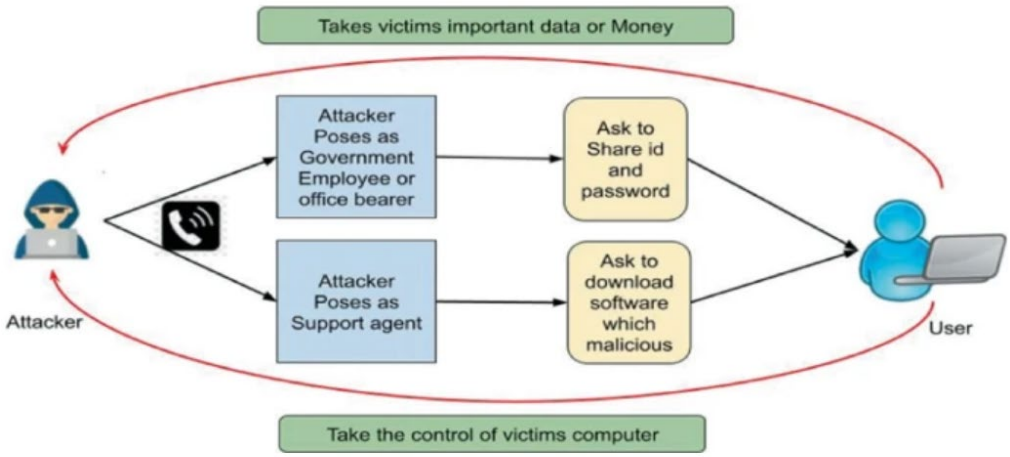


Figure 9: General vishing attack (Ashfaq et al., 2024, p. 413)

Instead of using emails or malicious websites, vishing exploits voice over internet protocol technology to trick individuals by imitated for legitimate scenario into revealing sensitive information (see Figure 9). Jones et al. (2021) implemented real-world vishing attacks and summarised that vishing attack rely heavily on emotional persuasion rather than reasoning. Triantafyllopoulos et al. (2025) said there were gaps in understanding vishing in terms of psychological perspectives. A case study of smishing, vishing and phishing, showed that vishing was the least common, however it proved to be more successful for attackers (Zimba, Mukupa, & Chama, 2024). Large financial funding organisations were also invested to develop next-generation security platforms that can simulate, detect, and respond to vishing attacks in real time using OpenAI (Thompson, 2025).

II. Smishing

Meanwhile smishing, a portmanteau of "SMS" and "phishing," a type of phishing attack conducted via mobile devices, involves sending deceptive text messages that lure users into accessing fake websites, apps, or links. Emerged in the early 2000s as mobile phones became ubiquitous. The first documented smishing attacks appeared in the US in 2003-2004, where

attackers sent text messages impersonating banks or credit card companies, requesting recipients to call a number or visit a website to 'verify' their account information (Abu-Nimeh, 2009). Unlike email phishing, smishing exploits the immediacy and higher open rates of text messages, typically 98% of SMS messages are read within 3 minutes (Shamy, Xie, & Zhong, 2025).

Smishing aims to steal financial details as well as personal information stored on the device (Akande et al., 2023). Smishing can have significant consequences for individuals who rely heavily on their smartphones (Blancaflor et al., 2021) or online applications such as. Smishing started to cause large financial losses in the US in the early 2000s (Abu-Nimeh, 2009). Author Morgan et al. (2023) studied smishing interactions from the users' perspective to understand users' behaviour, experience, and knowledge of smishing. They highlighted significant gaps between knowledge and behaviour when it comes to smishing.

III. Quishing

Quishing, a portmanteau of "QR code" and "phishing," constitutes a less-documented form of cybercrime (Rys, Ślusarek, & Zieliński, 2025). It is a sociotechnical attack wherein perpetrators harvest sensitive information by persuading victims to scan QR codes (Figure 10) that redirect them to fraudulent websites (Awuah & Hayfron-Acquah, 2022). The pandemic served as a catalyst for the propagation of digital payment technologies, with QR code payment systems emerging as a prominent and widely adopted solution (Le, 2022).

Figure 10 Example of QR Code

The vulnerability is exacerbated by the extensive integration of QR codes into trusted environments (ReliaQuest, 2023). The attack surface for quishing is vast because it exploits QR code usage in contexts where users' guards are naturally lowered. This includes educational institutions, where codes provide instant access to quizzes and learning materials (Boise State University, 2025); the hospitality sector, where establishments such as restaurants and bars use them for digital menus and promotional loyalty programmes (CE Noticias Financieras, 2024a); retail environments, where they facilitate promotions and coupon redemption (Okazaki, Li, & Hirose, 2012); social media platforms, where they are central to marketing campaigns and competitions and many others. The normalization of this technology in such as every day, benign scenarios, create a potent psychological vector for social engineering attacks. Consequently, while technical defences evolve (Tayachi et al., 2025), the average individual lacks the technical capacity resources, rendering them defenceless without integrated protection. Ultimately, this process depends on constant vigilance to overcome the convenience and urgency that attackers exploit, demonstrating that effective personal security is a continuous, conscious application of understanding rather than a passive awareness.

2.5.1.2. Deception Techniques

IV. Spear Phishing

Spear phishing is a targeted attack against an individual, with a significant success rate, due to the fact a phisher gathers personal information. Hence, the planning maximises success (Ahmetoglu & Das, 2022; Kwak et al., 2020; Sibi Chakkaravarthy, Sangeetha, & Vaidehi, 2019; Thomas, 2014; Varshney et al., 2024). Using gathered information makes it possible to tailor emails to appear more credible and trustworthy, making it likely that the victim will be deceived (Iannarelli & O'Shaughnessy, 2015). van der Heijden & Allodi (2019) argue that whether phishing attacks arrives via email, SMS, or social media, the ability to deceive a human is determined by its believability and persuasiveness. The effectiveness of spear phishing attacks is based on replicating the original website/email to look legitimate (PhishLabs, 2016), legitimacy of the email header (Grant et al., 2017), and the email styling (Mao et al., 2013). Whereas spear-phishing is directed at specific individuals or defined groups, whaling attacks represent a further refinement, characterised by an enhanced degree of targeting precision and strategic focus on high-value individuals within organisational hierarchies (Pienta, Jason Bennett, & Johnston, 2020).

Whaling is a classic example of a social engineering attack that manipulates human behaviour and trust (Boulton, 2016). Whaling is a highly targeted form of phishing that specifically targets high-level executives within organisations, aiming to exploit their privileged access to sensitive data (Alabdan, 2020; Gusev, 2022). Cybercriminals who carry out this type of attack are known as whalers (Pienta et al., 2020). General whaling attacks usually involve selecting their target, normally in the "C-Suite" level, a term that refers to an organisation's most senior executives, typically including the Chief Executive Officer, Chief Financial Officer, and Chief Information Officer, among others whose titles begin with "Chief", before they meticulously research the victims, and their immediate contacts, to gather

information, utilise manipulation strategies and select a suitable communication medium, such as email or telephone calls, to deceive the victim (Vanitha et al., 2024)

For example, the chairman of the board of Petroperú was targeted in recent whaling activities, out of many other victims (CE Noticias Financieras, 2024b). Many researchers propose approaches and methods to counteract whaling activity, acknowledging that while whaling, like all phishing, fundamentally exploits human behaviour (e.g. trust in authority or panic), technical solutions can reduce exposure before human judgement is tested. These include the use of ensemble Machine Learning (ML) techniques used for the detection and filtering of spam emails (Fatima et al., 2024), a deep learning-based method to capture the characteristics of the email content (Vanitha et al., 2024), and a control based approach with an implementation of cost evaluation (Olifer et al., 2017). However whaling attacks are found to be challenging since they involve people's behaviour and how they reason about their actions.

2.5.1.3. Dark patterns

The term *dark-patterns* defines as:

> *"Instances where designers use their knowledge of human behaviour (e.g., psychology) and the desires of end users to implement deceptive functionality that is not in the user's best interest" (Gray et al., 2018, p. 1).*

Dark patterns are deceptive design elements in user interfaces that manipulate users into taking actions they did not intend, such as clicking on malicious links, sharing excessive personal information, or agreeing to unfavourable terms. In the context of phishing, dark patterns include visual tricks (e.g., spoofed logos and fake security badges), linguistic manipulation (e.g., creating false urgency with phrases like 'Your account will be closed immediately'), and technical deception (e.g., hiding the true destination URL). As Gray et al. (2018, p. 1) define, dark patterns are "instances where designers use their knowledge of human

behaviour and the desires of end users to implement deceptive functionality that is not in the user's best interest".

The capacity to instantly modify, adapt, and customise various interfaces and features provides significant affordances for malicious acts. A practice defined as a dark patter, these capabilities allow for an attacker to target individuals with precisely tailored environments and messages, thereby manipulating users into performing unintended actions (David & Carmi, 2025). Certain populations are particularly susceptible to such manipulation. Children, for instance, are inherently vulnerable to dark patterns, as they have yet to develop the cognitive defence mechanisms needed to recognise and resist dark patterns (Renaud et al., 2024), youngsters such as university students are included (Gonzalez, 2018).

Dark patterns in phishing emails have evolved significantly from the rudimentary methods employed in the early years of such attacks. Phishing attacks incorporate dark pattern use sophisticated visual deception and refined psychological manipulation, carefully constructed to manipulate users into trusting the message with fake sender domains, urgency in language usage, and spoofed brand logos (Oh et al., 2025). Not only found in phishing emails, a significant number of applications and websites for online shopping often employ dark patterns to manipulate user behaviour to serve commercial interests at the expense of the buyers (Sapkale, 2024).

2.5.1.4. Goal

The primary goals of the deployment of social engineering attacks are fundamentally driven by a set of malicious objectives (Wang, Zhu, & Sun, 2021). Commonly, the objective is getting information (Zimba et al., 2024) or data exfiltration (Hafner et al., 2023), where attackers seek to steal sensitive data such as login credentials, financial details, personal identification information, or corporate secrets, often for use in further crimes such as identity theft or

espionage (Meng et al., 2023). In addition, system sabotage or malware installation, where the compromise of a device or network is intended to cause damage, deploy ransomware, create persistent access, or integrate the system into a botnet is another critical aim in social engineering attacks (Leonov et al., 2021). Another goal is to get the victim to click on a link; this action serves as the essential gateway, initiating the chain of compromise by redirecting users to fraudulent sites to harvest credentials or triggering the download of malicious payloads that lead to data theft, financial loss, or system infiltration. These goals are interconnected and cascading, as illustrated in the Figure 8 in page 29.

2.6. Preventing Phishing Success

2.6.1. Cyber Security Knowledge

A knowledgeable user in cyber threats acts as a crucial first line of defence against the subtle threats of social engineering attacks, thereby strengthening the cybersecurity stance of both organisations and individuals (He & Zhu, 2014). However, those without cyber knowledge will not realise that a cyber threat exists (Renaud & Weir, 2016). Given that no technical security solution can offer absolute protection when it comes to the human factor, it is imperative to focus on equipping users with the knowledge to mitigate these risks (Aldawood & Skinner, 2019).

Prior studies have concentrated on identifying common online safety practices (Revilla, Montoya, & Ramamoorthi, 2023). Although these investigations have advanced the field, a complete understanding of the factors driving online safety practices behaviours, especially attributed to students' cybersecurity knowledge, is lacking (Kovačević, Putnik, & Tošković, 2020; Li & Liu, 2021). Furthermore, the precise measurement of cyber hygiene and its relationship to specific cybersecurity areas remains under-explored.

A critical gap often lies in the practical, detailed knowledge required to implement cyber safe effectively. This underscores that enhanced cybersecurity awareness can only be achieved through a comprehensive understanding of the cybersecurity concept itself and recognizing the availability and function of security features. Enhanced cybersecurity awareness can only be achieved through impacting a comprehensive understanding of the cybersecurity concept itself (Zwilling et al., 2022) and recognizing the availability of security features (Furnell, 2005). Detailed cybersecurity knowledge seems to be key to enhancing user protection (Morgan et al., 2023).

Although a consensus in the field emphasises the importance of cyber knowledge (Jones, Siami, & Armstrong, 2018; Lee & Chua, 2024; Sikos, 2023; Zwilling et al., 2022) and a number of researchers have investigated cybersecurity awareness among young people, see, for example (Nicholson et al., 2020; Oksanen & Keipi, 2013; Quayyum, Cruzes, & Jaccheri, 2021). this study identifies a significant limitation in such an approach. To progress beyond foundational awareness, a specialised and differentiated understanding of specific cybersecurity domains is required. Consequently, this research investigates five cyber knowledge areas; password security, software/system security, human security, organisation security, and social security. This targeted approach is necessary because effective cybersecurity awareness depends on addressing the distinct threats, human factors, and required countermeasures unique to each domain. Recent initiatives have addressed procedural updates, yet there has been a distinct lack of effort to formally recognise or engage youngsters (Claudia & Erika, 2025; Khanzadeh et al., 2025; Nafees et al., 2017; Skopik et al., 2022), moving beyond a one-size-fits-all model of knowledge.

This is to describes the necessary cyber knowledge as *"you cannot secure and protect what you do not know you have"* (Ackerman, 2021, p. 27). The five domains are explained in detail in the sections that follow.

I. Password security

Research has expanded on these concepts, emphasizing the importance of protecting the confidentiality, integrity, and availability of data. As Schatz et al. (2017) noted, password security encompasses a range of practices and safeguards to protect the cyber environment and its users. It is an *"approach and actions associated with security risk management processes followed by organisations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users*" (Schatz et al., 2017, p. 66)

Despite efforts to establish secure practices in data protection, considerable evidence still indicates a widespread lack of password security among internet users. These passwords were often not chosen with security in mind, making them relatively easy to guess or crack (Revilla et al., 2023). Managing passwords is a critical component of maintaining cybersecurity in both daily routines and practical applications (Freminville, 2020). While this problem persists, as evidenced that people tend to have fewer weak passwords in social networking, chat, and webmail services compared to other online platforms (Bonneau, 2012), as they may be reluctant to change their current methods because they are comfortable with them (Renaud, Otondo, & Warkentin, 2019). For instance, a binary sequence with a length of 10 bits offers 1,024 possible combinations, while a 20-bit sequence increases this number to over one million. The necessity of using strong passwords is paramount for protecting sensitive information from unauthorised access. It is advisable to include a combination of letters (both uppercase and lowercase), numbers, and special characters, which collectively complicate the guessing process for attackers when creating password.

However, even the strongest passwords can be rendered ineffective by phishing attacks, which bypass technical brute-force defences by directly deceiving users into surrendering their

credentials. Phishing emails, messages, or websites trick individuals into entering their login details on fraudulent platforms, effectively nullifying password complexity as a security measure (Byun et al., 2024). While strong passwords are essential, they are rendered ineffective if users cannot recognise and resist the deceptive tactics of phishing attacks.

Although it is noted that two-factor authentication (2FA) bolsters security even if a password is compromised, and prevented from unauthorised access (Bhanderi et al., 2023; Jose & Rajasree, 2020). Despite the privilege to have the additional security layers to mitigate the risks posed by cyber threats like phishing and brute-force attacks, millennials display less apprehension about protecting their personal data compared to Generation X and Baby Boomers (Dance, 2019), considering their low knowledge in 2FA (Baraković & Baraković Husić, 2023). The pervasive use of social media platforms amplifies this vulnerability, as they may unintentionally disclose sensitive data or participate in activities that compromise their digital security (Maitland & Lynch, 2020).

II. Software and system security

Software security involves protecting software from security threats, such as viruses, malware, and other malicious software. Software security measures, such as firewalls, antivirus software, and regular updates, help prevent cyber-attacks by addressing vulnerabilities in applications and operating systems. While System security involves protecting the entire IT infrastructure, including networks, servers, and other devices.

Examples of system security measures include network segmentation, intrusion detection systems, and security audits. Neglecting to update software and apply security patches to the network can create vulnerabilities that invite cyber-attacks, for instance the T-Mobile data breach in 2021 (Sievert, 2021).

Depending on the user's software update behaviour preferences, a user may update based on the vulnerability's criticality introduced by vendor, their machines operating system, or based on an application's updates. There is a clear correlation that infected machine do not receive regular updates (Khan, Zehui, & Copeland, 2012) whole some users still lack the knowledge to differentiate between antivirus and firewalls (Talib, Clarke, & Furnell, 2010). This behaviour significantly increases the vulnerability to cyber-attacks. It has been demonstrated that user behaviour with software upgrades can lead to a computer's infection with malicious software or malware (Pérez-Sánchez & Palacios, 2022).

A direct event or failure caused by weaknesses in system and software security is ransomware; a form of malware that encrypts a computer system's data or restricts access until a ransom is paid (Or-Meir, Nissim, Elovici, & Rokach, 2020). While locker, crypto, and MAC ransomware each employ distinct spreading methods, a common denominator is the exploitation of a system and software vulnerabilities. These weaknesses have contributed to ransomware becoming one of the most prevalent and destructive cyber threats (Cohen & Nissim, 2018; Sweta, Sangita, & Bharti, 2022).

Peers (2022) conducted rigorous laboratory tests on various antivirus products to assess their overall security capabilities. Complementing these evaluations, the researchers independently examined how these products detected and blocked a range of Mac and Windows malware samples. This hands-on approach provided insights into real-world performance. Based on these comprehensive assessments, six antivirus products emerged as top performers: AVG, Avira, Bitdefender, Clario, Intego (comprising VirusBarrier antivirus and NetBarrier firewall), and Norton.

From the software development perspective, proactive software security prioritises the early detection approach such as using the fuzzing technique (Miller, Fredriksen, & So, 1990),

creating a large volume of random or unexpected input data to test the reliability and security of a software programme, aiming to uncover potential errors or vulnerabilities (Chen et al., 2018; Liang, Pei, Jia, Shen, & Zhang, 2018; Takanen, DeMott, Miller, & Kettunen, 2018) shown in Figure 11 within the software development lifecycle (SDLC). Pre-deployment security measures (proactive) include activities such as fuzzing, code reviews, and penetration testing conducted during the software development lifecycle (SDLC) before the software is released. Post-deployment security measures (reactive) include activities such as monitoring, patching, and incident response after the software is in use. Otherwise, ensuring the security of deployed code by using penetration testing (Antunes & Vieira, 2014; World, 2021) should be a standardised procedures in SDLC as part of software security defence (Pierce, Jones, & Warren, 2006). Penetration testing is a valuable proactive security measure, but it does not ensure complete security. It must be used alongside other defences, including continuous monitoring, user awareness training, and regular software updates. In addition, access control testing with human expertise and manual testing are still crucial for identifying and addressing access control vulnerabilities effectively (Rennhard, Kushnir, Favre, Esposito, & Zahnd, 2022; Zhong, 2023). Unlike traditional reactive measures that focus on blocking attacks, this approach is the best practice for software developers who seek to identify and rectify underlying weaknesses before they can be exploited.

Figure 11: Reactive post-deployment and proactive pre-deployment security measures for software security (Takanen et al., 2018, p. 11)

This thesis underscores the importance of user understanding, or usage, of post-deployment security measures, such as firewalls, antivirus software, vulnerability scanning, and access control as in complementing the critical role of pre-deployment software development in ensuring overall system security. For instance, Kovačević et al. (2020) in their research found that despite 99.3% of participants using the internet on their cell phones, a surprisingly low 32% reported having antivirus protection installed, which can lead to cyber threats.

III. Human security

Relying solely on technology is not enough, with the advancement of new technology, users must actively protect their information. The significance of human security is increasingly acknowledged (Khadka & Ullah, 2025) as technological measures cannot entirely eliminate the risk of human error or malicious intent (Hadlington, 2017). Human security, as stated by Hitomi (2010, p. 33) is defined as *"human security implies a shift in the way we think about the essence of security"*. Human security signifies a paradigm shift, establishing individuals at the core of security measures, positioning their decision-making based on the knowledge they have in protecting against threats in cyberspace. Essentially, human security is the way humans see threats. Policies and strategies need to be more responsive to the evolving needs and challenges people experience as they navigate digitalization in their daily routines (Zojer, 2020). Cain, Edwards, and Still (2018) reported a large number of users admitting to clicking, downloading attachments, or sharing sensitive information in response to emails from unknown senders. Individuals bear the responsibility for their own security.

Developing phishing resistance is a critical manifestation of this responsibility. The ability to recognise when one is being manipulated (Campbell, 2019) is essential for defending

against phishers, who consistently bypass technical measures (Parthy & Rajendran, 2019) y exploiting habitual actions (Wulandari et al., 2022), lower risk perceptions (Albladi & Weir, 2020), and reliance of indirect cues (Siddiqi, Pak, & Siddiqi, 2022), which signals that users rely on to assess email legitimacy that are not directly related to the email's technical integrity. Building phishing resistance thus requires equipping individuals with both awareness of deceptive tactics and the motivation to practice good cyber hygiene (Montañez et al., 2020). In contrast conceptualising humans, the approach from conceptualizing humans as the "weakest link" to framing them as the "solution", empowering individuals with the knowledge, resources, and motivation to engage proactively in security practices is the stronger approach (Zimmermann & Renaud, 2019).

IV. Organisational security

The term "organisational security" is commonly used to describe the procedures and policies put in place to safeguard a company's data, employees, and operations against external dangers such as those posed by hackers, natural disasters, and other human related threats.

Reducing cyber threats in organisations requires the implementation of defence policies and compliance measures. A security management system is typically put in place to enforce these policies. However, the review of existing literature revealed a gap: numerous organisations face challenges in determining the appropriate security policies for safeguarding their information and data, as they lack knowledge of the most effective policies to implement (Oyelami & Azleena Mohd, 2020). Adopting security management often involves hiring consultants. For instance, adopting the ISO27001 standard can cost up to £22,000 in consultation fees, an expense that poses a major obstacle for small to a small to medium organisations, (Gillies, 2011). Therefore, organisational security measures, such as comprehensive security awareness programmes that educate employees on established policies, are essential.

This is particularly critical as organisations often include early career employees/workers who enter the workforce directly after high school, so apprenticeship models represent a salient example, wherein high school students engage in concurrent employment and structure study. This educational structure has only gained prominence in recent years. This specific intersection of emergent apprenticeship pathways receive only limited scholarly attention according to our research.

Organisations may be exploited by an attacker as a possible entry point. Hence, it is imperative that all staff obtain learning and development opportunities and develop the necessary skills to reduce the risk of human vulnerabilities. Strategic training will influence employees' engagement to training. Adams & Makramalla (2015); van Steen & Deeleman (2021), for instance, found trainings may be futile if one approach fits all is used in an organisation. Hence they recommended combining gamification components that involve a component with player versus a machine since Baxter (2016) found that the implementation of gamification can have a positive impact on both the enjoyment and learning outcomes of the participants. This approach can fundamentally prevent human threat in an organisation. The encouraging results indication that gamification of cybersecurity can increase behavioural control (van Steen & Deeleman, 2021).

Organisational phishing resistance therefore requires a multi-layered strategy (Althobaiti & Alsufyani, 2024). First, technical controls such as email filtering (Mahalakshmi, Pansy, & Thejashree, 2025), domain authentication (DMARC, DKIM, SPF) (Akati & Conrad, 2021), and multi-factor authentication (MFA) (Cuyugan & Rey, 2024) can reduce the volume of attacks reaching employees and limit the damage of compromised credentials. However, as Oh et al. (2025) demonstrate, even technically savvy users can overlook phishing dark patterns. Thus, the second and equally critical layer is to educate employees. Training programmes must move beyond generic cybersecurity awareness to focus specifically on phishing recognition,

teaching employees to scrutinise sender addresses, hover over links before clicking, and question unsolicited urgent requests. Third, organisations should foster a culture where employees feel empowered to report suspicious emails without fear of blame, enabling rapid response to emerging threats (Ramluckan, van Niekerk, & Martins, 2020).

V. Social security

Social cybersecurity is an emerging area of research that intersects science and engineering evolving an area of national security with significant implications for future warfare (Beskow & Carley, 2019). Whereas traditional cybersecurity emphasises the protection of machines and digital systems, social cybersecurity focuses on the protection of individuals, groups and societies and protecting them from being lured, and exploited, from cyberattacks (Carley, 2020). Carley (2020) also implemented the BEND framework, categorizing and evaluating various techniques used to mislead and influence individuals and groups in the digital realm (Figure 12 pg. 47) which is an acronym representing seven categories of social cyber-attack techniques: Baiting, Exploitation, Notice, Distraction, Bias, Emulation, and Neutralisation. Data control in this context derives primarily from social media platforms, whose extensive collection of user information enables threat actors to craft highly personalised and convincing social engineering attacks. For example, 'Baiting' involves offering something enticing to lure victims, 'Emulation' involves impersonating trusted entities, and 'Distraction' involves diverting attention from malicious content. The BEND framework is relevant to this study because it provides a systematic way to understand the manipulation techniques used in phishing attacks targeting youngsters

	Information Maneuver		Network Maneuver	
	Knowledge network manipulation		Social network manipulation	
	Things you can do by effecting what is being discussed		Things you can do by affecting who is talking/listening to whom	
Positive	**Engage**	Discussion that brings up a related but relevant topic	**Back**	Actions that increase the importance of the opinion leader
Positive	**Explain**	Discussion that provides details or elaborates the topic	**Build**	Actions that creates a group or the appearance of a group
Positive	**Excite**	Discussion that brings joy/happiness/ cheer/enthusiasm with the topic	**Bridge**	Action that build a connection between two or more groups
Positive	**Enhance**	Discussion that encourages the group to continue with the topic	**Boost**	Actions that grow the size of the group or make it appear that it has grown
Negative	**Dismiss**	Discussion about why the topic is not important	**Neutralise**	Actions that limit the effectiveness of opinion leader such as by reducing the number who can or do follow or reply or attend to
Negative	**Distort**	Discussion that alters the main message of the topic	**Nuke**	Actions that lead to a group being dismantled
Negative	**Dismay**	Discussion about a topic that will bring worry/sadness/anger to group	**Narrow**	Actions that lead to the group becoming sequestered from other groups
Negative	**Distract**	Discussion about ta totally different topic and irrelevant	**Neglect**	Actions that reduce the size of the group or make it appear that the group has grown

Figure 12: BEND model (Beskow & Carley, 2019, p. 123)

These attacks often leverage the very social contexts that Wu, Edwards, and Das (2022) highlight that family relationships, workplace hierarchies, and even interactions among strangers. For instance, a spear-phishing email might impersonate a family member requesting financial assistance, a colleague sharing a seemingly legitimate document, or a trusted institution demanding urgent action. Therefore, phishing attacks extend beyond individual awareness to encompass a social dimension; fostering collective vigilance, encouraging verification norms, and building cultures where questioning suspicious communications is standard practice.

Data control presents a significant challenge considering the intricacies of how people interact and behave socially (Wu et al., 2022) be it within their families (Brush & Inkpen, 2007), work acquaintances (Watson et al., 2020) or with unacquainted persons (Bossauer et

al., 2020; Radke et al., 2011). Data control lies in its direct amplification of the BEND framework's influence techniques (discussed on page 48). Without access to granular personal data, adversaries cannot effectively deceive, manipulate, or exploit targeted individuals and groups. For example, a spear-phishing email that references a victim's recent vacation location or job title is far more convincing than a generic scam message. Thus, data control is a critical vulnerability that enables sophisticated social engineering attack.

To the best of this researcher's knowledge, no prior study has deconstructed cybersecurity awareness into five distinct knowledge domains and empirically tested their differential influence on behavioural intentions using the Theory of Planned Behaviour within the specific context of Malaysian youngsters aged 18-26. Furthermore, few studies have combined a large-scale survey with a controlled phishing simulation to directly compare self-reported intentions with observed behaviour in this demographic. It is this domain-specific, multi-method approach that distinguishes the present research from prior work on youngsters' cybersecurity.

2.6.2. Behavioural and demographic differences in Cyber Security

However, simply being aware of standard cybersecurity measures, such as strong passwords, firewalls, and access controls does not equate to their correct application (Frank & Eweniyi, 2013; Hawamleh et al., 2020; Mtair, 2023). Human behaviour is complex and dynamic and is influenced by a multitude of factors including demographic disparities. Understanding these characteristics can be challenging due to their unpredictable nature.

Age is known to be one of the demographic factors that significantly impacts the behaviour in cybersecurity (Branley-Bell et al., 2022; Jarvie & Renaud, 2024; Mwagwabi & Jiow, 2021). Young people, heavily reliant on the internet for daily life, are increasingly vulnerable to cybercrime (Zhang et al., 2020). Their active engagement in online communities,

such as social media platforms, makes them prime targets. Coupled with their often-limited ability to discern online threats, this heightened exposure significantly increases their risk of falling victim to cyberattacks. Although they can be more confident in using online banking (Chiew, Yong, & Tan, 2018), research conducted in Finland by Oksanen & Keipi (2013) revealed that teenagers are significantly more likely to experience cyberattacks than adult, owing to their status as more native internet users with particularly heavy engagement in social media platforms (Alqahtani et al., 2023; Angela, Huda, & Rusdiyan, 2025; Pangrazio & Cardozo-Gaibisso, 2020).

Anwar et al. (2017) found that sociodemographic factors, particularly gender, significantly influence cybersecurity behaviours. The study revealed a statistically significant gender gap in cybersecurity knowledge, with males demonstrating higher levels of cybersecurity knowledge (Cain et al., 2018). While males may be viewed as more technologically proficient, females might exhibit greater caution and risk aversion (Shehata & Eldakar, 2024). While these traits appear stable on average, an important question is whether a 'tipping point' exists, for instance, a specific level of cybersecurity knowledge or a particular age at which the protective benefit of female caution is eclipsed by male technical proficiency.

In addition, academic achievement can be a factor in determining levels the effectiveness in cybersecurity hygiene (Donalds & Osei-Bryson, 2020). Academic institutions and private companies are increasingly offering cybersecurity awareness training to boost individual protection (Ugwu et al., 2023). However, a crucial question arises: how can those without a university education access similar knowledge and skills?

In Scotland, structured cybersecurity education terminates at Primary 7, and jeopardises cohesive readiness to secondary students, resulting in a significant deficiency as secondary students are the common targets of cyber threats (Prior & Renaud, 2022). Research on

Australian adolescents indicated that knowledge, on its own, does not consistently lead to protective behaviours, as the persistence of adolescents' behaviour in security threats highlights the security paradox, suggesting a gap in cybersecurity knowledge and behaviour (Al-Saggaf & Maclean, 2024; Quayyum et al., 2021). Youngsters navigate the cyberspace environment where the traditional boundaries separating content, contact, and conduct risks are not distinct but are instead overlapping and blurred, complicating their ability to differentiate between real and perceived threats (Gaspard, 2020).

Research with students in two different countries, Hungary and Vietnam, exhibited similar deficiencies in cyber security knowledge but neglected secure smartphone practices and established that this is a widespread issue that other countries would also identify (Thao & Tick, 2021). Hence, deficiency is not attributable to a single cause but rather the behavioural neglect and the inherent characteristics of mobile device use. This research acknowledges this multi-faceted reality by incorporating dark pattern cues (e.g., urgency, visual deception, and language manipulation) into the phishing email designs, as detailed in Section 3.4.2.2, and by ensuring that the phishing simulation emails were compatible with both mobile phone and computer viewing. Research indicates that young users, who bear increasing responsibility for their own digital safety, tend to make riskier decisions when faced with unfamiliar online interactions (Nicholson et al., 2020). Research from Finland (Oksanen & Keipi, 2013) showed that individuals aged 15–24 were more likely to experience cyberattacks, as compared to older age groups, and the absence of a comprehensive cybersecurity curriculum across all educational levels should be further mitigated as most of the research and implementation at University level and should be implemented much earlier in educational levels (Martti, 2020).

On the other hand, students in academic institutions basically integrated cybersecurity awareness within the institution whist their studies to the fundamental in cybersecurity, which determined the difference with other level of education (Donalds & Osei-Bryson, 2020).

This perspective is not without contention. Multiple authors have found that demographic differences do not significantly correlate with certain cyber-attacks, for instance malware attacks (Lévesque et al., 2018), this research believe in contrasts with two other findings (Lévesque, Fernandez, & Batchelder, 2017; Shehata & Eldakar, 2024) and related to phishing attacks (Holbrook et al., 2010) which contradict or challenge its conclusion with indication to a significant correlation.

2.6.2.1. Theory of Planned Behaviour (TPB)

The Theory of Planned Behaviour (TPB) builds upon the Theory of Reasoned Action (TRA), introduced by (Fishbein & Ajzen) in the 1970s. Central to the TPB is the notion that an individual's intention to perform a specific behaviour is the primary determinant of that behaviour. This intention is shaped by three factors: personal attitudes toward the behaviour, subjective norms (perceived social pressure), and perceived behavioural control (self-efficacy). It is important to clarify the causal direction: subjective norms influence intentions, and intentions influence behaviour. Behaviour does not directly shape intentions, although past behaviour can influence future intentions through habit and experience, in Figure 13 (Ajzen, 2024). This framework is directly applicable to this study's objective of understanding the relationship between youngsters' knowledge and their actual behaviour during a phishing simulation.

The TPB allows us to move beyond simple knowledge assessment and investigate why a user falls for a phish: Is it due to carelessness? Is it the influence of a workplace culture not prioritising security (a subjective norm)? Or is it a lack of confidence in their ability to identify a threat (low Perceived Behaviour Control (PBC))? With both subjective norms and PBC explained in Section 2.6.2.2. Consequently, the TPB provides a multi-faceted lens to dissect the behavioural antecedents of phish detection, making it a highly suitable and robust theory for this research, despite its noted underutilisation in the cybersecurity domain (Akhyari,

Abdullah, & Rashid, 2018; Anderson & Agarwal, 2010; Burns & Roberts, 2013; Donalds & Osei-Bryson, 2020; Safa et al., 2015; Sulaiman et al., 2022).

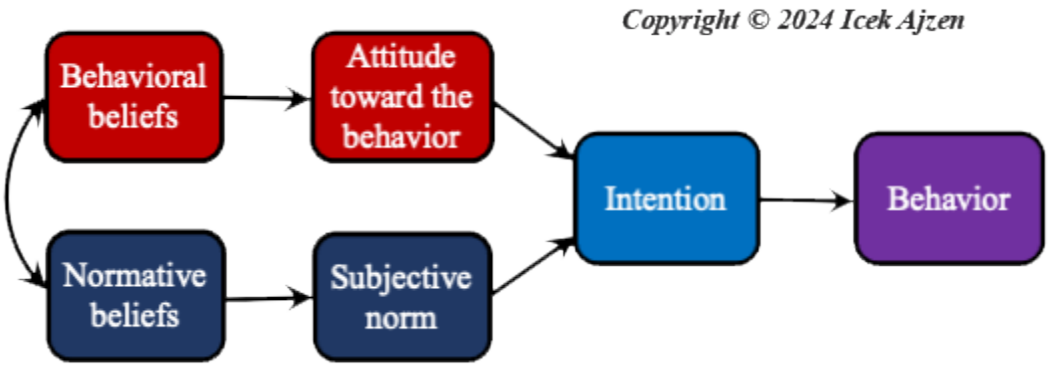


Figure 13 Theory of Reasoned Action. Reprinted from Theory of Reasoned Action, by Ajzen, I., Retrieved November 17, 2024, from https://people.umass.edu/aizen/tra.html

The Theory of Reasoned Action (TRA) posits that a person's intention to perform a behaviour is a primary determinant of that behaviour. Intentions are shaped by attitudes towards the behaviour and subjective norms, reflecting perceived social pressure. The TRA remains a cornerstone for understanding human behaviour across diverse fields. Its enduring influence is evident in contemporary research (Akther & Nur, 2022; Al-Husseini, 2023; Alzahrani, Hall-Phillips, & Zeng, 2019; Bauer & Bernroider, 2017; Davis et al., 2022). The importance of this model underscores its value in exploring the complex relationships between attitudes, subjective norms, and behavioural intentions within today's dynamic and expanding research environment.

Building on the foundation of the Theory of Reasoned Action (TRA), the Theory of Planned Behaviour (TPB) incorporates the additional construct of perceived behavioural control, providing a more comprehensive framework from for understanding and predicting human behaviour. Figure 14 presents the full TPB model; the leftmost column specifically delineates

the three belief types (behavioural, normative, and control) that serve as the foundational antecedents to attitude, subjective norm, and perceived behavioural control, respectively.

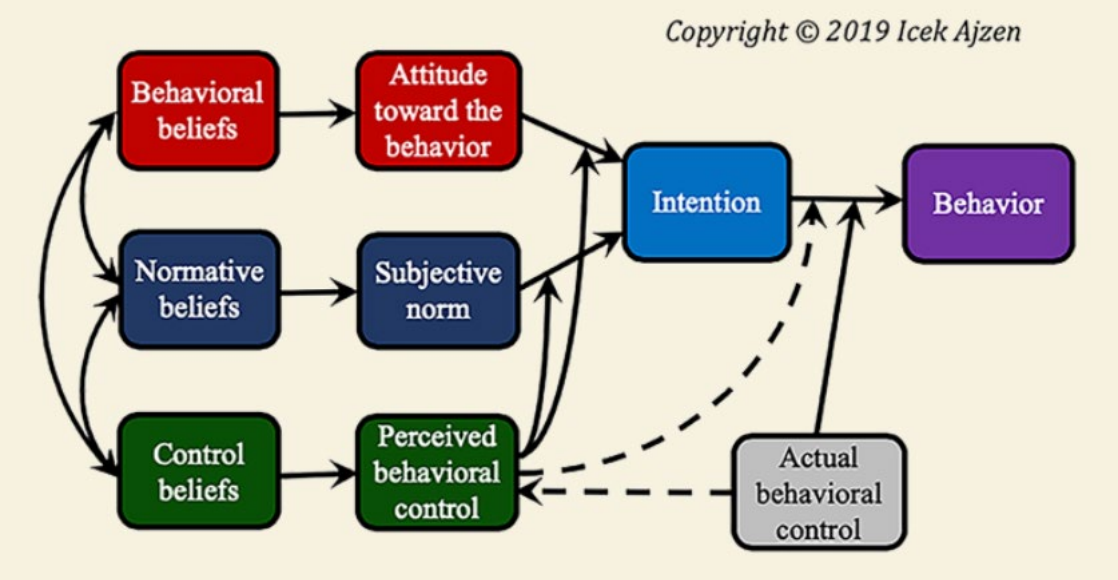


Figure 14: The theory of Planned Behaviour (Ajzen, 2019)

"*According to the theory of planned behaviour, intention (and behaviour) is a function of three basis determinants, one personal in nature, one reflecting social influence, and the third is dealing with issues of control*" (Ajzen, 2005, p. 117). In 1985, Ajzen identified the significant flaw and the boundary conditions of Ajzen's theory of reasoned action, which did not adequately address transitioning between intention and behaviour, (Ajzen, 1985). TRA was first developed by two scholars and the theory stated that intention is the best predictor of behaviour. Intention, based on TPB, is the product of three different processes, (Fishbein & Ajzen, 1975, 1980, 2011).

This addition acknowledges that while attitudes and subjective norms influence intention, their impact can vary depending on an individual's perceived ability to perform the behaviour (self-efficacy). As Ajzen (1991) noted, the relative importance of these factors depends on both the behaviour itself and the environmental context. Importantly, intentions

reflect an individual's motivation and commitment to a behaviour, reflecting anticipated effort and action. These core components of the TRA and TPB, as outlined in Table 2, provides a foundation for understanding and predicting human behaviour.

Table 2 Differences Between Theory of Reasoned Action (TRA) and Theory of Planned Behaviour (TPB)

Aspect	Theory of Reasoned Action (TRA)	Theory of Planned Behaviour (TPB)
Founders	Martin Fishbein and Icek Ajzen (Fishbein & Ajzen, 1975)	Icek Ajzen (Ajzen, 1985)
Core elements	• Attitude toward behaviour	• Attitude toward behaviour
	• Subjective norms	• Subjective norms
		• perceived behavioural control (PBC)
Introduction	Introduced in the late 1970s as a framework for understanding and predicting human behaviour based on rational decision-making processes.	Developed in the late 1980s as an extension of TRA, adding the dimension of perceived behavioural control to provide a more comprehensive model of behaviour prediction
Determinants of Behaviour	**Attitude** Reflects an individual's personal evaluation of a specific behaviour as positive or negative.	**Attitude** Remains a key determinant of behavioural intention, representing an individual's overall assessment of a behaviour's desirability.
	Subjective norms Perceived social pressures and expectations from significant others related to the behaviour.	**Subjective norms** Like in TRA, TPB considers the influence of perceived social pressures and expectations on behaviour.
		Perceived Behavioural Control (PBC) Adds perceived behavioural control as a factor influencing behavioural intention. This considers an individual's belief in their capability to perform the desired behaviour, detail in 2.6.2.2 (III).

Role of Intention	An individual's intention is the primary determinant of behaviour.	Intention is a key predictor of behaviour, influenced by attitudes, subjective norms, and perceived behavioural control.
Incorporates	TRA focuses on the attitudinal and normative aspects of behaviour.	TPB extends TRA by adding the dimension of perceived behavioural control (PBC), which addresses the influence of perceived control and self-efficacy on intention and behaviour.
Example Scenario	An individual's decision to initiate recycling is influenced by personal views on recycling and the perceived expectations of close associates (Sujata et al., 2019)	The intention to use a secure password manager is shaped by: (1) personal opinions about the tool (attitude); (2) social pressures from peers and colleagues (subjective norms; and (3) confidence in effectively managing the tool (perceived behavioural control – an individual self-efficacy belief, not group conformity
Applicability	TRA is used in various fields to understand and predict behaviour, particularly in domains where attitudes and social norms play a significant role.	TPB is applied in situations where perceived control and self-efficacy are important factors influencing behaviour, such as technology adoption, healthcare, and environmental sustainability.

2.6.2.2. Application of TPB in Cyber Security Research

The adoption of the Theory of Planned Behaviour (TPB) for this research is justified by robust empirical evidence supporting its core constructs, which have proven effective in understanding and predicting human behaviour. While the theory of planned behaviour is undeniably one of the most successful theories in the field of psychology, the recognition of the theory can also be seen from other fields such as computer science and technology, others such as business and economics (Jimmieson, Peach, & White, 2008; Kautonen, van Gelderen, & Fink, 2015; Liobikiene, Mandravickaite, & Bernatoniene, 2016; Tan, Ooi, & Goh, 2017), engineering (Chen, 2016; Mohammadinezhad & Ahmadvand, 2020; Wang et al., 2014; Zhao et al., 2018) and others (Shapiro, 2000; Sukhmani, 2017; Wynn, Smith, & Killen, 2021).

Especially in the context of cybersecurity, the use of TPB has also increased over time. However, these applications remain largely general rather than domain-specific to cybersecurity. Specifically, there were researchers that used the same theory to investigate the connection between cybersecurity and human behaviour, (Askew et al., 2019; Choi, Cho, & Lee, 2019; Palmieri, Shortland, & McGarry, 2021; Rana et al., 2019) and this has gradually increased.

The Theory of Planned Behaviour has been recognised as a powerful model in predicting and explaining various types of human behaviours, including those related to information security (Akhyari et al., 2018; Burns & Roberts, 2013; Farhana, Fahmie, & Wan, 2021; Sulaiman et al., 2022)

I. Attitude Towards Cybersecurity Practices

In the context of cyber security, an individual's attitude towards behaviours like using strong passwords or enabling two-factor authentication is shaped by perceived consequences, such as the risk of account compromise. Subjective norms, influenced by peers and social groups, also impact cybersecurity actions. Additionally, perceived behavioural control, determined by factors like technical skills and resource availability, plays a crucial role.

Understanding these factors is pivotal for designing effective interventions. Educational programmes can enhance knowledge and skills, while social marketing can positively influence attitudes and norms. The TPB provides a valuable framework for predicting, explaining, and changing cybersecurity behaviours.

Previous research (Donalds & Osei-Bryson, 2020; Lorenz, Kikkas, & Osula, 2019; McGuire, 2015) has emphasised the importance of cybersecurity knowledge. Moreover, their study failed to identify the underlying motivations for this behaviour. Wang (2013) anti-phishing study revealed a positive correlation between knowledge and attitudes towards

cybersecurity solutions. Burcu, Hasan, and Izak (2010) and Jensen et al. (2017) also found that employee attitudes, influenced by factors like compliance benefits and costs, impact the effectiveness of security awareness training.

II. Subjective Norms

The Theory of Planned Behaviour also considers the role of subjective norms, which refer to an individual's perception of the social pressure exerted by important referents, such as family, friends, or peers, to engage or not engage in a particular behaviour. In the context of cybersecurity, subjective norms can play a significant role in shaping an individual's intentions and behaviours. Existing research indicates that individuals who perceive strong encouragement and support from their peers, family members, or other influential groups to adopt cybersecurity practices are more likely to follow through and engage in such behaviours (Lin et al., 2021). Findings based on Wiafe et al. (2020) strengthen the argument that the actions of others significantly impacted individuals' willingness to justify their own security transgressions, thereby normalising such behaviour (Kim, Yang, & Park, 2014). However, for teenagers, the strong influence of peers significantly discourages compliance with cybersecurity best practices, thereby increasing risky online behaviour (Mwagwabi & Jiow, 2021).

III. Perceived behavioural control

The third key construct in the Theory of Planned Behaviour is perceived behavioural control, which refers to an individual's perceived ease or difficulty of performing a particular behaviour. In the context of cybersecurity, this construct is particularly relevant as it can influence an individual's confidence and willingness to engage in protective behaviours. Studies have shown that when individuals feel more in control and confident in their ability to use cybersecurity measures, they are more inclined to adopt and maintain such practices (Yi et al., 2025).

Empowering young people, such as by making strong password habits feel achievable and manageable, is important, as they often feel overwhelmed by password requirements or doubt their ability to remember complex passwords (Renaud et al., 2019). Whether people seek both control over their circumstances **and** the ability to act freely (Köse & Doğan, 2019), there can be a mismatch between individuals' beliefs about their secure behaviour and their actual behaviour (Hoong, 2021). This discrepancy can significantly affect cybercrime.

IV. Intention

A fundamental premise of the Theory of Planned Behaviour is that an individual's intention to perform a particular behaviour serves as a strong predictor of their actual engagement in that behaviour. Research has demonstrated that individuals with a stronger intention to adopt protective measures, such as using strong passwords, updating software, or being cautious when sharing personal information online, are more likely to engage in these behaviours in the context of cybersecurity (Burns & Roberts, 2013).

V. Behaviour

The goal of the Theory of Planned Behaviour is to predict and explain actual behaviour. In the context of cybersecurity, this would translate to individuals' actual engagement in protective behaviours, such as using strong passwords, updating software, and being cautious when sharing personal information online. Extensive empirical evidence has consistently shown that the key constructs of the Theory of Planned Behaviour, including attitude, subjective norms, and perceived behavioural control, are highly effective in predicting and explaining individuals' cybersecurity-relate.

Internet users' actions can significantly influence the outcome of various situations, as technological advancements have created a wider range of factors that can trigger individual behaviour (Warren, 2018).

2.7. Malaysia's Cyber Security: Challenges, Initiatives and Legislative Practices

Figure 15 Administrative divisions of Malaysia (Central Intelligence Agency, 2021)

Malaysia is a Southeast Asia country (Figure 15), consisting of fourteen states which has undergone significant economic and technological development (Department of Statistics Malaysia, 2021). The country has transformed from a primarily agricultural economy to a diversified, export oriented, driven by the manufacturing and services sectors. The government has made efforts to promote technological advancement and innovation, leading to the growth of various industries, including information and communication technology (ICT). Malaysia has invested substantially in ICT infrastructure, becoming a hub for technology companies and startups (Bawaba, 2014; Tang & Rosidi, 2025; Tiong, Cheng, & Choong, 2022).

2.7.1. Public-Private Collaboration Initiatives to govern cybersecurity in Malaysia

2.7.1.1. Malaysia's Legislative Measures

The Malaysian government has implemented substantial measures to tackle cybersecurity concerns; the Dewan Negara (Senate, the upper house of the Parliament of Malaysia) has recently approved the Cyber Security Bill 2024 (Bernama, 2024) and enacted as the Cyber Security Act 2024 by the Attorney General's Chamber in June 2024 (National Cyber Security Agency, 2024), to govern National Critical Information Infrastructure (NCII) in Malaysia.

Critical National Infrastructure (CNII) for Malaysia is defined as:

"*A computer or computer system which the disruption to or destruction of the computer or computer system would have a detrimental impact on the delivery of any service essential to the security, defence, foreign relations, economy, public health, public safety or public order of Malaysia, or on the ability of the Federal Government or any of the State Governments to carry out its functions effectively*" (National Cyber Security Agency, 2024, p. 9).

Malaysia has established a robust legal framework for cybersecurity, encompassing a range of legislation since 1997. The cyber laws in Malaysia are shown in Figure 16.

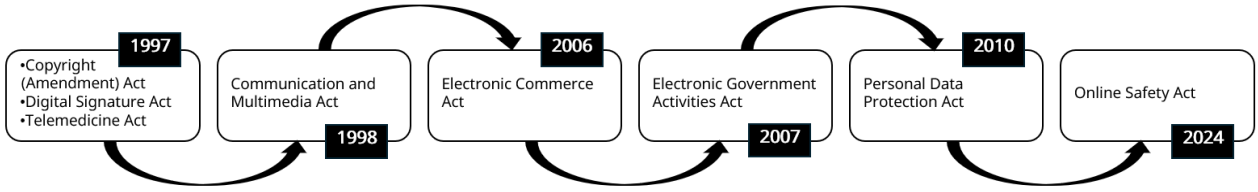


Figure 16: Cyber laws in Malaysia

2.7.1.2. National Cyber Security Agency (NACSA)

NACSA is Malaysia's leading agency for cybersecurity, tasked with safeguarding the Critical National Information Infrastructure (CNII) by coordinating cybersecurity efforts, countering cyber threats, and raising public awareness. NACSA develops and implements cybersecurity policies, enhances capacity, and collaborates internationally to address cyber challenges.

One notable establishment under NACSA is the National Cyber Coordination and Command Centre (NC4), which handles national-level cybersecurity threats and disasters. NC4 is linked to various Security Operation Centres (SOCs) in Malaysia, including CyberSecurity Malaysia SOC, Government Integrated Telecommunications Network (GITN) SOC, Cyber Defence Operation Centre (CDOC), and MCMC Network Security Centre. Additionally, X-Maya, a National Cyber Crisis Exercise from the National Cyber Crisis Management Plan (NCCMP), is another initiative by Malaysia to counteract cybersecurity threats and attacks.

2.7.1.3. National Cyber Security Policy (NCSP)

Meanwhile, the adoption of the NCSP in 2006 marked a significant advancement prompted by Malaysia's recognition of cybersecurity as a crucial national concern in the digital age. The main objective of the NCSP framework is to effectively handle and reduce risks related to the Critical National Information Infrastructure (CNII). The NCSP promotes worldwide collaborative efforts in tackling global cyber threats. Malaysia actively collaborates with other states and international organisations to strengthen Malaysia's strategic position in information security.

2.7.1.4. Cybersecurity Malaysia

Figure 17: Toward a safer and more secure cyberspace (Cyber Security Malaysia, 2024)

Another Malaysian government's effort to counter cyber threats is services offered by Cybersecurity Malaysia are shown in Figure 17 above. The Cyber Security Awareness for Everyone (CyberSAFE), an initiative focuses on enhancing cybersecurity knowledge among children, youngsters, parents, and organisations. However, the CyberSAFE programme has yet to achieve optimal public engagement. While approximately 170,000 individuals, primarily within the 15-64 age group, participated in the programmes in 2018 (Abdullah, Mohamad, & Yunos, 2018). Broader participation is essential to maximise its impact. Complementing these efforts is the Mobile Assessment Security Scanning Application (MASSA), developed by MyCERT (Khalid, Aziz, Arif, & Rifai, 2023). While MASSA offers a valuable tool for Android

users to assess mobile security, its exclusivity to this platform restricts its overall reach. Expanding MASSA to encompass other operating systems would significantly enhance its potential to protect the public from cyber threats.

2.7.1.5. National Security Council (NSC)

The implementation of Malaysia Cyber Security Strategy 2020-2024 (Malaysian National Security Council, 2020) aims to enhance cybersecurity awareness among Malaysian citizens through well-coordinated and effective programmes and initiatives. The strategy is built on four strategic pillars:

a. Pillar 1: Governance, Legal and Regulatory Framework
b. Pillar 2: Cyber Security Technology and Operations
c. Pillar 3: Cyber Security Culture and Public Awareness
d. Pillar 4: Cyber Security Education, Skills and Talent Development

This study centres on pillar 4 as in Figure 19, which emphasises skill and knowledge development, raising awareness, and providing education to the people – with specific attention to youngsters as a target group. For instance, Pillar 4 suggests introducing cyber security as a subject in primary, secondary a.d tertiary curricula in collaboration with the Ministry of Education Malaysia. For instance, it suggested to introduce cyber security subject as one of the syllabi at primary, secondary and tertiary level with the collaboration with Ministry of Education Malaysia. The statement acknowledges that although there have been efforts to create required initiatives and programmes, there are obstacles in terms of resources, approaches, and target groups when it comes to improving cybersecurity awareness in Malaysia. The report emphasises the necessity of a more comprehensive implementation plan for promoting awareness of cybersecurity.

In order to successfully increase awareness, it is imperative for all parties involved to collaborate to provide fundamental education in the field of cybersecurity to individuals who utilise technology. The initiative needs to be widely exposed to assess the value of cybersecurity information and comprehend the correlation between demographic and behavioural factors in this setting.

The government has launched initiatives in the Digital Malaysia programme (Chong, Puah, & Teh, 2025) such as Digital Free Trade Zone (DFTZ) and National Fiberisation and Connectivity Plan (NFCP), aiming to increase the country's digital competitiveness and establish Malaysia as a developed digital economy. Additionally, the government has encouraged the development of the e-commerce industry and taken steps to promote cybersecurity (Athena Information Solutions, 2022; Powell, 2021).

Since then, widespread internet access in Malaysia has increased dramatically. By 2019, 98% of the population in Malaysia owned mobile phones, and 76% had home internet subscriptions (Department of Statistics Malaysia, 2019). The digital revolution has brought significant benefits, but it has also come with a darker side, as it heightened cybersecurity risks. As the reliance on online platforms grows, so does the potential for cyberattacks, data breaches and other malicious activities.

Alongside these positive development, businesses and individuals face a rising tide of threats from phishing, ransomware, and cybercrime, which can inflict significant financial damage, compromise sensitive information, and disrupt critical services (See Figure 18).

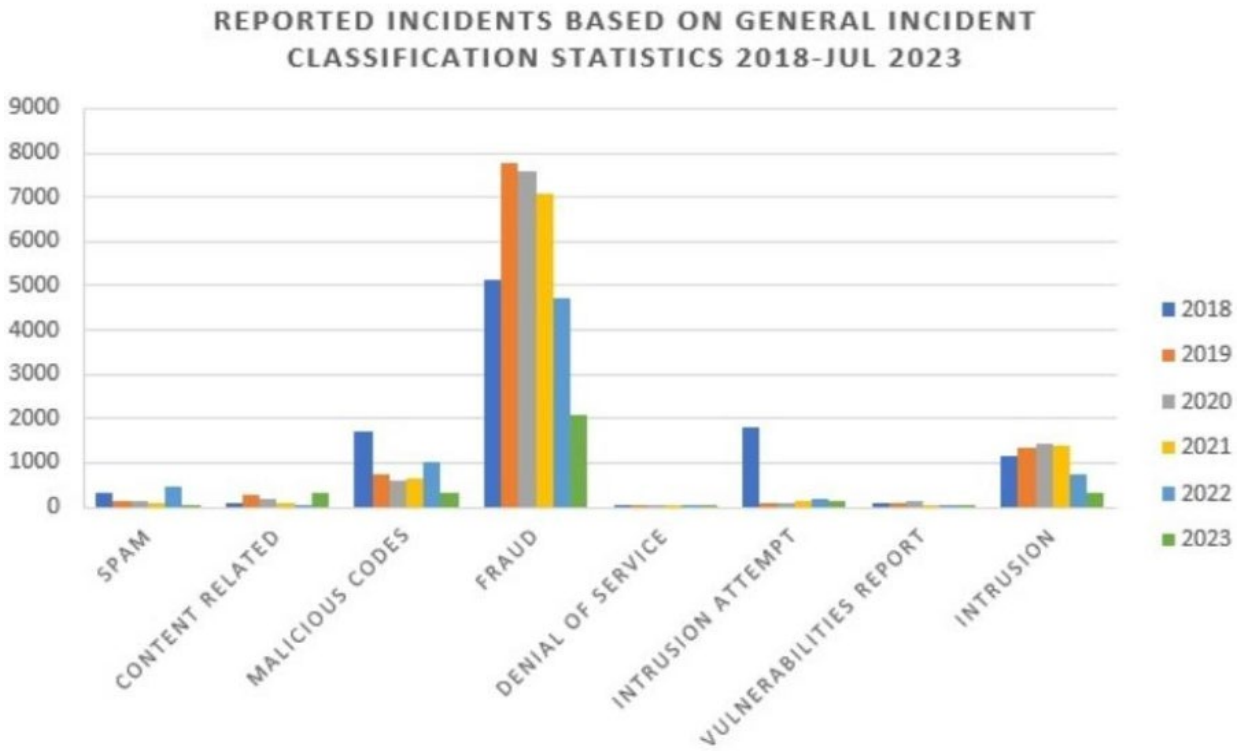


Figure 18: Cybercrime classification in Malaysia, 2018-2023

Cybercrime in Malaysia has surpassed traditional crime, with Malaysia leading Southeast Asia in malware attacks, recorded at sixteen million in one year to (Digital News Asia, 2019). The Royal Malaysia Police reports that seventy percent of crimes are now cyber-related (Ariffin & Letchumanan, 2020). Malaysia incurred losses amounting to RM2.23 billion (£382 million) due to cyberattacks. Not only that, but Malaysia has also been ranked 8th among the world's most breached nations, in 2024 Q2, the population has experienced a sharp rise of 144% with a large majority of online or phone scam (Azmin & Serota, 2024).

These attacks can cripple the critical infrastructure and destabilise economic, political, and social activities (Yunos et al., 2010). tech savvy youngster are a prime target for cybercriminals. Their confidence and frequent online activity may lead to risk-taking behaviours, such as reusing passwords or clicking unverified links, increasing their vulnerability. Research highlighted that youngsters are particularly vulnerable to cyber threats

despite, or sometimes because of, their digital skills (Bordonaba-Juste, 2020; Fatokun et al., 2019).

Figure 1 in Section 1.1 page 7 shows the demographic distribution demonstrates a shift from 4.0% (ages 15–19) to 4.6% (ages 20–24), highlighting a growing young adult population. This 0.6% increase reflects a larger demographic group entering early adulthood. In Malaysia, adults aged 15 to 64, who are most likely to understand cyberspace and the impact of cyber threat, dominate the population at 69%. Youngsters' population between 15-30 is approximately 40% of Malaysia's population. In contrast, minors under 15 make up 23%, while seniors aged 65 and above account for just 7% (Department of Statistics Malaysia, 2019).

This research concentrates on 18–26-year-olds; underlines the relevance of studying this age group, as they represent a transitioning population (from high-schooler to university and adulthood) where cyber behaviour and knowledge are expected to grow dramatically.

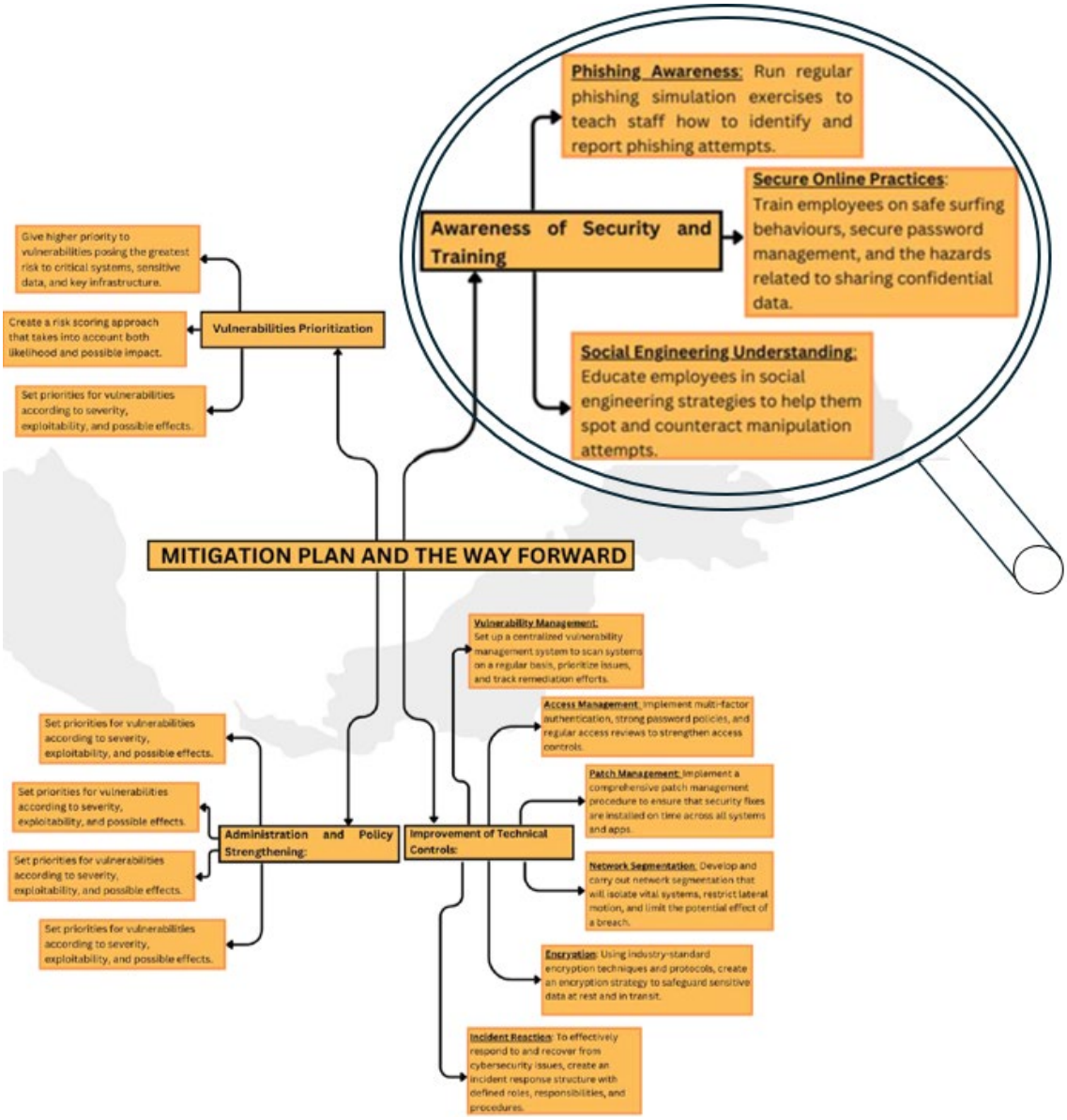


Figure 19 (CyberSecurity Malaysia, 2023)

Based on the latest mid-year threat landscape report, phishing and malware attacks remained persistent threats throughout the first six months of 2023 (CyberSecurity Malaysia, 2023) and can be seen in Figure 18 in page 65. Echoing this point, Figure 19 outlines key mitigation initiatives from CyberSecurity Malaysia, emphasising those related to security awareness and training to minimise cyber threats. It adds to the discussion by illustrating the gap between existing national initiatives and the needs of the youngster demographic.

However, while the mitigation plan offers a strategic framework for securing organisational infrastructure and staff, it presents a critical limitation by overlooking the security of native internet users, who are a primary target of the cited phishing and malware threats. The plan's focus on management performance and standardised organisational metrics fails to account for generalisation of vulnerabilities. This omission directly underscores the research gap this thesis addresses, validating the necessity to shift focus beyond institutional security and develop targeted awareness interventions that are holistically tailored to the demographics, who represent a critical front in the modern cyber threat landscape.

2.8. Malaysian Youngsters' Cybersecurity Knowledge–Behaviour Intention Gap

Youngsters represent one of the most active groups in the digital environment, relying heavily on the internet for education, entertainment, communication, and financial transactions. Malaysian secondary students use social media for an extensive five hours daily (Ahmad et al., 2018). This extensive engagement, while enhancing digital literacy, also increases exposure to cyber threats such as privacy issues and cyberbullying. Studies consistently highlight a paradox: despite being adept technology users, youngsters often lack the depth of cybersecurity knowledge necessary to protect themselves effectively (He & Zhu, 2014; Renaud & Weir, 2016). This knowledge deficit is compounded by risky behavioural patterns that heighten their vulnerability.

For instance, Saudi et al. (2021) presents a proof-of-concept security model (Mobotder) for detecting vulnerabilities in mobile gaming apps, determined that 70% of tested games in the Google Play Store posed medium security risks with recommendation for a better education, secure development practices, and tools like Mobotder to mitigate exploitation. Further Yaacob, Haryani, and Zahurin Ma (2021) stated that youngsters in Malaysia possess gaming disorders with online addiction in over three-quarters of the youngsters surveyed

(76.9%) engaged in gaming via mobile phones. In the Malaysian context, a comprehensive and validated assessment instrument capable of delineating and evaluating these type of Problematic Internet Use (PIU) remains notably absent (Siaw et al., 2025). Not only online game addition, but cyberbullying, personal data misuse, unwanted exposure to pornography (Yusuf et al., 2023) correspondingly lead to youngsters experiencing risky online behaviour. In addition, using a phishing simulation using a link in WhatsApp, a cross-platform instant messaging (IM) and voice-over-IP (VoIP) service owned by Meta Platforms (Farooq, Dahabiyeh, & Javed, 2024) to detect users' susceptibility in phishing attack, Ali & Rahman (2025) found that the convergence of financial strain, a tendency toward impulsivity, and increased receptiveness to incentives, renders younger adults more prone to phishing attack.

In CyberSAFE Malaysia (2017) it is noted that a substantial percentage (50%) of middle school students in Malaysia engage in online activities without supervision from their parents Furthermore, as active users in cyberspace especially for social media user, university students in Malaysia demonstrated moderate levels for protecting themselves from cyber threat and scam (Shahidah et al., 2021). Ramakrishnan, Yasin, and Periasamy (2022) seconded in their survey that through an improved cybersecurity awareness defined by the interrelationship of knowledge, behaviour, and attitudes, and how these elements influence one another.

Cybersecurity knowledge is a critical first line of defence against threats such as phishing, malware, and social engineering. Yet, evidence suggests that many youngsters are unaware of fundamental security principles or fail to apply them consistently in daily digital practices. For example, weak password habits remain common, with individuals frequently reusing credentials across platforms or neglecting to adopt protective measures such as two-factor authentication (Baraković & Baraković Husić, 2023). While technical measures such as firewalls and antivirus software are widely available (Nick, 2022), many youngsters either fail

to install them or misunderstand their functionality (Talib et al., 2010), leaving systems open to exploitation.

Behavioural studies reinforce this gap between knowledge and behaviour. Although young users are often aware of threats like phishing, their online conduct does not always reflect this awareness. This may manifest in clicking on suspicious links, oversharing personal information on social media, or ignoring security warnings (Cain et al., 2018; Maitland & Lynch, 2020). Overconfidence in their digital skills could lead them to underestimate risks, while habitual online behaviours, formed through convenience and speed, encourage shortcuts that compromise safety (Wulandari et al., 2022). Furthermore, peer influence can normalise unsafe practices, such as sharing account credentials or bypassing security protocols (Murtaza et al., 2022)

While young adults may demonstrate confidence in activities like online banking (Chiew et al., 2018), this confidence does not always correlate with secure behaviours. Differences in education also play a role: university students often receive some formal cybersecurity training, whereas peers outside academic institutions may lack structured exposure to such content (Donalds & Osei-Bryson, 2020).

The inconsistency between knowledge and behaviour among youngsters aligns with the constructs of the Theory of Planned Behaviour (TPB). Attitudes toward cybersecurity can be shaped by perceived inconvenience, leading to neglect of protective measures despite recognising their importance. Subjective norms, such as the influence of friends or online communities, may encourage risky practices even among knowledgeable users. Perceived behavioural control is also a factor, with some youngsters feeling overly confident in their technical skills without fully understanding the scope of cyber threats. These constructs help to explain why cyber knowledge and technical interventions alone may be insufficient in

preventing successful attacks without addressing the underlying psychological and social influences on behaviour.

Researchers have developed multi learning techniques to engage in cyber security education such as student-centric learning, problem-based learning, game-based learning, self-paced learning, and integrated learning, as proposed by Te-Shun (2019), to a virtual escape room (Löffler et al., 2021) as an effort to strengthen cybersecurity resilience among youngsters. To align this, research by Mwagwabi & Jiow (2021) highlighted the lack in motivating better cybersecurity practices in teens with the use of theory-based studies on teen cybersecurity behaviour. However, this engagement must not only enhance technical understanding but also actively address human vulnerabilities, social influences, and biases that undermine secure practices.

Integrating behavioural science with cybersecurity education, tailored within these multi learning techniques, offers a promising path to bridge this gap.

2.9. Summary

This literature review explored the dynamic interplay between cybersecurity knowledge and behavioural practices among Malaysian youngsters, with a particular focus on phishing vulnerability. It highlights the pressing need for cyber resilience in a rapidly digitalizing society, emphasizing the importance of understanding both technical and human-aspects of cybersecurity.

The foundational concept of cybersecurity is rooted in preserving the confidentiality, integrity and availability principles. While definitions vary across academic, governmental, and international contexts, they converge on the core objectives of preventing unauthorised access, ensuring data integrity, and maintaining system availability. The review underscores that effective cybersecurity is not solely a technical issue but increasingly a human-centric

challenge, with social engineering attacks, such as phishing and exploiting psychological vulnerabilities.

The human factor is identified as one of the most significant and persistent vulnerability in cyberspace (Aigbefo et al., 2022). A well-established premise in cybersecurity is that human error, low cyber awareness, and behavioural tendencies contribute to the majority of security breaches (Alexei & Alexei, 2023). Psychological traits such as stress, fatigue, and cognitive biases make individuals susceptible to manipulation, particularly through phishing, vishing, smishing and whaling (Montañez et al., 2020). A knowledgeable and vigilant user base forms the first line of defence, yet gaps in cyber knowledge, especially among youngsters, remain as a critical issue (Bonsaksen, Kleppang, & Steigen, 2024; Meadows & Sambasivam, 2023).

In the Malaysian context, while the government has made strides through initiatives such as the Cyber Security Act 2024 and the National Cyber Security Policy (NCSP), cybercrime continues to surge. Malaysia ranks among the countries with the highest rates of cyber incidents in Southeast Asia. Public-private collaborations and educational programmes like CyberSAFE and MASSA indicate progress, but widespread engagement and tailored interventions are still lacking.

The review classifies cybersecurity knowledge into five domains: password security, software/system security, human security, organisational security and social security (See RQ1). Each domain highlights specific knowledge gaps, such as weak password habits, misunderstanding of basic protections like 2FA and antivirus software and a lack of policy awareness in organisational settings. The emerging field of social cybersecurity further reveals the risks of manipulation within digital communities.

To analyse cybersecurity behaviour, the Theory of Planned Behaviour (TPB) is adopted (RQ3). TPB posits that attitudes, subjective norms and perceived behavioural control

collectively shape intentions, which in turn influence behaviour. In cybersecurity, attitudes toward best practices, the influence of peers and confidence in executing safe behaviours are all critical predictors of whether individuals act securely online. Prior studies show that interventions targeting these factors whether through education, gamification and simulation may significantly improve cyber hygiene, although many fail to address youngsters-specific needs.

This chapter has identified a critical research gap: the absence of an understanding that connects specific cybersecurity knowledge areas directly to the actual behaviour of youngsters. It concludes that current approaches are insufficient without this link.

Furthermore, the chapter underscores the necessity for more targeted and effective cybersecurity strategy. It explicitly calls for strategies that are designed around key demographic variables such as age, gender and educational background arguing that these factors are not merely incidental but essential to developing impactful cybersecurity awareness programmes.

In summary, the core mandate moving forward is to reveal the nature of the gap between knowledge and intention behaviour while systematically accounting for demographic diversity. This establishes a direct foundation for the next chapter, which will propose and develop a strategy (or plan) to address these specific shortcomings.

CHAPTER 3 RESEARCH METHODOLOGY

This chapter outlines the methodological and procedural foundations that underpin the research. Grounded in a multimethod approach, it delineates how both quantitative and experimental strategies were integrated to investigate the gap between cybersecurity knowledge intention and behaviour among Malaysian youngsters. The methodology was informed by a pragmatist epistemology, which afforded flexibility in the selection of tools and strategies appropriate for addressing the complexity of the research questions.

The chapter is structured as follows. Section 3.1 presents the research design and the rationale underpinning its selection. Section 3.2 provides a detailed account of the sampling strategy, instrument development and data collection procedures implemented across the two sequential phases of the study (see Figure 20).

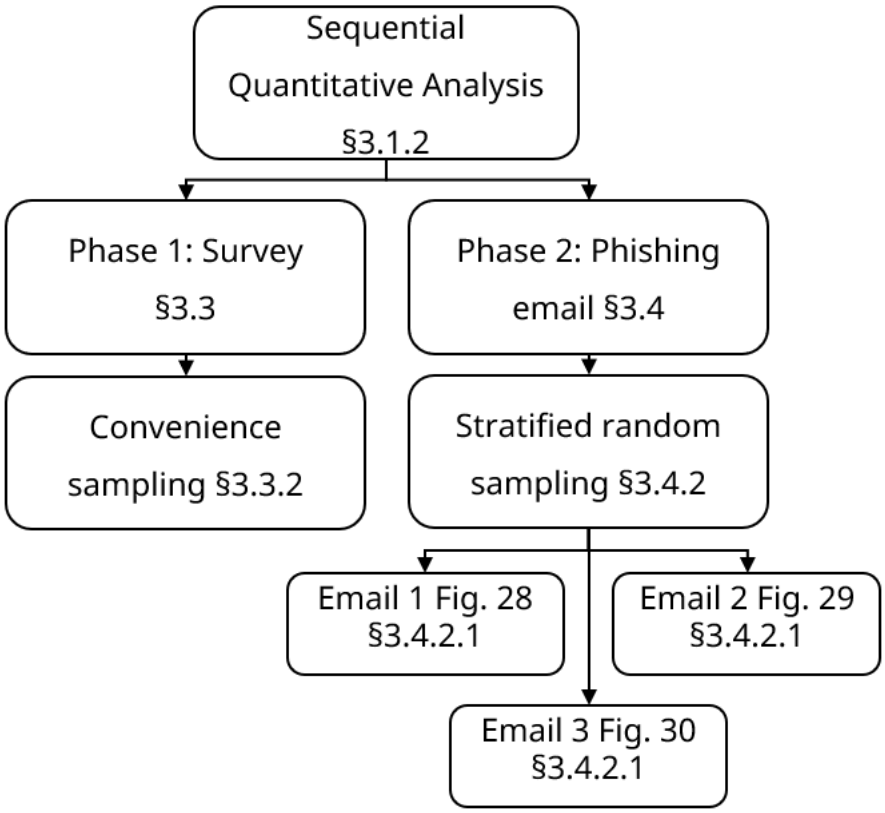


Figure 20: Proposed Research Design

Ethical considerations and adherence to institutional research governance frameworks were also comprehensively addressed to ensure conformity with established academic standards in section 3.2. Section 3.3 describes Phase 1, a structured survey employing convenience sampling to examine cybersecurity knowledge domains and their association with demographic variables. Section 3.4 details Phase 2, a controlled phishing simulation designed to capture actual behavioural responses. The inclusion of pilot studies in both phases enhanced the validity and reliability of the research instruments and procedures. Finally, Section 3.5 provides a summary of the research methodology.

3.1. Selection Strategy

Sampling methods are important in research because they allow researchers to draw conclusions about a larger population based on a smaller sample. By selecting a representative sample, researchers can make inferences about the characteristics of the larger population with greater accuracy and efficiency (Creswell, 2018).

There are two sorts of sampling methods: probability and non-probability. Based on Babbie (2008), when the goal is to obtain a sample that is representative of the wider population and to estimate population parameters with a particular degree of precision, probability sampling should be used. Non-probability sampling, on the other hand, is implemented when the research phenomenon is exploratory, the population is difficult to reach, or other practical constraints make probability sampling impossible or impractical. However, an extended explanation of probability and non-probability sampling can be seen below.

3.1.1. Sampling Design

Sampling methods fall into two categories: probability and non-probability, each with significant epistemological implications for generalisability and bias, and to mitigate singular-method limitations (Brewer & Hunter, 2006)

The first category is probability sampling. It relies on randomness to achieve representativeness and comprises numerous systematic procedures. These methods encompass simple random sampling; where each element has an equal chance of selection, stratified sampling; which proportionally represents subgroups, systematic sampling; selection at fixed intervals, cluster sampling; drawing from predefined groups, and multi-stage sampling; which is hierarchical randomization (Cochran, 1977; Fink, 2002; Lewis-Beck, 2004). In contrast, a second category is a non-probability sampling, used when random selection is not practical to be used in the research, focusing instead on practical or theory-driven considerations. This approach includes convenience sampling; which relies on readily available participants, purposive sampling; targeting specific traits or criteria, quota sampling; ensuring demographic balance, and snowball sampling; where existing participants help recruit others through referrals (Chiew & Pieprzyk, 2010), albeit at the cost of statistical generalisability (Renaud, Searle, & Dupuis, 2021). It is more common in exploratory research which involve diverse demographics, for instance, in cybersecurity behaviour studies (Adebowale et al., 2021) where depth and logistical constraints supersede broad representativeness.

3.1.2. Choice of Sampling

A multi-method approach promises “more sociologically significant conclusions and greater opportunities for both verification and discovery”, (Brewer & Hunter, 1989).

Phase 1- Convenience Sampling

it is practical to employ convenience sampling to gather respondents since Malaysia’s geographically and demographically dispersed, thus selected to ensure feasibility while capturing heterogeneous perspectives in phase 1. In addition, we tried to maximise the sample size comprehensively, in order to balance statistical accuracy (Kumar, 2018), within limited time and expenditures (Schreuder, Gregoire, & Weyer, 2001). We inferred the use of this

approach based on our research objective and established practices in behavioural research (Ahmead, El Sharif, & Abuiram, 2024; Anderson & Agarwal, 2010; Dzidzah, Owusu Kwateng, & Asante, 2020; Jinyin et al., 2025; Rich, 2018).

Phase 2- Stratified Random Sampling

Stratified random sampling was then employed in phase 2 (Figure 20 pg.74). Respondents who consented and submitted a valid email address subsequently randomly assigned at a random in one of the three phishing email experiment as our strata criterion. The thematic content and structural composition of the emails were carefully standardised in technical design (see 3.4.3.1) to maintain uniformity across experimental conditions. Every participant had an equal probability of receiving Email 1, 2, or 3 (see Figure 28 pg. 97, Figure 29 pg. 98, and Figure 30 pg. 99) thereby supporting the validity of the experimental design. This sequential design practically balances both the generalisability and rigorous of the research, where strategic combination is a key strength in applied cybersecurity research.

3.2. Ethical Considerations

Prior to commencing the first phase of this research, which involved a survey (application ID: 1639, Appendix A), and the second phase, which involved a phishing simulation (application ID: 2249, Appendix B), ethical approval was obtained from the University of Strathclyde Computer and Science Department. This approval ensured that all study procedures adhered to the ethical guidelines and standards set forth by the department and the university, safeguarding the rights and well-being of the participants involved in both phases of the research.

An informed consent was obtained from participants through a comprehensive Participant Information Sheet (See Appendices **C** and **F**). This sheet detailed the purpose of the study, the procedures involved, the voluntary nature of participation, and the researchers'

contact information. Participants were also provided with a Consent Form, which reiterated the voluntary nature of participation, the option to withdraw at any time, and the measures taken to ensure confidentiality and anonymity. The form explicitly stated that the data collected would be used solely for research purposes and would be destroyed after the completion of the study. Additionally, it emphasised that any information recorded in the research would remain confidential, and no identifying information would be made publicly available.

3.3. PHASE 1: Survey

The primary purpose of this survey is to explore the link between cybersecurity knowledge and behavioural intention in Malaysian youngsters. Specifically, it seeks to determine not only what knowledge matters most (**RQ1: How do different cybersecurity knowledge domains (password, software/system, human, organisational, and social security) predict Malaysian Youngsters' self-reported cybersecurity behavioural intentions?**) but also how it influences intention, by analysing the mediating role of attitude, social pressure, and perceived control (**RQ2: To what extent do the Theory of Planned Behaviour constructs (Attitude, Surrounding Pressure, and Perceived Control**) mediate the relationship between cybersecurity knowledge domains and behavioural intentions among Malaysian youngsters?) (see Section 1.2).

3.3.1. Data Collection

Surveys are an indispensable tool for data collection based on its flexibility to support quantitative and qualitative data analysis (Dawson, 2017). The survey instruments were considered carefully to ensure all questions could be answered comprehensively. The wording was designed to be accessible to respondents of all socio-demographic backgrounds. Given that English is not the first language in Malaysia, to limit misinterpretation and enhance linguistic accessibility, the survey was not only made in English also translated into Bahasa

Malaysia and was professionally verified by a translator. Offering the survey in multiple languages was considered crucial for ensuring the inclusion of diverse respondents (Normand, Paternò, & Winckler, 2014). we designed the survey to be flexible, allowing individuals to complete it at their own convenience.

The complexity of questions was also considered. A funnel approach was used, starting with basic questions and progressing to more specific ones. This approach aimed to gradually increase the intensity of the questions and ensure a consistent and unbiased respondent experience. Finally, to incentivise participation, all survey participants were entered into a lucky draw for two online shopping vouchers of 100 Ringit Malaysia. Considering a minimum wage in Malaysia is 1,700 Ringgit Malaysia and taking a minimum number of working days in week of 98.08 based on Hun (2025), offering RM100 for a specific task is reasonable, as it represents less than half of one day's minimum wage for that week, and this were included in the ethical approval.

Participants aged 18 to 26 years, representing demographics such as age, gender, and education level, were invited to take part. This research focused on gathering data from young individuals across Malaysia, so we prioritised convenience to encourage participation from diverse backgrounds. To further enhance accessibility, we provided a direct link to the survey, enabling participants to begin immediately with a single click.

The survey was distributed strategically over five working days. We began by partnering with social media influencers from Malaysia who shared the survey link through their stories, which can be seen in Figure 21. We then disseminated the survey link through our own social media channels and other platforms, including targeted emails distributed through HR departments.

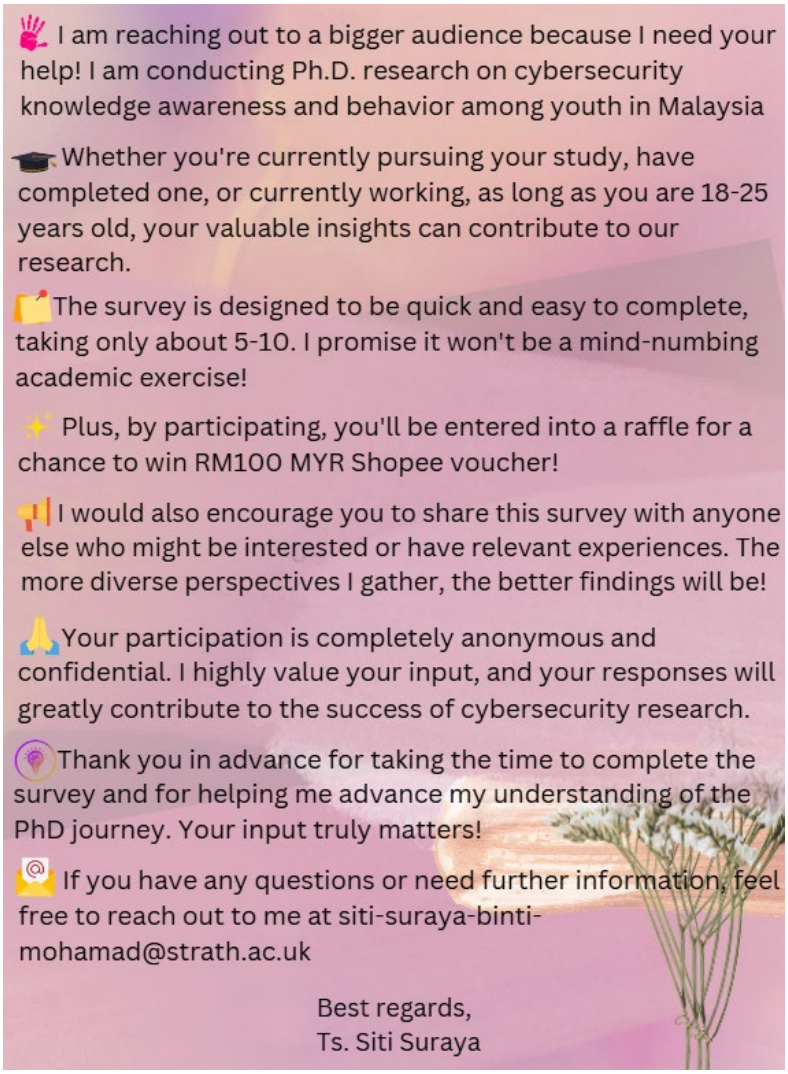


Figure 21 Social media post and story distribution

3.3.1.1. Development of Instruments

We reviewed previously conducted surveys on similar topics to identify established instruments and research designs (Rachad, 2012). This allowed us to adapt existing survey items with proven validity and reliability, minimizing the need for extensive modifications

Section A: In direct response to **Research Question 3 (RQ3)**, this research examined three demographic variables which is age, gender and level of education to analyse relationships to cyber knowledge and user behaviour. The demographics were included based on empirical evidence from previous research in section 2.7 indicating that user behaviour differed based on

these factors. Specifically, studies showed significant gaps in cyber behaviour among users (Howe et al., 2012; Redmiles, Kross, & Mazurek, 2016, 2017).

Section B: Likewise, to investigate cyber knowledge domain areas to youngsters, the survey was designed to address **Research Question 1 (RQ1)**. The structure and instruments for the survey questionnaire were adapted from established research and explained further in Section 3.3.3.1.

Section C: To understand youngsters' behaviour, we initiated instruments for cyber behaviour and compared these with the actual behaviour in our phase 2 of the study, to eliminate any disparities and support accuracy. The questionnaire was revised to ensure straightforward language, clear terminology, and the elimination of any prejudiced language to support the **Research Question 2 (RQ3)** and **Research Question 4 (RQ4)**.

Careful consideration was given to the arrangement and structure of questions to ensure clarity and understandability for all demographic groups while maintaining a professional tone. Clear headings and page breaks were used to guide respondents and indicate the intensity of the questions. A funnel approach was used (Fink, 2002), starting with basic demographic questions (e.g., age, gender, level of education) and progressing to more specific, cognitively demanding questions about cybersecurity knowledge and behaviours. The questionnaire transitioned smoothly between sections to prevent confusion, and basic graphics were incorporated to aid comprehension. Qualtrics XM was used to create a systematic and professional form and layout. Moreover, clear instructions were provided at the beginning to assist respondents.

Drafting and pilot testing the questionnaire before distribution were essential steps to ensure the reliability and validity of the instrument. Validity ensured the accurate measurement

of the intended variables, while reliability ensured consistent results upon repeated application under similar conditions (Rachad, 2012).

3.3.1.2. Pilot Study

Because this study employed convenience sampling to maximise the number of survey respondents, it was crucial to minimise potential inaccuracies after distribution. Pilot studies played a vital role in refining the survey methodology. They helped identify and address practical challenges, preventing errors, validating research instruments, and ensuring consistency across survey items (Bailar & Lanphier, 1978; Cranfield et al., 2021; Renaud, Zimmermann, et al., 2021; Srinivasan & Lohith, 2017; van Teijlingen et al., 2001).

While there is no strict rule on the number of pilot tests required, it is common practice to conduct at least two: an initial and a conclusive pilot test (Hunter & Brewer, 2006) and depends on factors such as its complexity, target audience, and available resources.

For this research, the survey instruments underwent multiple rounds of pilot testing. Feedback was gathered from a diverse group of individuals, including potential respondents within the target demographic, colleagues from the Chief Information Security Office (CISO) department at Maybank Ageas Holdings Berhad (Malaysia), PhD students at the University of Strathclyde's Computer and Information Science department, former colleagues from AirAsia X Berhad Malaysia, and thesis supervisor. Adjustment was made until the fifth round of pilot testing with an overall of 22 people tested, and feedback wes taken during the pilot testing.

3.3.1.3. Post Adjustment

The pilot study feedback proved an invaluable in refining the survey and adding essential elements. For example, at first, during the pilot testing, we acknowledged that feedback on Section A for email requirements highlighted the need to make it as required field (force response requirement) as shown in Figure 22). As it is vital for our second phase of the

research, we collected respondents who provided their accurate email address to deploy our Phase 2, and we replied based on email collected in our Phase 1. However, after our last pilot testing, we decided to remove the force response requirement because we especially wanted to maintain the voluntary nature of our respondents and ethical research practice, as well as to avoid survey abandonment from respondent frustration.

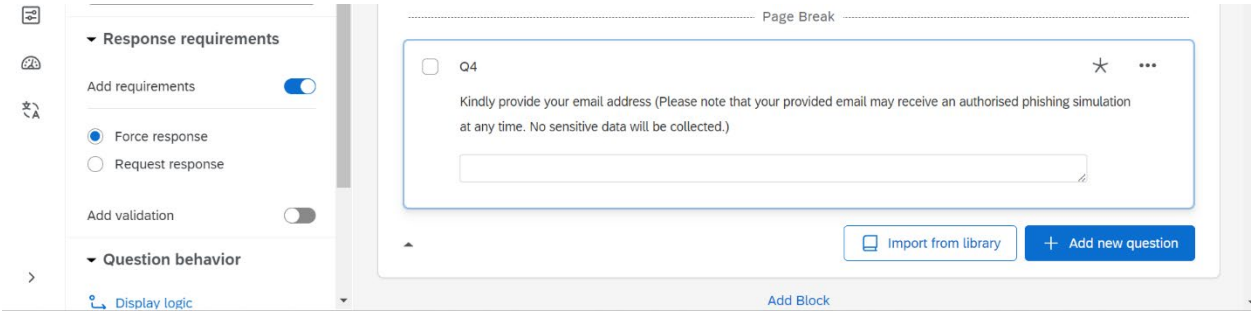


Figure 22: Qualtrics Force Response Requirement

The second feedback that we gathered from the pilot testing indicated the need for attention checks within the survey. To ensure high-quality data, it was essential to identify unreliable responses, such as those from participants who might not be fully engaged with the questions (Renaud & Ophoff, 2021). Therefore, we incorporated three factual attention checks throughout the questionnaire to encourage careful reading and accurate responses, see Table 3.

Table 3 Attention check response

Variable name	Label	Values: Level of Codes
Att1= Attention 1	If you're paying attention, click Sometimes	2= “Sometimes”
Att2= Attention 2	If you're paying attention, click Never	1= “Never”
Att3= Attention 3	If you're paying attention, click Disagree	2= “Disagree”

Our approach included incorporating an error statement for each attention check within the survey. Attention checks were included to see whether respondents have meaningfully engaged with the questions and accurately answered a given survey question (Beach, 1989). While attention check items were intentionally basic, they are widely used and validated in online survey research as a design called 'instructed response items' or 'instructional manipulation checks' (IMCs) (Shamon & Berning, 2020). They conducted a comprehensive study comparing different attention check formats and found that even simple instructed response items are effective for detecting inattentive respondents. Their meta-analysis showed that respondents who fail such checks produce significantly lower-quality data across all items, with higher rates of straight-lining (selecting the same response for all questions), shorter completion times, and inconsistent responses.

Gummer, Roßmann, and Silber (2021) further demonstrated that IMCs are particularly effective in online surveys where researchers cannot directly observe respondents' engagement. They recommend using multiple attention checks (three in this study) and retaining respondents who fail only one, while excluding those who fail two or more. This strategy balances data quality with sample retention.

Shamon & Berning (2020) validated this approach, showing that respondents who fail one attention check are often still attentive to other questions, whereas those who fail two or more are consistently inattentive. Therefore, this study's threshold (exclude if 2 or more checks are failed) follows established best practices, ensuring their valuable input contributed to the research findings, and respondents who overlooked two or more attention checks were excluded from the analysis (Table 3 and Figure 23).

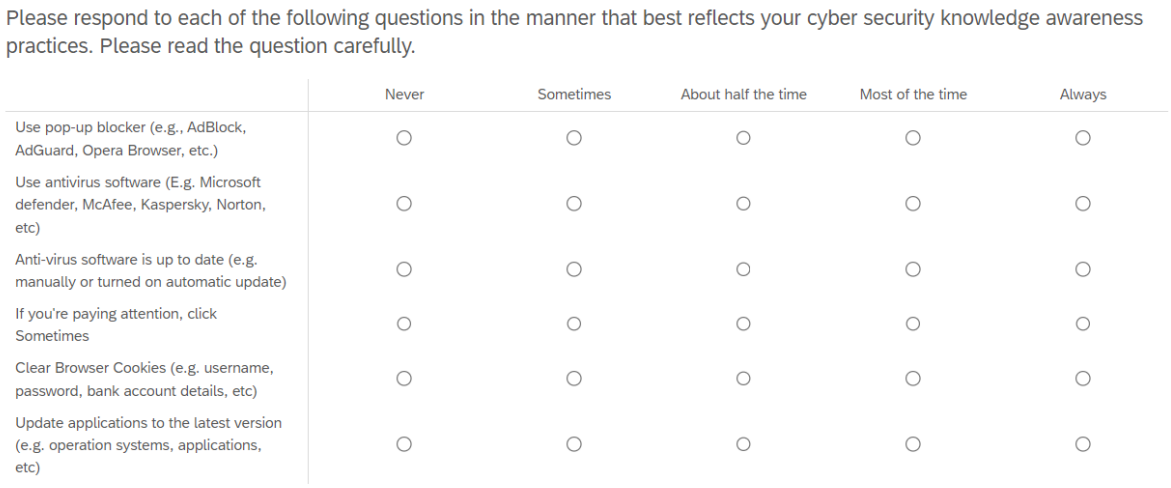


Figure 23: Attention response in the survey items using Qualtrics

Another feedback that we evaluated is that customised validation procedures initially filtered out individuals exceeding the age criteria for participation. However, based on pilot feedback, this validation error message was removed for future research that can be analysed (Figure 24). Despite this removal, responses from participants not meeting the age criteria were still excluded from our data analysis.

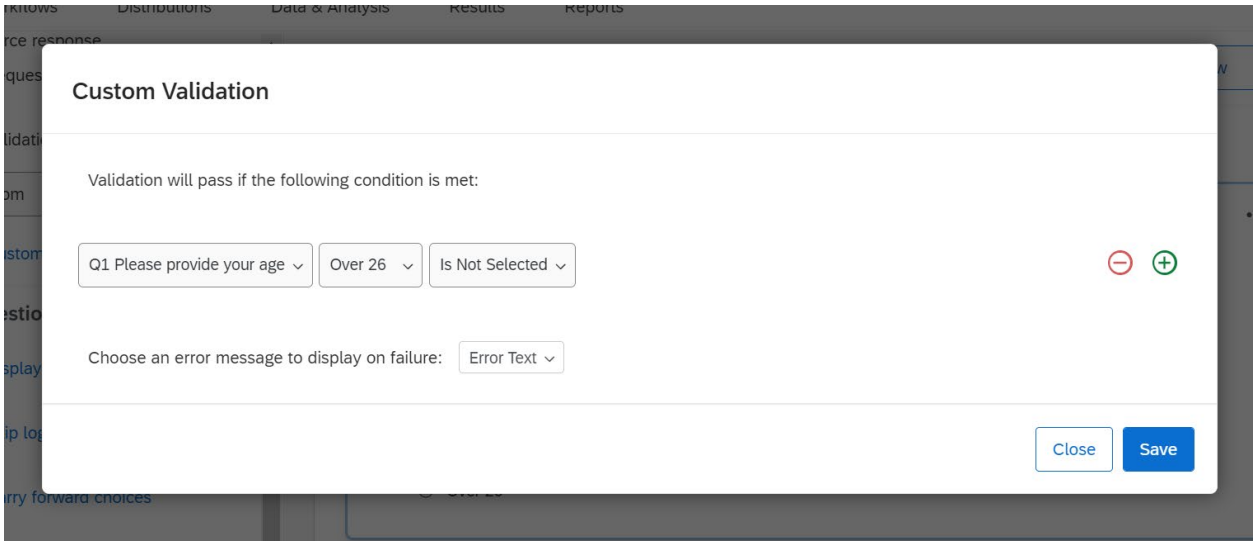


Figure 24: Custom Validation for Respondents

3.3.2. Cyber Knowledge Domain Items

To examine cyber knowledge domain areas, the survey was divided into sections, each targeting specific domain, such as password security (see Table 4), software/system security (see Table 5), human security (see Table 6), organisational security (see Table 7), and social security (see Table 8). The selection of these specific knowledges came from our empirical findings in our literature review, that researchers often overlooking the role of distinct and more focused knowledge domains in shaping cybersecurity awareness, generally addressed only on the general knowledge in cybersecurity without understanding the root cause from respondents.

Therefore, this lack of specificity presented as limitation in understanding how focused knowledge in particular domains may influence youngsters' cybersecurity. This can be seen from passive engagement in cybersecurity awareness and some deemed ineffective (Jarvie & Renaud, 2024; Kianpour, Kowalski, & Øverby, 2022; Venter et al., 2019; Vikas et al., 2025; Yulianto et al., 2025) and highlighted a notable gap in current literature and these cyber knowledge domain areas were chosen based on their fundamental theoretical and practical relevance.

Using established instruments with known psychometric properties reduces the risk of measurement error and allows for comparison with prior studies . All items were pilot tested (see Section 3.3.1.2) and adapted for the Malaysian youngster context, including translation into Bahasa Malaysia by a professional translator. Item wording was simplified where necessary to ensure accessibility for respondents with varying English proficiency levels

Table 4 Summary of Survey Instrument Sources

Instrument	Item Codes	Source	Number of Items
Password Security	PassSec1 – PassSec5	Adapted from Ion, Reeder, & Consolvo (2015) '*... No one can hack my mind*': Comparing Expert and Non-Expert Security Practices	5
Software/System Security	SoftSysSec1 – SoftSysSec5	Adapted from Ion, Reeder, & Consolvo (2015)	5
Human Security	HumSec1 – HumSec5	Adapted from Ion, Reeder, & Consolvo (2015)	5
Organisation Security	OrgSec1 – OrgSec5	Adapted from Ion, Reeder, & Consolvo (2015)	5
Password Combination Items	PassSec3	Additional items from Djukanovic et al. (2021) and Ng, Kankanhalli, & Xu (2009)	1 (embedded within PassSec1-5)
Social Security	SociSec1 – SociSec5	Developed based on CyberSecurity Malaysia guidelines (Abdullah, Mohamad, & Yunos, 2018)	5
Theory of Planned Behaviour Constructs (Attitude, Subjective Norms, Perceived Control, Intention)	YoungATT1-4, YoungSP1-4, YoungPC1-4, YoungCCI1-4	Adapted from van Steen & Deeleman (2021) '*Successful Gamification of Cybersecurity Training*'	16

3.3.2.1. Password security

The seminal work by Denning (1982) laid the foundation for understanding password security risks in computer systems, identifying threats such as unauthorised access, data leakage, and inference attacks. Existing research suggested that password security is widely regarded as the creation and management of passwords for online accounts and confidential data as well as enhancing the integrity of the password.

We acknowledge that the password standard guidelines has changed since 2017 from the National Institute of Standards and Technology (NIST), by promoting length and memorability over complexity such as in Table *5* for Code:PassSec3 which is “Use a

combination of uppercase and lowercase letters (e.g. aBc, ABC, or abc, etc), numbers (e.g., 123, etc), and special characters (e.g., !@+, etc) in your password". However, we implemented the item this way because we found that many people had never even heard of the update password guideline, hence, by first showing them the old guideline and also implementing the updated guideline, we don't just teach them what is new, we demonstrate why password security has improved, making the knowledge and behaviour integrated simultaneously.

Table 5 Password Security Items

Code	Item
PassSec1	Use two-factor authentication (e.g., 2-step verification, etc) for at least one of the online accounts.
PassSec2	Use password manager to keep track of all passwords (E.g., 1Password, LastPass, Dashlane, etc)
PassSec3	Use a combination of uppercase and lowercase letters (e.g. aBc, ABC, or abc, etc), numbers (e.g., 123, etc), and special characters (e.g., !@+, etc) in your password.
PassSec4	Use personal information (e.g., your name, last name, date of birth, etc) in your password.
PassSec5	Reveal confidential information (e.g. Identification Number (ID), credit card number, and CVV number, etc)

3.3.2.2. Software And System Security

The item in this section is to understand a youngster's knowledge in using software security for their electronic devices and internet usage security. We also included system security as part of understanding the overall secure internet infrastructure.

Table 6 Software and system security items

Code	**Item**
SoftSysSec1	Use pop-up blocker (e.g., AdBlock, AdGuard, Opera Browser, etc.)
SoftSysSec2	Use antivirus software (E.g. Microsoft defender, McAfee, Kaspersky, Norton, etc)
SoftSysSec3	Anti-virus software is up to date (e.g. manually or turned on automatic update)
SoftSysSec4	Clear Browser Cookies (e.g. username, password, bank account details, etc)
SoftSysSec5	Update applications to the latest version (e.g. operation systems, applications, etc)

3.3.2.3. Human Security

Meanwhile, the item in human security is employed to youngsters understanding of secure browsing and whether youngsters understand the vulnerabilities in internet browsing.

Table 7 Human security items

Code	*Item*
HumSec1	Visit websites you have not heard of
HumSec2	Check if the website you're visiting uses HTTPS
HumSec3	Enter password after clicking on a link in an email and that link take to a website
HumSec4	Open emails or attachments from unknown sources
HumSec5	Look at the URL bar to verify visiting the website

3.3.2.4. Organisation Security

To account for the professional context of participants within our target age groups, this study also incorporated measures to determine their exposure to organisational security practices. Specifically, items were included to ascertain whether respondents had received formal cybersecurity training or whether their employing organisations had implemented robust security protocols. This approach served two key purposes. First, it established a benchmark for organisational security knowledge among participants who were already in a workplace environment. Second, it provided a basis for analysing, in the study's second phase, whether such organisational factors influenced their security behaviours, such as their propensity to uphold or inadvertently violate security protocols. This was a necessary consideration, as the sampling strategy aimed for inclusivity within the demographic factor, which included individuals who had entered the workforce after high school or had completed higher education, rather than being exclusively enrolled in formal education.

Table 8 Organisation security items

Code	*Item*
OrgSec1	Work device(s) is monitored by administrator
OrgSec2	Organisation's Information Technology helpdesk sends out alert messages/emails concerning security
OrgSec3	Organisation constantly reminds to practice computer security
OrgSec4	Organisation distributes security newsletters or articles
OrgSec5	Organisation organises security talks

3.3.2.5. Social Security

As we already know and had been justified in the literature review, Malaysia also governed initiatives for cybersecurity practices. Hence social security implementation is to assess the public's knowledge and information dissemination regarding awareness between youngster's. We used guidelines for cyber resilience based on Cybersecurity Malaysia (Abdullah, Mohamad, & Yunos, 2018) and developed this instruments.

Table 9 Social security items

Code	*Item*
SociSec1	Have ever encountered any cyber-attack(s)? (e.g. Phishing attack, malware and virus attack, ransomware attack, etc.)
SociSec2	Exposed to cyber security practices through government initiatives (e.g. Cyber Security and Awareness for Everyone (CyberSAFE), national cyber exercise in Malaysia, etc.)
SociSec3	Exposed to cyber security knowledge through past education (e.g. high school, universities, etc.)
SociSec4	Exposed to cyber security policy in Malaysia (e.g. Malaysia Cyber Security Strategy 2020-2024, National Cyber Security Policy in Malaysia, National Cyber Exercise in Malaysia, etc.)
SociSec5	Know how to report cybercrime (e.g. Cyber999, National Scam Response Centre (NSRC), Malaysian Communication and Multimedia Commission (MCMC), etc.)

3.3.2.6. Youngsters Cyber Behaviour

Whilst Whitty et al. (2015) found that knowledge alone is insufficient to deter harmful cyber behaviour, other scholars indicated that additional behavioural factor such as self-reported behaviour, controlled task behaviour, cognitive behaviour and others, must be put into consideration (Anwar et al., 2015; Gainsbury et al., 2014; Hill et al., 2010). Hence, Table 10 utilises the Theory of Planned Behaviour (TPB) to contribute to youngsters' adoption of safe online practices with their behaviour and how youngsters make decisions regarding their online

safety with the cyber knowledge areas were implemented. Eight items for this section were adapted from van Steen & Deeleman (2021).

Table 10 Measurement items for Behaviour using the TPB Components

Component	Item
Attitude	It is important to at all times to adhere to cybersecurity knowledge awareness To me, cyber security knowledge awareness practices will affect cyber behaviour It is important to always behave accordingly in cyberspace To me, I behave differently if I have cyber security knowledge awareness
Subjective Norms	Most people around me obey to cybersecurity knowledge awareness My family and friends think that cyber security knowledge awareness will affect cyber behaviour Most people around me think that it is important to behave accordingly in cyberspace My surrounding think that I behave differently if I have cyber security knowledge awareness
Perceived behavioural Control	I find it easy to ensure that I always comply with the cybersecurity knowledge awareness Following cyber security knowledge awareness affecting my cyber behaviour I find it easy to ensure I behave accordingly in cyberspace I find it easy to behave differently if I have cyber security knowledge
Intentions	I plan to always comply to cybersecurity knowledge awareness

	I expect to follow cyber security knowledge awareness for my cyber behaviour I plan to always behave accordingly in cyberspace I expect to behave differently if I have cyber security knowledge

3.3.2.7. Additional comment

To complement the quantitative data and provide richer contextual insights, the survey concluded with an optional, open-ended question. Greene, Caracelli, and Graham (1989) stated that this can serve as a complementary function. The primary purpose was to elucidate, enhance, and illustrate the quantitative findings by capturing youngsters' own voices, nuanced explanations, and unanticipated perspectives on cybersecurity. The textual data from this open-ended question were analysed using a hybrid approach to thematic analysis (Byrne, 2022), which combined the use of NVivo software recommended by Braun & Clarke (2006) for initial coding and management, followed by a structured analytical process performed in Microsoft Excel to ensure rigour and transparency, as shown in Table 31 p133.

All qualitative responses were imported into NVivo 14 to facilitate the first two phases of analysis: familiarisation and initial coding. During the coding phase, a systematic, data-driven process was employed to generate concise labels capturing key concepts. To enhance analytical thoroughness and provide a clear audit trail, the coded data was subsequently exported into Microsoft Excel for theme development and refinement (Robinson, 2022). Within Excel, each code and its associated text excerpts were organised in a tabular format, enabling a granular, side-by-side comparison of all instances across participants.

The final set of themes provided a structured, rich description of the qualitative data, which was integrated with the quantitative results to offer a triangulated, comprehensive understanding of the cybersecurity knowledge-intention-behaviour gap.

3.4. PHASE 2: Phishing Simulation Method

Building on the survey of intentions, Phase 2 implements a phishing simulation to gather actual behavioural data. This phase directly compares intention with action, specifically asking: which factors predict real failure (**RQ3: How do demographic factors (gender, age, education level) and cybersecurity knowledge domains influence actual cybersecurity behaviour, as measured by susceptibility to phishing simulations**?), and how significant is the 'intention-behaviour gap in the cybersecurity context (**RQ4: What discrepancies exist between Malaysian youngsters' self-reported cybersecurity intentions and their actual behaviour when faced with a simulated phishing attack**)? (see Section 1.2).

3.4.1. Participants And Sampling

We invited participants to continue their involvement in this second phase of the research, to which they had given their consent by giving their email address in the initial survey. Randomization of participants to experimental conditions was achieved using Microsoft Excel. The RANDBETWEEN(1, 3) function was employed to generate a random sequence of numbers, where 1 corresponded to Experiment 1, 2 to Experiment 2, and 3 to Experiment 3. We deployed three experiments considering the practicality of a controlled and staged manner. We understand the ethical monitoring and avoided large-scale risky deployment.

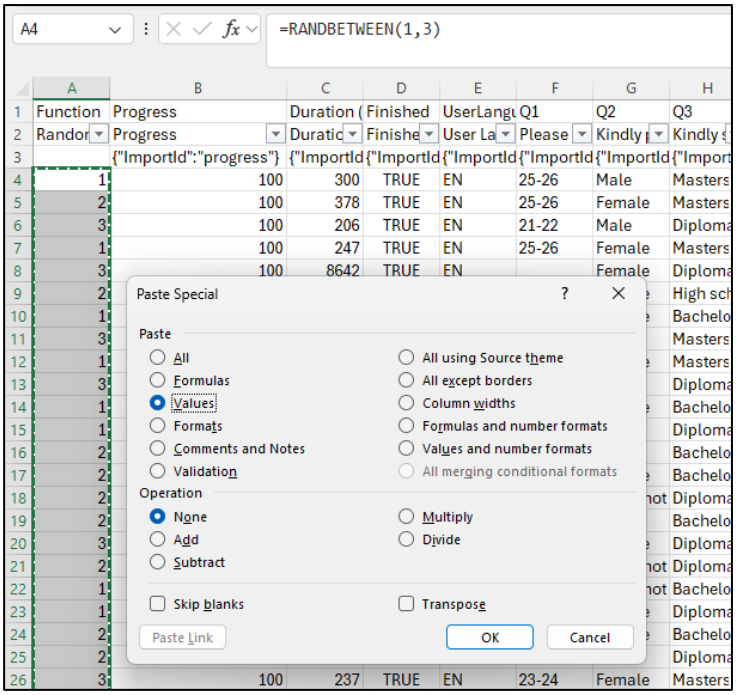


Figure 25: Randomisation of Participants to Experimental Function Condition

In addition, this method ensures an equal probability of each participant being assigned to any of the three experimental conditions. Figure 25 shows the same cells after the random numbers were 'frozen' by pasting them as values, ensuring that the randomisation scheme remained constant throughout the study.

3.4.2. Phishing Simulation Design

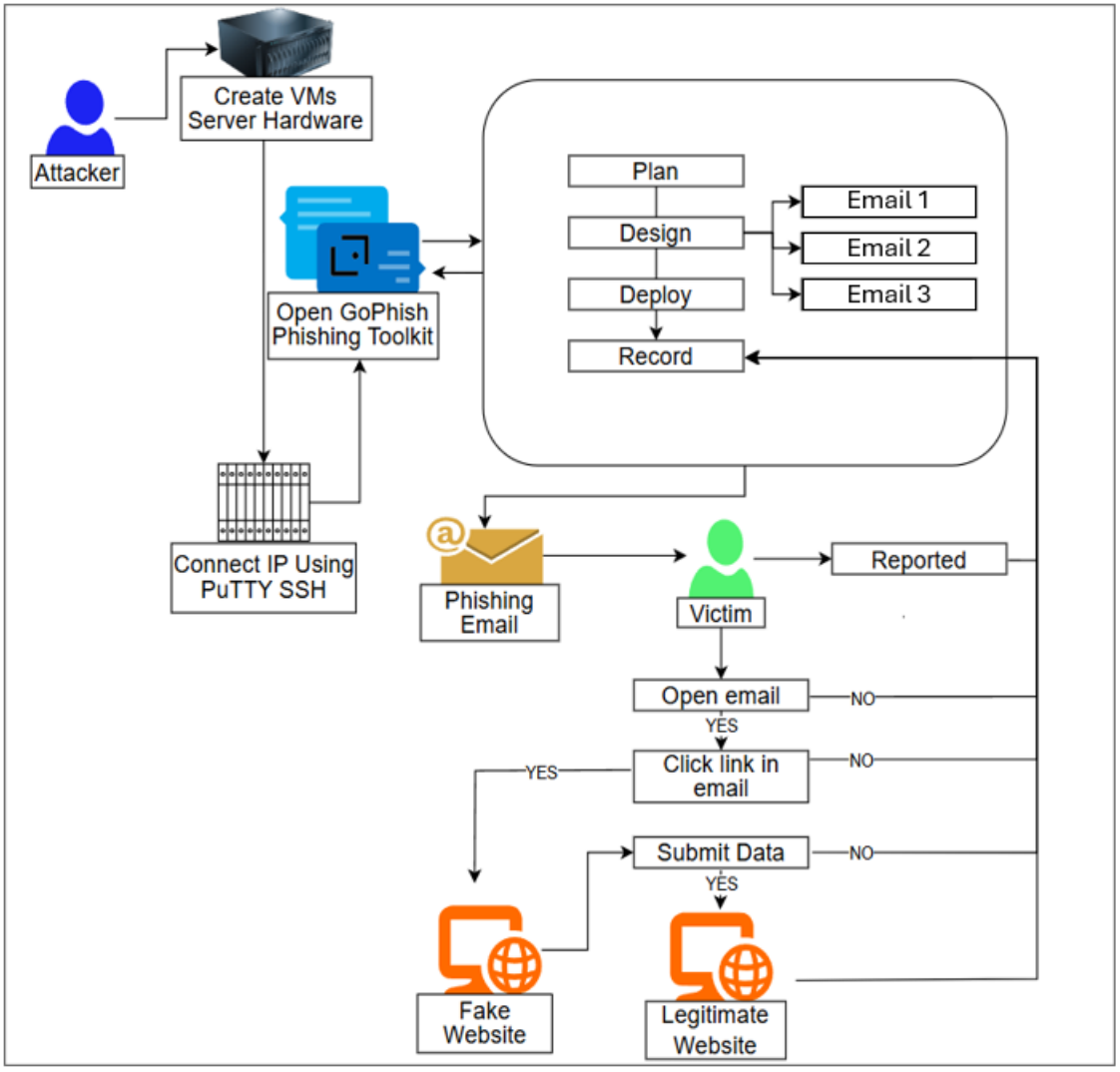


Figure 26: Phishing campaign simulation flow diagram

Figure 26 depicted our systematic phishing campaign simulation workflow. We first initiated the process by establishing the necessary infrastructure, which included creating virtual machines on server hardware to create the IP address, then connected using a PuTTY SSH terminal, enabling remote access and control. We utilised the GoPhish phishing toolkit, which facilitated the design, deployment, and recording of phishing campaigns.

3.4.2.1. Phish Simulation Campaigns

The primary objective of this simulation was to observe and analyse participant actual behaviour in response to a phishing email in regard to their cyber knowledge areas. Key metrics included email opening rates, which provided insights into the effectiveness of the email subject lines in capturing participant attention. Additionally, link click-through rates were monitored to gauge the persuasiveness of the email content in enticing participants to interact with the embedded links. Finally, the study tracked the submission of personal information to the simulated phishing websites, providing a crucial measure of the emails' overall effectiveness in deceiving participants.

This study employed a sophisticated phishing simulation campaign, incorporating three distinct email designs, as illustrated in Figure 27, Figure 28 and Figure 29. These variations aimed to assess the effectiveness of different visual and textual cues in eliciting participant interaction. while there was no actual concept of a universally optimal “prime time” for phishing attacks, we initially considered factors such as target audience: When are they most likely to be online and checking emails? This could be during work hours, lunch breaks, or evenings.

With research from Hoheisel et al. (2023) and Hendrik (2018) where the phishers exploited people when they are busy or distracted to consider the best time to deploy phishing simulation campaign. Corresponding to periods when youngsters are more likely to be engaged in study-work-related activities and thus more susceptible to phishing attempts. The emails were strategically disseminated at 9:00 AM and 6:00 PM local time (Malaysia) and during weekdays. This timing aimed to maximise the potential for participant interaction with the emails, providing a more accurate reflection of real-world phishing scenarios.

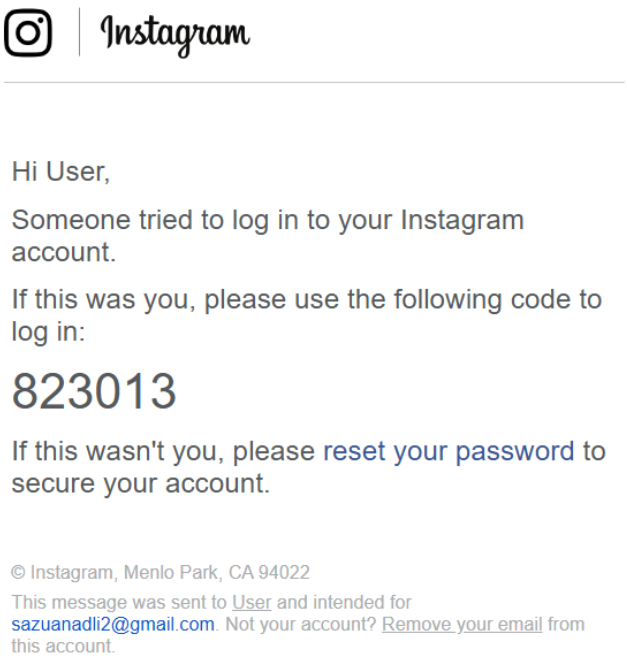


Figure 27: Phishing Simulation Campaign 1

The first phishing simulation designed to mimic an Instagram security alert. This email was utilised in the first phishing simulation campaign. Since most of youngsters in Malaysia used Instagram, this campaign co-opted panic and urgency. Youngsters, whose lives are centred on social media, may demonstrate naivety with respect to differentiating between legitimate and fake emails. We tested this potential naivety with our experiments.

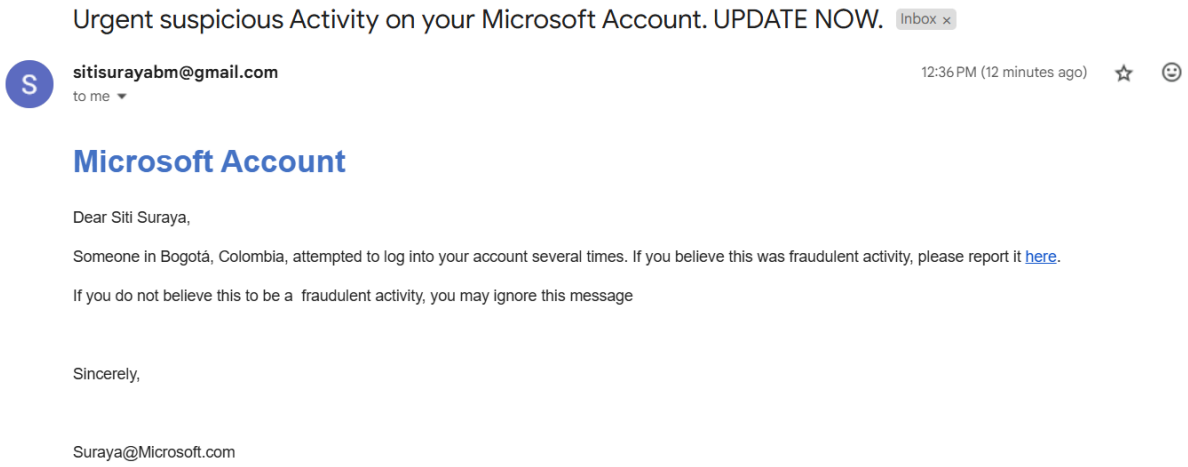


Figure 28: Phishing Simulation Campaign 2

This phishing simulation campaign is strategically designed to investigate the correlation between demographic factors, specifically an individual's level of education and their status (such as being a student or employed), and their susceptibility to phishing attacks. The research objective is grounded in academic literature, as it draws upon the work of Donalds & Osei-Bryson (2020), positioning the campaign within a broader scholarly context that seeks to understand how these variables influence cybersecurity knowledge and behaviour. The phishing email itself was meticulously constructed with a set of specific, measurable cues that served a practical test of the recipient's vigilance, which will be detailed in the next section. Furthermore, the email incorporated deliberate red flags, including an anomalous extra spacebar at the bottom, designed to test the recipient's attention to detail against the compelling urgency of the message.

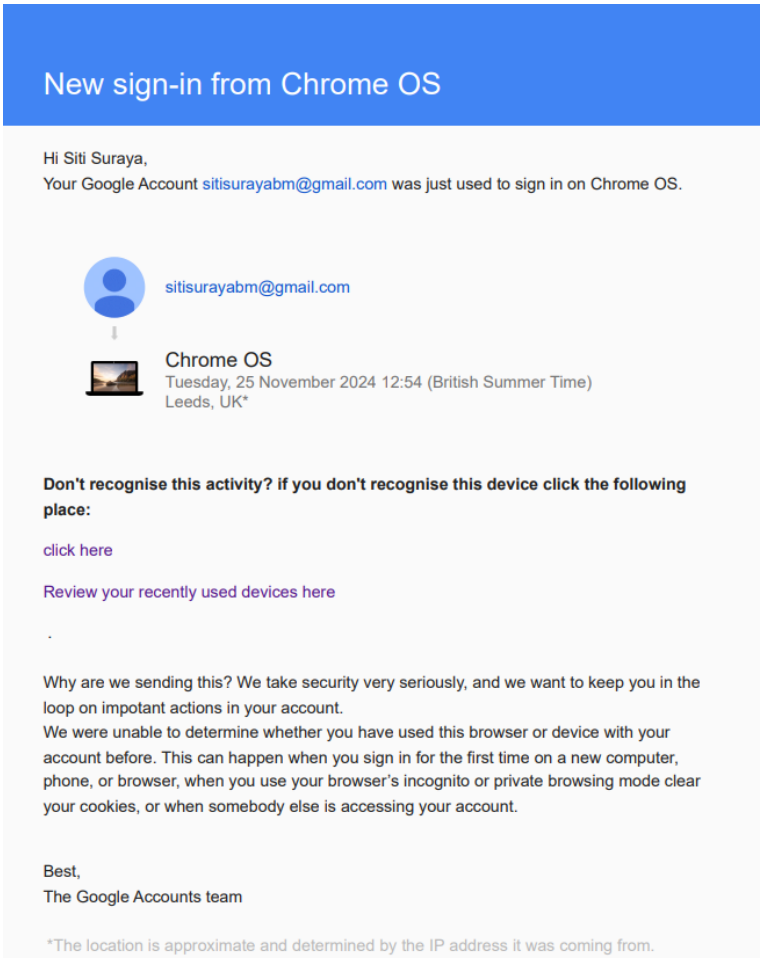


Figure 29: Phishing Simulation Campaign 3

This phishing attempt is more refined and less overtly aggressive with less noticeable phishing cues. It adopts a neutral tone and incorporates Google's branding and standard notification style to enhance credibility. This understated strategy may be more effective in deceiving recipients, particularly those less vigilant to common phishing indicators.

To facilitate this comprehensive analysis, the GoPhish platform was utilised for both the construction of the phishing emails and the subsequent collection and analysis of participant's data. This platform offered a robust and versatile framework for conducting the phishing simulation, enabling precise control over email content, delivery timing, and data logging. The integrated analytic capabilities of GoPhish provided valuable insights into

participant behaviour, facilitating a comprehensive evaluation of the effectiveness of the different email designs and dissemination strategies.

To ensure the reliability and validity of the findings, we make use of standardisation in our experiments, each of the phishing experiments has cues utilised in the experiments with the intention to focus on participant behaviour within a controlled environment.

3.4.2.2. Phishing Email Cues

The existing literature on phishing susceptibility reveals a wide array of experimentation approaches and ways of measuring how people react to phishing emails (Parsons et al., 2016; Williams & Polage, 2019), from live phishing simulation without any training (Xu & Rajivan, 2023), to phishing training before simulation (Steves, Greene, & Theofanos, 2020).

The absence of a consistent pattern in the deceptive cues employed in phishing email varies, thus, we employed cues based on the literature reviewed. The phishing email employed:

1. Urgency
2. Visual (logo, banners, etc.)
3. Language (grammatical errors, email personalisation)
4. 4. Technical (URL and HTTPS) factors.

These cues were included in all three phishing were carefully integrated into the email design based on the validity of the cues where respondents have successfully identified phishing emails (Carle & Ophoff, 2024; Köhler, Pünter, & Meinel, 2024), frequently utilised cues for detecting phishing signs (Jampen et al., 2020; Williams & Polage, 2019), and only used human judgement (Stuart et al., 2014). The examples of phishing email cues employed in the campaign can be seen in Figure 30 and Figure 31.

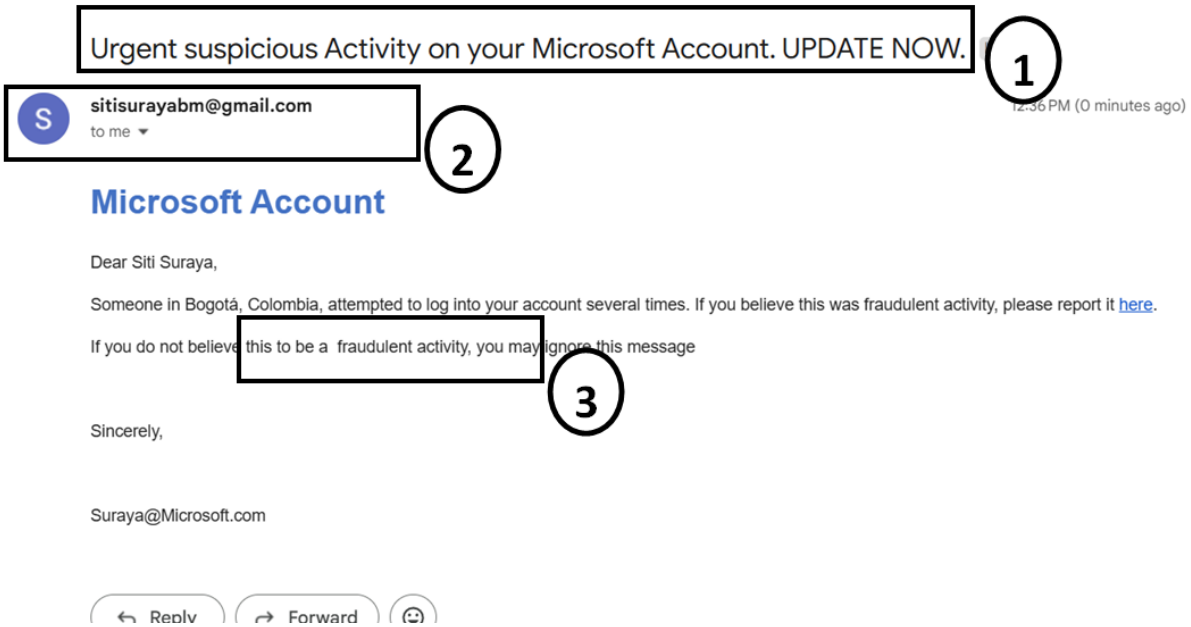


Figure 30: Visual, Language and Urgency Cues Dark Patterns

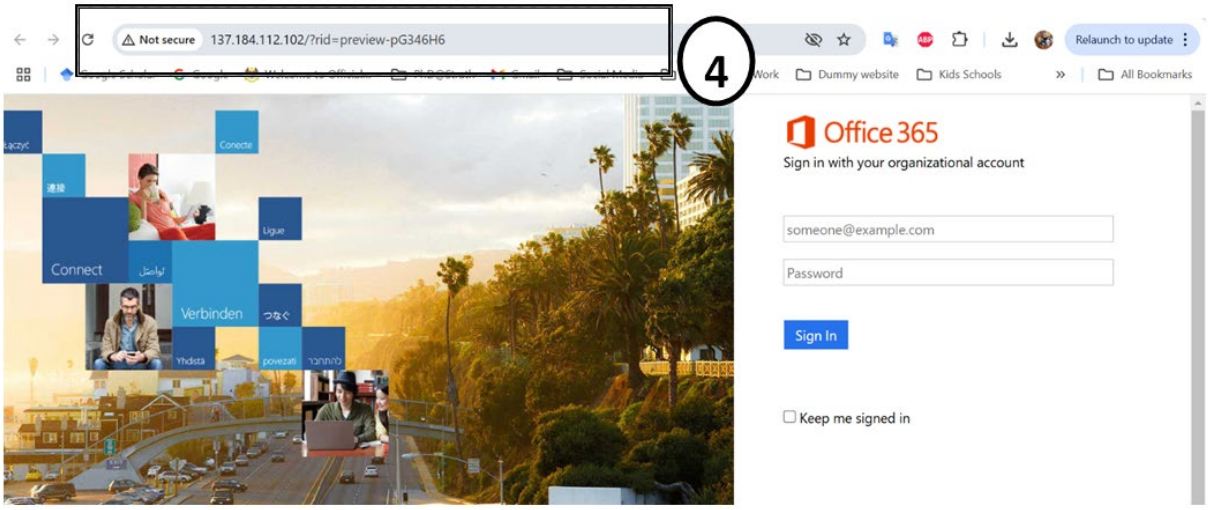


Figure 31: Technical Email Cues

3.4.2.3. Pilot Study

A pilot study was conducted with a small group of individuals to assess the functionality and design of the phishing emails. This focused on evaluating the technical aspects, such as the

embedded links, attached files, and tracking codes, to ensure their proper implementation. The pilot did not involve sending emails to actual study participants, as this could have inadvertently alerted them to the upcoming phishing simulation, potentially influencing their behaviour and compromising the integrity of the study's findings. While participants were informed during the initial survey phase that a phishing email would be part of the study, this pilot aimed to minimise any further hints or cues that could bias their responses.

3.4.3. Instrumentation and Data Analysis Methods

The data gathered from the phishing campaign simulation was analysed using a quantitative approach. Participant interactions with the phishing emails and landing page, was exported from the GoPhish platform into Microsoft Excel for initial organisation and cleaning. Variables within the Excel dataset were carefully labelled to maintain clarity and consistency throughout the analysis. We used IBM SPSS, SPSS SEM and other statistical analysis that explained above.

3.5. Summary

This chapter defined the methodological framework for the research, which was based on a multimethod approach to examine cybersecurity knowledge and behaviour among Malaysian youngsters. The research was conducted in two consecutive phases, informed by a pragmatic epistemology to guarantee adaptability and relevance in tackling the research enquiries.

A convenience sampling method was utilised to effectively collect a substantial and diverse sample from the geographically scattered target population. The survey instrument was carefully crafted, completing several rounds of pilot testing and professional translation into Bahasa Malaysia to guarantee clarity, validity, and accessibility. Ethical measures, such as

informed permission and data confidentiality, were rigorously followed, and attention-check questions were incorporated to ensure data quality.

During the second phase, a regulated phishing simulation was executed to transcend self-reported data and obtain genuine behavioural responses. Participants who provided consent in the initial phase were randomly allocated, employing a stratified random sampling technique, to one of three separate phishing email trials. These emails, crafted to replicate typical situations from platforms such as Instagram and Google, employed recognised deceptive indicators including urgency, graphic imitation, and technical subterfuge. The major purpose was to examine real-world interactions with these simulated threats, recording measures like email opening and link click-through rates.

Throughout all rounds, ethical approval was gained, and the strict procedural design ensured the study's trustworthiness. The strategic combination of a broad survey and a targeted experiment was highlighted as a key strength of the research, skilfully balancing generalisability with experimental rigor to provide a comprehensive knowledge of the complicated research subject, see appendices A and D.

CHAPTER 4 RESEARCH ANALYSIS

4.1. Introduction

This chapter discusses the findings obtained from two phases of quantitative data. The first phase involves the analysis of a hybrid survey completed by 765 participants, which included 48 closed-ended and one open-ended questionnaire. We report the outcome of the three phishing experiments, which participants from the first phase volunteered for.

The data analysis process followed a four-step guidance from Zainudin (2012), encompassing data mining as in Section 4.2, analysis for phase one in Section 4.3, analysis for phase 2o in Section 4.4 and analysis for the overall model in Section 4.5. Finally, this chapter summarises all findings based on the analysis and provides a discussion bridging the sequential quantitative data.

4.2. Data Preparation and Screening

The necessity of data cleaning prior to analysis has been emphasised by Hurley (2014), who outlines three primary justifications for this critical step. First, without proper data cleaning, analytical outcomes may lack reliability, compromising the validity of the study. Second, if inaccuracies persist within the dataset, they are likely to surface during analysis, leading to incorrect results or flawed assumptions rather than mere inefficiencies. Third, maintaining data integrity reflects respect for the contributions of study participants, ensuring their input is accurately represented.

Huxley (2020) further elaborates on practical methodologies for preliminary data inspection, including reviewing data inputs, assessing missing data, examining distribution patterns, and identifying anomalies such as outliers. Aligning with these recommendations, the

present study implemented four essential procedures to ensure error-free and precise analysis. Following this procedure, a refined dataset comprising 765 respondents was obtained.

4.2.1. Data Screening and Post Adjustment

The dataset was collected via Qualtrics and subsequently transferred to Microsoft Excel for initial cleaning, following Fink (2003) guidance before being imported into SPSS for statistical analysis. The following steps were undertaken:

4.2.1.1. Comprehensive Data Cleaning

To ensure the quality and reliability of the data for subsequent analysis, of the 991 initial responses received, 226 (22.8%) were excluded from the final analysis, resulted in a final dataset of 765 responses available for analysis. This involved a meticulous examination of each record to address inconsistencies arising from the collection process and to verify adherence to the study's inclusion criteria. A primary step in this process was the removal of incomplete survey responses (n = 168, 16.9%), respondents started the survey but did not complete all sections. These partial responses were excluded because missing data could not be assumed to be missing at random, and listwise deletion would have reduced statistical power for the Structural Equation Modelling (SEM) analysis, thereby focusing the analysis on fully answered and coherent datasets.. Following Fink (2003) a guidance on handling missing data, no statistical imputation was performed to ensure the analysis was based solely on the direct responses provided by participants, thereby maintaining the integrity of the original data. Furthermore, the absence of outliers was confirmed through the inclusion and analysis of attention response items within the survey instrument, this screening removed potential outliers arising from inattentive responding (n = 58, 5.8%). Respondents failed two or more of the three attention checks (Att1, Att2, Att3 in Table 3, p. 83). Following the recommendations of (Gummer et al., 2021), respondents who failed only one attention check were retained as they

demonstrated consistent focus, while those who failed two or more were excluded. detail discussed above in Table 3 and Figure 23 in page 83-84. Thus, the final dataset (N = 765) responses thus represent a completion rate of 77.2% among those who started the survey. This completion rate is consistent with typical online survey response rates reported in cybersecurity research (Cranfield et al., 2021; Renaud, Searle, et al., 2021). No statistical imputation was performed for missing data as the analysis is based solely on complete responses to maintain data integrity.

4.2.1.2. Identification and Rectification of Data Errors

The dataset was meticulously screened for inconsistencies arising during data collection. For instance, 21 entries containing invalid email addresses (e.g., respondents entering physical addresses instead of email credentials) were excluded, as they did not meet the study's data requirements.

4.2.2. Systematic Data Coding

Upon completing data cleaning, the dataset was systematically coded to facilitate analysis. Data coding involves assigning numerical or symbolic identifiers to questionnaire responses, thereby enhancing clarity and analytical efficiency (Fink, 2002). In this study, coding was integrated during the instrument design phase to streamline subsequent data processing. A detailed coding scheme is presented in Appendix I.

4.3. PHASE 1 ANALYSIS: Survey Data

4.3.1. Demographic Analysis

A key objective of the sampling design was to secure a demographically diverse respondent base. While the study's focus on a younger population inherently shaped the primary age distribution, we ensured significant variation within other demographic

parameters. The final sample is thus characterised by its diversity in gender and educational levels, affirming the inclusion of a heterogeneous group of participants.

4.3.1.1. Age

The largest percentage grouping of 28.0% (n=214) was for those aged 25–26 years, and the second largest was for 18-year-olds at 21.7% (n=166). The overall distribution offers a representative sample of the age groups, with 19–20 year olds comprising 18.7% (n=143), 21–22 year olds representing 14.4% (n=110), and 23–24 year olds accounting for 17.3% (n=132), as shown in Table 11 and Figure 32.

Table 11 Frequency distribution for age

		Frequency	Percent	Cumulative Percent
Valid	18-19	166	21.7	21.7
	20-21	143	18.7	40.4
	22-23	110	14.4	54.8
	24-25	132	17.3	72.0
	26>	214	28.0	100.0
	Total	765	100.0	

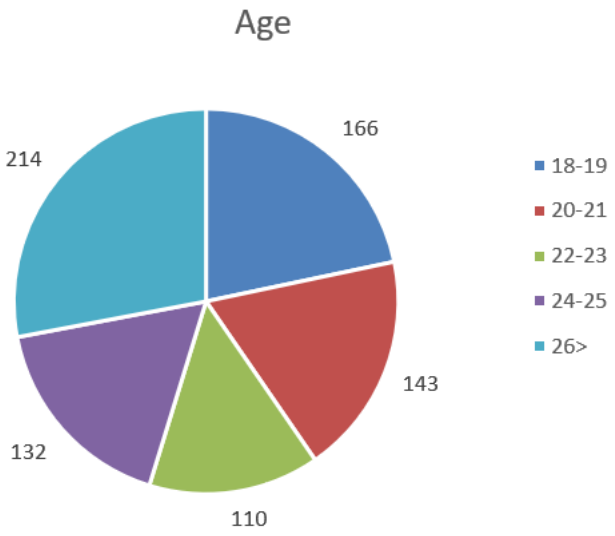


Figure 32 Age frequency

4.3.1.2. Gender

The sample of youngsters' cyber knowledge behaviour consisted of 484 (63.3%) female, 266 (34.8%) Male, and 15 (2.0%) preferred not to disclose their gender, (n=765). This is shown in Table 12 and Figure 33.

Table 12 Frequency distributions for gender

		Frequency	Percent	Cumulative Percent
Valid	Male	266	34.8	34.8
	Female	484	63.3	98.0
	Others	15	2.0	100.0
	Total	765	100.0	

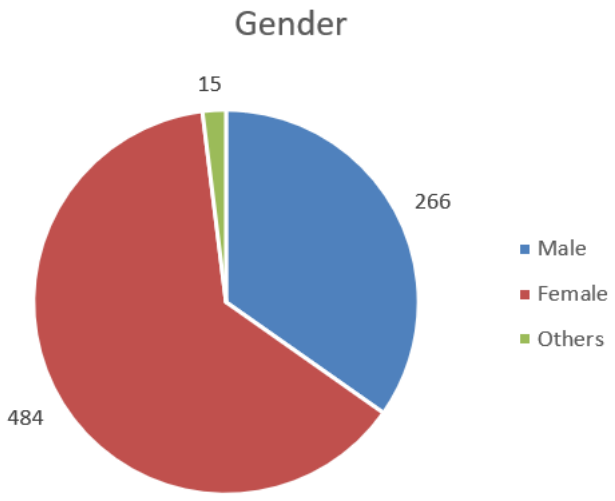


Figure 33 Gender frequency

4.3.1.3. Level of education

In terms of educational attainment, nearly half of the respondents held a bachelor's degree (46.5%, n=356). Those with a high school qualification constituted 22.0% (n=168) of the sample, while 21.2% (n=162) held a diploma. Postgraduate representation included those with a master's degree (9.2%, n=70) and a doctoral degree (1.2%, n=9), as shown in Table 13 and Figure 34.

Table 13 Frequency distribution for level of education

		Frequency	Percent	Cumulative Percent
Valid	High Sch	168	22	90.8
	Diploma	162	21.2	67.7
	Bachelor	356	46.5	46.5
	Master D	70	9.2	100
	Doctoral	9	1.2	68.9
	Total	765	100.0	

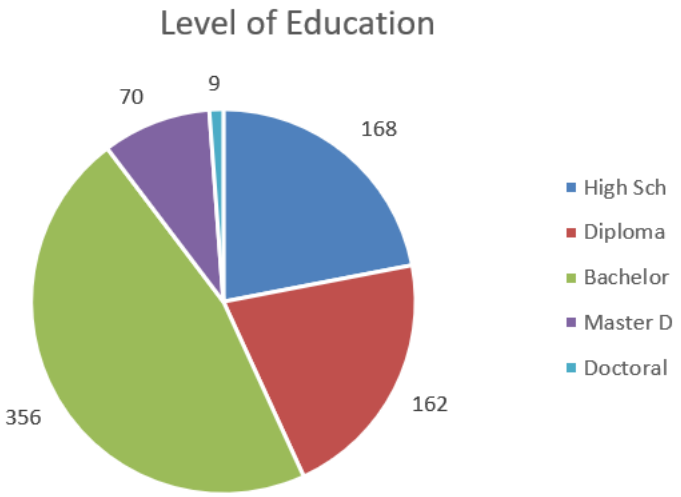


Figure 34 Level of education frequency

To understand the youngsters in Malaysia, we produced 5 × 3 cross-tabulation table for demographic differences (see Table 14). It revealed significant differences in level of education based on gender and age. Females considerably outnumbered males in higher education, particularly in older age groups. For instance, among individuals aged 25-26, 94 females hold bachelor's degrees compared to only 17 males. Conversely, younger males, ages 18-22, are more likely to have obtained high school qualifications, with 105 males versus 38 females in the 18-year-old group. There is a noticeable trend in educational attainment as individuals age: females tend to pursue higher degrees, be it for bachelor's and master's in their mid-20s, while males primarily complete basic education at younger ages.

However, any claims about gender differences must be tempered by the sample composition: the sample included 484 females (63.3%) and only 266 males (34.8%), which may overrepresent female perspectives and underrepresent male perspectives. Future research with a more balanced gender distribution (e.g., quota sampling) is needed to confirm whether these observed differences are statistically reliable or artefacts of sampling bias. The 'Prefer not to say' category (n = 15, 2.0%) is too small for meaningful subgroup analysis.

Table 14 Distribution of education levels by gender and age group (N=765)

		Male					Female					Others		
		Education_Group					Education_Group					Education_Group		
		High Sch	Diploma	Bachelor	Master D	Doctoral	High Sch	Diploma	Bachelor	Master D	Doctoral	Diploma	Bachelor	Master D
Age Group	18	105	7	0	0	0	38	13	3	0	0	0	0	0
	19-20	4	19	11	2	0	5	35	56	7	1	1	1	1
	21-22	1	6	19	2	1	1	16	55	5	0	2	2	0
	23-24	2	3	28	3	2	1	14	64	9	3	0	3	0
	25-26	5	17	17	12	0	6	29	94	27	2	0	3	2

4.3.2. Cybersecurity Knowledge and Behaviour Analysis

All constructs for cybersecurity knowledge were measured on a 5-point Likert scale, where 1 = “Never”, 2 = “Sometimes”, 3 = “About half the time”, 4 = “Most of the time” and 5 = “Always”, as seen in Table 24 p118. Descriptive statistics were calculated for all key constructs. The results indicate a mixed level of cybersecurity engagement among the respondents. Participants demonstrated moderate engagement with practices like using password managers (mean=3.34) but showed lower consistency in safeguarding sensitive information (mean=2.03) and avoiding personal details in passwords (mean=2.14). Overall, knowledge scores were moderate in areas like software/system security (mean=3.29) and low in human security (mean=2.27) and social security (mean=2.24).

Observation on Password Security Results (Table 15): It is notable that PassSec_4 ('Use personal information in your password') and PassSec_5 ('Reveal confidential information') have the lowest means (2.14 and 2.03, respectively), indicating that most respondents rarely or never engage in these insecure practices. This is expected and positive, as it suggests awareness of basic password hygiene. However, the moderate mean for PassSec_2 ('Use password manager') at 3.34 suggests room for improvement in adopting more advanced password management tools. This pattern as good awareness of basic rules but lower adoption of sophisticated tools, is consistent with prior research (Baraković & Baraković Husić, 2023).

4.3.2.1. Password security

Descriptive statistics for password security reveal an overall score of 2.8170 (*SD*=0.75687). This shows a negative perception of password security amongst youngsters (see Table 15). PassSec_2 *"Use password manager to keep track of all passwords (E.g., 1Password, LastPass, Dashlane, etc)"* had the highest mean value indicating that youngsters' implemented efficacy towards password manager.

Table 15 Password security construct

Items	N	Minimum	Maximum	Mean	Std. Deviation
PassSec_1	765	1	5	3.27	.786
PassSec_2	**765**	**1**	**5**	**3.34**	**.860**
PassSec_3	765	1	5	3.30	.843
PassSec_4	765	1	5	2.14	1.278
PassSec_5	765	1	5	2.03	1.256
PassSec	765	2.00	5.00	2.8170	.75687
Valid N (listwise)	765				

For the full list of Password Security items and their sources, see Section 3.3.2.1 (Table 5 pg. 87). The interpretation of Likert scale values (1 = Never to 5 = Always) is explained in Section 4.3.2.

4.3.2.2. Software/system security

SoftSysSec reveal an overall mean score of 3.2937 (*SD* = 0.90708) in Table 16. This shows that a positive attitude of software and system security amongst youngsters, with SoftSysSec_5 having the highest mean score of 3.84 *"Update applications to the latest version (e.g. operation systems, applications, etc)"*, indicating that youngsters always ensure that the application is updated to the latest version.

Table 16 Software/System security construct

Items	N	Minimum	Maximum	Mean	Std. Deviation
SoftSysSec_1	765	1	5	3.15	1.466
SoftSysSec_2	765	1	5	3.24	1.402
SoftSysSec_3	761	1	5	3.17	1.333
SoftSysSec_4	765	1	5	3.06	1.393
SoftSysSec_5	**765**	**1**	**5**	**3.84**	**1.079**
SoftSysSec	765	1.20	5.00	3.2937	.90708
Valid N (listwise)	765				

4.3.2.3. Human security

HumSec reveal (Table 17) an overall mean score of 2.2667 (*SD* = 0.77972). This indicates a relatively lower level of human security awareness among the youngsters, with HumSec_5 having the highest mean score of 2.82 *"Look at the URL bar to verify visiting the website",* suggesting that some aspects of human security are perceived with more attention, while relatively low level of cautiousness of "HumSec_5: Open emails or attachments from unknown" sources but still, there is a general room for improvement in the overall security practices among youngsters.

Table 17 Human security construct

Items	N	Minimum	Maximum	Mean	Std. Deviation
HumSec_1	765	1	5	2.30	1.137
HumSec_2	765	1	5	2.53	1.367
HumSec_3	765	1	5	1.89	1.033
HumSec_4	765	1	5	1.79	.966
HumSec_5	**765**	**1**	**5**	**2.82**	**1.280**
HumSec	765	1.00	5.00	2.2667	.77972
Valid N (listwise)	765				

4.3.2.4. Organisation security

The descriptive statistics for OrgSys (Table 18) items reveal an overall mean score of 2.6886 (*SD*= 0.80784), suggesting a negative level for organisation security among youngsters. OrgSys_3 received the highest mean score of 2.94 "*Organisation constantly reminds to practice computer security*", indicating that active awareness within organisations, while OrgSys_5 had the lowest mean score of 2.41, suggesting that the need of more security talk or trainings.

Table 18 Organisation security construct

Items	N	Minimum	Maximum	Mean	Std. Deviation
OrgSys_1	765	1	5	2.66	1.491
OrgSys_2	765	1	5	2.79	1.367
OrgSys_3	**765**	**1**	**5**	**2.94**	**1.327**
OrgSys_4	765	1	5	2.64	1.255
OrgSys_5	765	1	5	2.41	1.254
OrgSys	765	1	5	2.68	.8078
Valid N (listwise)	765				

4.3.2.5. Social security

Descriptive statistics for Social Security in Table 19 reveal an overall mean score of 2.2438 (*SD*= 0.87975), indicating negative perception of social security among the youngsters. Formal education "SociSec_3: *Exposed to cyber security knowledge through past education (e.g. high school, universities, etc.)*" is the most significant factor influencing cybersecurity social security with the mean score of 2.86, whereas government initiatives, policy knowledge, and cybercrime reporting mechanisms are less familiar to the youngsters.

Table 19 Social security construct

Items	N	Minimum	Maximum	Mean	Std. Deviation
SociSec_1	765	1	5	1.90	1.067
SociSec_2	765	1	5	2.19	1.203
SociSec_3	**765**	**1**	**5**	**2.86**	**1.338**
SociSec_4	765	1	5	2.09	1.226
SociSec_5	765	1	5	2.17	1.304
SociSec	765	1.00	5.00	2.2438	.87975
Valid N (listwise)	765				

4.3.2.6. Youngsters' Attitude

Descriptive statistics for YoungATT reveal an overall mean score of 6.1039 (*SD* = 1.02584). This shows a positive perception of YoungATT amongst youngsters. YoungATT_1 has the highest mean value, indicating that the youngsters showed a positive attitude towards adhering to cybersecurity knowledge, in Table 20.

Table 20 YoungATT construct

Items	N	Minimum	Maximum	Mean	Std. Deviation
YoungATT_1	765	1	7	6.26	1.148
YoungATT_2	765	1	7	6.04	1.188
YoungATT_3	765	1	7	6.19	1.093
YoungATT_4	765	1	7	5.93	1.293
YoungATT	765	1.00	7.00	6.1039	1.02584
Valid N (listwise)	765				

4.3.2.7. Youngsters' Surrounding Pressure

Surrounding pressure' refers to perceived social influence from important others, including family members, friends, peers, educators, and colleagues; to engage in cybersecurity-safe behaviours. This construct operationalises the 'Subjective Norms' component of the Theory of Planned Behaviour (see Section 2.6.2.1).

Youngsters perceive a moderate level of surrounding pressure, as indicated by the overall mean score of 4.9382 (*SD*= 1.17624) for YoungSP. Breaking this down further, the most significant factor, measuring item "YoungSP_2 "*My family and friends think that cyber security knowledge awareness will affect cyber behaviour*" has the highest mean score (5.18), underscoring the strong role of belief from youngsters' close relationship with surrounding people in shaping cybersecurity. In contrast, YoungSP_1 with item "*Most people around me obey to cybersecurity knowledge awareness*" shows the lowest mean (4.49), was intended to measure whether respondents perceive that their social circle follows cybersecurity best practices, suggesting that other surrounding factors exert relatively weaker influence (see Table 21).

Table 21 Youngsters' Surrounding Pressure (Subjective Norms) Construct

Items	N	Minimum	Maximum	Mean	Std. Deviation
YoungSP_1	765	1	7	4.49	1.537
YoungSP_2	765	1	7	5.18	1.447
YoungSP_3	765	1	7	5.20	1.340
YoungSP_4	765	1	7	4.89	1.534
YoungSP	765	1.00	7.00	4.9382	1.17624
Valid N (listwise)	765				

4.3.2.8. Youngsters' Perceived Control

Descriptive statistics for YoungPC reveal an overall mean score of 5.6095 (*SD* = 0.91688), indicating a relatively positive perception of perceived control among youngsters. YoungPC_2, which refers to "*Following cyber security knowledge awareness affecting my cyber behaviour*" has the highest mean score of 5.85, suggesting that youngsters feel they have the most control over their actions based on their knowledge related to cybersecurity. Conversely, YoungPC_1, "*I find it easy to ensure that I always comply with the cybersecurity knowledge awareness*" had the lowest mean score of 5.36, reflecting a slightly lower perception of control in some areas. Overall, the data suggests a moderate level of perceived control among youngsters over their cybersecurity behaviours (see Table 22).

Table 22 YoungPC construct

Items	N	Minimum	Maximum	Mean	Std. Deviation
YoungPC_1	765	1	7	5.36	1.237
YoungPC_2	765	1	7	5.85	1.149
YoungPC_3	765	1	7	5.58	1.132
YoungPC_4	765	1	7	5.65	1.234
YoungPC	765	1.00	7.00	5.6095	.91688
Valid N (listwise)	765				

4.3.2.9. Youngsters' Cyber Cautiousness Intention

Descriptive statistics for YoungCCI reveal an overall mean score of 5.6095 (*SD*=0.91688), indicating that youngsters generally perceive themselves to have a moderate level of control over their cybersecurity actions (Table 23). Among the items, YoungCCI_5 received the highest mean score of 5.93 "*I expect to behave differently if I have cyber security knowledge*". Conversely, YoungCCI_1 had the lowest mean score of 5.79 "*I plan to always comply to cybersecurity knowledge awareness*", indicating that some areas of perceived control

might need further attention. Overall, the data shows that youngsters have a relatively strong sense of control, but there are variations across different aspects of cybersecurity.

Table 23 YoungCCI construct

Items	N	Minimum	Maximum	Mean	Std. Deviation
YoungCCI_1	765	1	7	5.79	1.154
YoungCCI_2	765	1	7	5.85	1.082
YoungCCI_4	765	1	7	5.90	1.086
YoungCCI_5	765	1	7	5.93	1.103
YoungCCI	765	1.25	7.00	5.8667	.94101
Valid N (listwise)	765				

4.3.3. Instrument validity: Reliability and Validity of the Survey Instrument

4.3.3.1. Reliability Analysis

Cronbach alpha (α) is used to construct a validation score to test the credibility of the analysis (Cronbach, 1951). While alternative metrics for assessing reliability exist, such as coefficient H (McNeish, 2018), Cronbach's alpha remains the predominant instrument within psychological and behavioural research, justifying its application in this study. The score for Cronbach's alpha is calculated by formula:

$$\alpha = \frac{k}{k-1}\left(1 - \frac{\sum s_i^2}{s_X^2}\right)$$

The need of Cronbach alpha in survey and construct validation is fundamentally axiomatic, function as necessary, to warrant the credibility of a construct into a composite score for subsequent analysis. This study employed Cronbach's alpha to verify that the items within each construct (e.g., the five Password Security items) consistently measured their intended construct before aggregating them into composite scores for subsequent analysis (EFA, CFA, SEM). While alternative metrics exist (e.g., coefficient H, omega), Cronbach's alpha remains the most widely reported reliability statistic in behavioural research, facilitating comparison

with prior studies. Scholars have varying perspectives on acceptable thresholds score for Cronbach's alpha. Hair (2009, p. 14) suggest a minimum reliability coefficient of 0.7 as the standard cutoff value as in Table 24, however Straub, Boudreau, and Gefen (2004) suggested that the minimum acceptable value is set at .60 for exploratory research and .70 for confirmatory research, though Bujang, Omar, and Baharum (2018) argues that a lower alpha value of 0.5 may still be acceptable, particularly when dealing with a small number of items in the scale.

Table 24 Cronbach's interpretation values to five-point Likert scale

Response	**Score**	**Cronbach's Alpha**	**Interpretation**
Always	5	>=0.90	Excellent
Most of the time	4	0.80-0.89	Good
About half the time	3	0.70-0.79	Acceptable
Sometimes	2	0.60-0.69	Questionable
Never	1	0.50-0.59	Poor
		<0.50	Unacceptable

The thesis used Cronbach's alpha to assess the internal consistency reliability of the multi-item scales measuring each cybersecurity construct (password security, software/system security, human security, organisational security, social security, and the Theory of Planned Behaviour components: attitude, subjective norms, perceived behavioural control, and intention). It is used appropriately based on Barbera et al. (2021) recommendations, as it was employed appropriately for single-administration internal consistency. Common misinterpretations were avoided; it did not claim equivalence across different test forms nor make assertions regarding item difficulty. Transparent justification for the selected thresholds was provided, and the relevance of the statistic for establishing the reliability of the multi-item constructs was clearly explained prior to their aggregation and subsequent analysis using EFA, CFA, and SEM.

Table 25 indicated all constructs complied with the reliability measurement, therefore, all variables are accepted for further analysis.

Table 25 Reliability analysis for each variable

Variables	Cronbach's Alpha	N of Items
Password security	.78	5
Software/system security	.70	5
Human security	.69	5
Organisation Security	.84	4
Social security	.76	5
Youngsters' attitude	.89	4
Youngsters' subjective norms	.81	4
Youngsters perceived control	.77	4
Youngsters' cyber intention	.87	4
Youngsters' behaviour	.63	13

4.3.3.2. Construct Validity (Factor Analysis)

After assessing the reliability of the variables, we then employed exploratory factor analysis (EFA) to evaluate their validity and uni-dimensionality. In addition to EFA, validity can also be examined through confirmatory factor analysis (CFA), which provides measures of convergent validity and discriminant validity.

4.3.3.2.1. Exploratory Factor analysis (EFA)

Exploratory Factor Analysis (EFA) is a statistical technique used to identify the underlying structure among a set of observed variables. EFA answers the question, for instance "Do these survey items group together into meaningful clusters (factors)?". Unlike Confirmatory Factor Analysis (CFA), which tests a pre-specified structure (Thompson, 2004), EFA is data-driven and does not impose a predetermined pattern (Gorsuch, 1997). EFA allows researchers to explore how variables interrelate and to identify whether they can be grouped into broader latent constructs, known as factors (Pett, Lackey, & Sullivan, 2003).

For this research, EFA was performed using principal axis factoring (PAF) with varimax rotation in SPSS version 29. The minimum factor loading criterion was set to 0.50, meaning that only items with a loading of 0.50 or higher on a given factor were considered to have a meaningful relationship with that factor. Several key statistical concepts are essential for understanding the EFA results.

First, a factor loading refers to the correlation between an observed item (e.g., a survey question) and its underlying factor, with loadings ranging from -1 to +1. A loading of 0.50 or above indicates that the item shares at least 25% of its variance ($0.50^2 = 0.25$) with the factor.

Second, communality represents the proportion of variance in an observed variable that is explained by all extracted factors combined, with values ranging from 0 to 1 (Yong & Pearce, 2013). In this study, communality values below 0.50 were considered insufficient, indicating that the factors did not adequately explain the item's variance.

Third, cross-loading occurs when an item shows significant factor loadings (≥0.50) on two or more factors simultaneously, indicating that the item does not clearly represent a single construct. This phenomenon threatens discriminant validity, which is the extent to which distinct constructs remain empirically distinct from one another (Nájera, Abad, & Sorrel, 2025).

Fourth, the phrase "failed to load" means that an item did not achieve a factor loading of 0.50 or higher on any factor. In practical terms, this indicates that the item shares no meaningful relationship with any of the extracted factors.

A simplified version of EFA term definition diagram is reproduced below as in Table 26. Consequently, such items in construct variable were removed from further analysis because they did not contribute to any coherent construct.

Table 26 EFA Terms Definition

Term	Definition	How Applied in This Study
Factor Loading	Correlation between an item and its underlying factor	Minimum loading set to 0.50; higher loadings indicate stronger item-factor relationship
Communality	Proportion of item variance explained by all extracted factors	All values exceeded 0.50, indicating items were well-explained by the factors
Dimension/Factor	Latent construct grouping related observed variables	Four behavioural factors (Attitude, Subjective Norms, Perceived Control, Intention); Five knowledge factors (Password, Software/System, Human, Organisation, Social Security)
Bartlett's Test	Tests if correlation matrix differs from identity matrix	Significant ($p < .001$), confirming data suitability for factor analysis
KMO Measure	Assesses sampling adequacy	Values >0.50, indicating appropriate data for factor analysis
Total Variance Explained	Cumulative percentage of variance accounted for by retained factors	64.035% for behaviour; 65.327% for knowledge

i. Youngsters' Cyber Behaviour

The result show that communalities were over 0.50. An important step involved weighing the overall significance of the correlation matrix through Bartlett's Test of Sphericity,

which provide a measure of the statistical probability that the correlation matrix has significant correlations among some of its components. The results were significant, x^2 (n=765) = 5778.219 ($p < 0.001$), which indicate its suitability for factor analysis. The Kaiser-Meyer-Olkin measure of sampling adequacy (MSA) which indicates the appropriateness of the data for factor analysis, was 0.861. In this regard, data with MSA values above 0.500 are considered appropriate for factor analysis. Finally, the factor solution derived from this analysis yielded four factors for the scale, which accounted for 60.379 per cent of the variation in the data.

Nonetheless, in this initial EFA, two items (i.e "YoungPC1: I find it easy to ensure that I always comply with the cybersecurity knowledge awareness", "YoungPC4: I find it easy to behave differently if I have cyber security knowledge") loaded onto its factor and other than its underlying factor. In addition, one item "YoungPC4: I find it easy to behave differently if I have cyber security knowledge" loaded onto its factor and other than its underlying factor. Hence, the two items were removed from further analysis.

While the Kaiser-Meyer-Olkin (KMO) measure indicates the proportion of variance among variables that might be common variance, Bartlett's Test of Sphericity confirms that the correlation matrix is not random, hence the reason the test is used in this research. Together, they satisfy the statistical assumptions required to justify the use of EFA (KaaliÌ, Özkal, & DemiÌrer, 2025).

We then repeated the EFA without these items. The results of this new analysis confirmed the five-dimensional structure theoretically defined in this research (see Table 27). The Kaiser-Meyer-Olkin MSA was 0.843. The three dimensions explained a total of 64.035 per cent of the variance among the items in this study. The Bartlett's Test of sphericity proved to be significant, and all communalities were over the required value of 0.500. the four factors identified as part of this EFA aligned with the theoretical proposition in this research. Factor 1

includes items YoungATT1 to YoungATT4, referring to Youngsters' Attitude (YoungATT). Factor 2 gathers items YoungCCI1 to YoungCCI4, which represents Youngsters' Cyber Cautiousness Intention (Youngcci). Factor 3 indicates items YoungSP1 to YoungSP4, which represents Youngsters Surrounding Pressure (YoungSP). YoungSP is one of the four constructs derived from the Theory of Planned Behaviour (TPB) to measure subjective norms. Specifically, the perceived social pressure from family, friends, peers, and surrounding influences to engage in cybersecurity-safe behaviours. Finally, Factor 4 includes items YoungPC1 and YoungPC2, which represent Youngster's Perceived Control (YoungPC). Factor loading is presented in Table 28.

Table 27 Youngsters' Cyber Behaviour EFA Result

	Factor			
Items	1	2	3	4
Youngsters' Attitude				
YoungATT1	.868			
YoungATT2	.810			
YoungATT3	.800			
YoungATT4	.656			
Youngster's cyber cautiousness intention				
YoungCCI1		.717		
YoungCCI2		.683		
YoungCCI3		.845		
YoungCCI4		.770		
Youngsters Surrounding Pressure				
YoungSP1			.615	
YoungSP2			.807	
YoungSP3			.751	
YoungSP4			.626	
Youngsters Perceived Control				
YoungPC1				.870
YoungPC3				.549

ii. Youngsters' Cyber Knowledge Areas

Initially, the analysis showed that not all communalities were above 0.50. An important aspect of the analysis was testing the overall significance of the correlation matrix using Bartlett's Test of Sphericity. This test determines whether significant correlations exist among

the variables in the matrix. The results were statistically significant, with χ^2 (n = 765) = 6617.923 ($p < 0.001$), confirming that the data was appropriate for factor analysis. In addition, the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy was 0.684, which indicates that the data is suitable for factor analysis, as values greater than 0.500 are deemed acceptable. The factor solution identified four factors, accounting for 40.402 per cent of the total variance in the data, generally considered to explain a moderate amount of the total variance in the data.

We then removed 12 items for exploratory factor analysis (EFA) (see Table 28) as they did not load significantly on any of the factors to statistical criteria where the factor loadings < 0.50 (“failed to load”), communalities < 0.50, or cross-loading ≥ 0.50 on two or more factors. Items meeting any of these criteria were removed to ensure the statistical validity of the factor structure for subsequent analysis (EFA, CFA, SEM). Items for cybersecurity knowledge were removed, including:

a. HumSec2 ('Check if the website you're visiting uses HTTPS') failed to load (loading < 0.50). This is surprising, as checking HTTPS is a fundamental security practice. One possible explanation is that Malaysian youngsters may not be familiar with HTTPS or may not distinguish between HTTP and HTTPS, rendering this item ineffective for this population. Alternatively, mobile browsing, where HTTPS indicators are less visible, may be the primary mode of internet access for this demographic
b. HumSec5 ('Look at the URL bar to verify visiting the website') failed to load. Like HumSec2, this may reflect mobile browsing habits where the URL bar is often hidden or truncated.
c. SoftSysSec4 ('Clear browser cookies') and SoftSysSec5 ('Update applications to the latest version') failed to load. These are technically oriented practices that

may not resonate with non-expert users, particularly youngsters who may rely on automatic updates rather than manual checks

d. OrgSec1 ('Work device(s) is monitored by administrator') and OrgSec2 ('Organisation's IT helpdesk sends out alert messages'), these items cross-loaded onto both Organisation Security and Social Security, suggesting that youngsters who are not in full-time employment may not distinguish between workplace monitoring and broader social cybersecurity initiatives.
e. OrgSec5 ('Organisation organises security talks') was removed due to low loading. This item assumes participants work in organisations that provide formal security training, which may not apply to students or early-career workers.

Statistical removal does not mean these behaviours are unimportant for cybersecurity. Rather, it suggests that, within this specific sample of Malaysian youngsters aged 18-26, these items did not co-vary strongly with other items in their intended constructs. Possible explanations include; (1) Item may be to basic that respondents did not discriminate between them and other items; (2) Instrument adapted from Ion, Reeder, and Consolvo (2015) was originally designed for a general adult population, which may have stronger corporate security exposure. Malaysian youngsters, many of whom were students or early-career workers, may not encounter organisational security practices for instance “Clear browser cookies” as frequently as corporate employees. This 'corporate emphasis' in the original instrument may explain why some organisation-related items were removed; (3) The importance placed on certain security practices may differ between Malaysian youngsters and the populations in which the original instruments were validated.

Moreover, above justification aligned with the analysis using eigenvalues values at <1.00 and communalities of <0.500.

Same repetition as 4.3.3.2.2 were made to the items that were included for EFA which Kaiser-Meyer-Olkin MSA analysed at 0.654. The three dimensions explained a total of 65.327 per cent of the variance among the items in this study. This outcome suggests that the derived factor structure provides a coherent and well-supported representation of the data, offering a more interpretable framework. The Bartlett's Test of sphericity proved to be significant, and all communalities were over the required value of 0.500. The five factors and items identified in this analysis aligned well with the theoretical framework shown in Table 29.

Table 28 Items removed from CFA analysis

Code	Items
PassSec4	Use personal information (e.g., your name, last name, date of birth, etc) in your password
PassSec5	Reveal confidential information (e.g. Identification Number (ID), credit card number, and CVV number, etc)
SoftSysSec4	Clear Browser Cookies (e.g. username, password, bank account details, etc)
SoftSysSec5	Update applications to the latest version (e.g. operation systems, applications, etc)
HumSec2	Check if the website you're visiting uses HTTPS
HumSec5	Look at the URL bar to verify visiting the website
OrgSec1	Work device(s) is monitored by administrator
OrgSec2	Organization's Information Technology helpdesk sends out alert messages/emails concerning security
OrgSec5	Organization organizes security talks

Table 30 provides the Confirmatory Factor Analysis (CFA) results, which validate the factor structure identified in EFA.

Table 29 Youngsters' Cyber Knowledge EFA Result

	Factor				
Items	1	2	3	4	5
Password security					
PassSec1	0.671				
PassSec2	0.848				
PassSec3	0.66				
Software/System Security					
SoftSysSec1		0.636			
SoftSysSec2		0.858			
SoftSysSec3		0.819			
Human Security					
HumSec1			0.682		
HumSec3			0.681		
HumSec4			0.82		
Organisation Security					
OrgSec3				0.775	
OrgSec4				0.785	
Social Security					
SociSec2					0.751
SociSec3					0.602
SociSec4					0.885
SociSec5					0.713

4.3.3.2.2. Confirmatory Factor Analysis (CFA)

Rather than simply extracting patterns from data, CFA directly evaluates how well a proposed factor structure aligns with the observed relationships (Roos & Bauldry, 2021). A structural equation model (SEM) was generated through moment structure (AMOS) 29.0 from SPSS version 29.0 to draw a graph of the Measurement Model for CFA. All the constructs in this research are drawn and then covaried with each other to perform CFA. Then the model is assessed for Model Fit, and the reliability and validity of the constructs is assessed as in Figure 35.

Referring to Table 30 (Reliability and Convergent Validity), the concept of a "dominant factor" or statistically called as strongest measurement properties can be understood in two ways: by factor loading magnitude (from EFA) and by construct reliability and validity (from CFA). Among all constructs, Youngsters' Attitude (YoungATT) exhibits the highest composite reliability (CR = 0.991) and the highest average variance extracted (AVE = 0.685), indicating that it explains the greatest proportion of variance in its observed indicators. This suggests that, among the behavioural constructs derived from the Theory of Planned Behaviour, attitude toward cybersecurity practices is the most reliably measured and conceptually coherent factor in this study.

Several noteworthy values deserve explicit commentary. YoungPC2 (loading = 0.905) is particularly striking, as it demonstrates that the item "Following cyber security knowledge awareness affecting my cyber behaviour" shares approximately 82% of its variance ($0.905^2 = 0.819$) with the Perceived Control construct. This indicates that respondents who perceive a direct link between their cybersecurity knowledge and their behavioural outcomes are exceptionally strong indicators of overall perceived behavioural control. Conversely, SoftSysSec1 ("Use a pop-up blocker") has the lowest loading in the table (0.445), with only 19.8% of its variance explained by the Software/System Security factor and a correspondingly high measurement error (0.802). This suggests that pop-up blockers may not be a salient or recognised cybersecurity practice among Malaysian youngsters. Similarly, PassSec3 (loading = 0.485) falls slightly below the 0.50 threshold, implying that traditional password complexity rules may be less relevant to this demographic, possibly due to the increased adoption of password managers or updated password guidelines.

On the other hand, SoftSysSec3 ("Anti-virus software is up to date") demonstrates the strongest loading among the knowledge domains (0.896), confirming that keeping antivirus software updated is a well-understood and coherent cybersecurity practice. Among the

behavioural constructs, YoungATT1 (loading = 0.892) shows that youngsters hold a strong positive attitude toward the consistent adherence to cybersecurity knowledge. These highlighted values provide a clearer understanding of which items most reliably represent their respective constructs, and which may warrant reconsideration in future research.

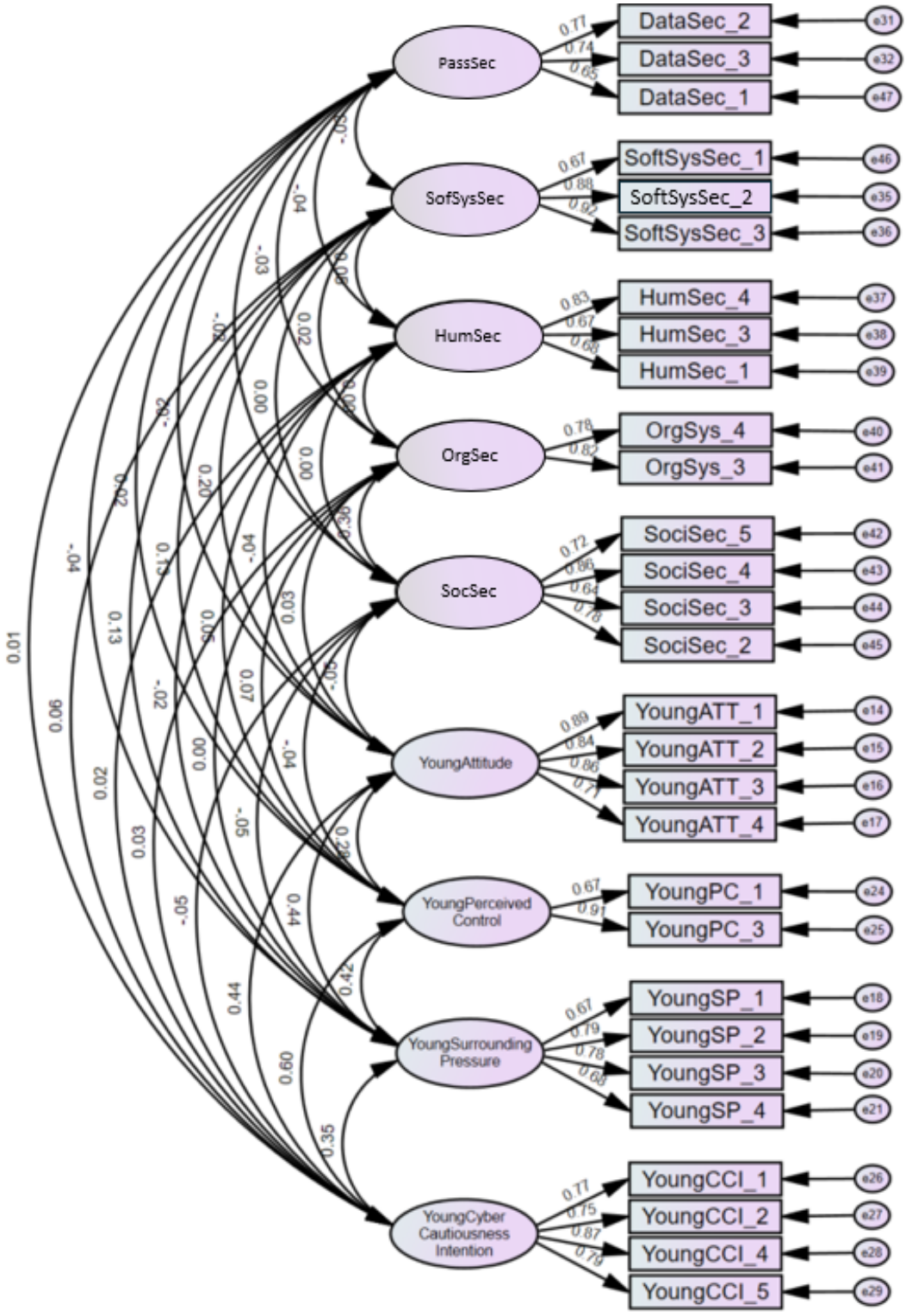


Figure 35 Final CFA Model

Table 30 Reliability and Convergent Validity

Variables/ Constructs	Items	Standardised Factor Loadings	Cronbach Alpha	Composite Reliability (CR)	Average Variance Extracted (AVE)	Maximum Shared Varience (MSV)	Standardised Factor Loading^2	Error (1-loading*2)
YoungAttitude	YoungATT1	.892	.868	.991	.685	.194	.796	.204
	YoungATT2	.839	.810				.704	.296
	YoungATT3	.858	.800				.736	.264
	YoungATT4	.711	.656				.506	.494
YoungSurrounding_Pressure	YoungSP1	.670	.615	.830	.536	.194	.449	.551
	YoungSP2	.789	.807				.623	.377
	YoungSP3	.779	.751				.607	.393
	YoungSP4	.682	.626				.465	.535
YoungPerceived_Control	YoungPC1	.677	.870	.786	.639	.359	.458	.542
	YoungPC2	.905	.549				.819	.181
YoungCyber_Cautiousness_Intention	YoungCCI1	.767	.717	.852	.636	.359	.588	.412
	YoungCCI2	.754	.683				.569	.431
	YoungCCI3	.873	.845				.762	.238
	YoungCCI4	.790	.770				.624	.376
Password Security	PassSec1	.793	.671	.745	.444	.001	.629	.371
	PassSec2	.683	.848				.466	.534
	PassSec3	.485	.660				.235	.765
Software/System Security	SoftSysSec1	.445	.636	.605	.540	.038	.198	.802
	SoftSysSec2	.787	.780				.619	.381
	SoftSysSec3	.896	.797				.803	.197
Human Security	HumSec1	.682	.682	.772	.533	.003	.465	.535
	HumSec3	.670	.681				.449	.551
	HumSec4	.827	.820				.684	.316
Organisation Security	OrgSys3	.825	.775	.784	.645	.129	.681	.319
	OrgSys4	.780	.785				.608	.392
Social Security	SociSec2	.778	.751	.838	.567	.129	.605	.395
	SociSec3	.641	.602				.411	.589
	SociSec4	.863	.885				.745	.255
	SociSec5	.712	.713				.507	.493

The measurement model was assessed to evaluate its reliability, convergent validity, and discriminant validity. The confirmatory factor analysis (CFA) results in Table 30 indicate a good fit of the model to the data. The fit statistics ($X^2/df = 2.96$, RMSEA = .051, RMR = .062, GFI = .918, CFI = .933) fall within the acceptable thresholds recommended by Li-tze & Bentler (1999) and Browne & Cudeck (1992), thus confirming a satisfactory model fit.

All constructs demonstrated strong internal consistency reliability, with both Cronbach's Alpha and Composite Reliability (CR) values exceeding the recommended value of 0.70.

Convergent validity was generally supported. The standardised factor loadings for most measurement items were above the 0.60 criterion, and all were significant. Furthermore, the Average Variance Extracted (AVE) for most constructs surpassed the 0.50 benchmark (Claes & Larcker, 1981), indicating that the constructs adequately explain the variance of their indicators. For the "Password Security" construct, the AVE value was 0.444, slightly below the 0.50 threshold. However, its Composite Reliability (0.744) was well above the 0.70 acceptability standard. Following the guidance of Hair et al. (2010), this combination indicates that the convergent validity for this construct remains adequate, as the CR confirms its internal consistency. Similarly, one item for "Software/System Security" (SofSysSec1) had a factor loading of .445. This loading was retained as it meets the more liberal but acceptable 0.40 threshold suggested by (Stevens, 2009) and was deemed essential for maintaining the content validity of the construct.

Finally, discriminant validity was established for all constructs, as the Maximum Shared Variance (MSV) for each was less than its corresponding AVE (Claes & Larcker, 1981).

In summary, the results confirm that the measurement model is both reliable and valid, providing a solid foundation for testing the structural model.

4.3.4. Open-Ended Response Analysis

To complement the quantitative data and gain deeper, contextual insights into participants' perceptions, a thematic analysis was conducted on the single open-ended survey item requesting "Additional Information". This qualitative approach was essential to capture the nuanced, unprompted concerns and suggestions of the respondents (Nowell et al., 2017),

providing a rich understanding that closed-ended questions could not fully elicit (Braun & Clarke, 2006).

4.3.4.1. Data Preparation and Analytical Process

The analysis followed a systematic, multi-stage process. Initially, the textual data from all 54 respondents who provided additional comments were extracted and compiled. The analysis was conducted using a hybrid approach, leveraging both software-assisted analysis with NVivo 15 (Release 1.7.2) and manual coding in Microsoft Excel to ensure rigor and comprehensiveness.

1. **Familiarisation and Initial Theme Generation using NVivo:** The qualitative data was first imported into NVivo 15. As the initial step in the analysis process, prior to any manual coding, the software's word frequency query was conducted to identify the most frequently occurring terms across all 54 responses. This provided an unbiased, data-driven overview of prominent concepts without researcher-imposed categories. The analysis visually highlighted words such as "awareness", "cybersecurity", "exposed", "elderly", "education", and "government", as evident in Figure 36. These frequent terms, generated directly from participants' own language, served as a foundational guide for the initial inductive coding process. Following this, the data underwent a process of immersive and repeated reading to ensure deep familiarity with the content, after which a preliminary set of codes was generated based on the data's content.

Figure 36 Word Cloud Query from NVivo

2. **Development of a Structured Codebook and Systematic Coding in Excel:** The preliminary codes from NVivo were refined and organised into a structured codebook comprising 11 distinct themes, each with a corresponding code (e.g., CMA, VGE, VGY), as detailed in Table 31. This codebook was then applied systematically in an Excel spreadsheet. To ensure coding consistency and to validate the themes identified in NVivo, the frequent words from the NVivo query were actively cross-referenced during the Excel coding process. This cross-referencing ensured that the final themes were not only comprehensive but also directly anchored in the specific language used by the participants.

Table 31 Thematic codebook for open-ended responses

Code	Themes	Description
CMA	Call for More Awareness	Explicitly states a need for more exposure, campaigns, or highlights a current lack of awareness.
VGE	Vulnerable Groups: Elderly	Identifies the elderly, older people, or parents as a vulnerable group.
VGY	Vulnerable Groups: Youngsters	Identifies children, teenagers, students, or the younger generation as a target group.
EDU	Education & Training	Focuses on formal education, training programmes, or curriculum integration.
SYS	Systemic & Government Role	Mentions the role of authorities, government, or organisations.
BAC	Barriers: Cost & Accessibility	Identifies financial cost as a barrier to security.
BAK	Barriers: Knowledge & Complexity	States that cybersecurity is hard to understand or that knowledge is lacking.
POS	Positive Feedback/General Support	Provides general positive feedback or agrees with the importance of cybersecurity.
NEG	Negative Feedback/Critique	Criticises the survey method or data collection.
PRAC	Personal Practice	Describes the respondent's own cybersecurity habits.
N/A	No Additional Info / N/A	The field is empty or contains no additional info.

3. **Data Structuring for Quantitative Analysis:** To facilitate the quantitative analysis of qualitative data, a "one theme per row" structure was initially adopted during the coding process in Excel. This meant that a single response expressing multiple ideas was assigned multiple codes across separate rows, with participant sentences duplicated to maintain context for each code. This duplication was necessary for the systematic counting of theme frequencies and proportions during analysis. However, for the final presentation in Table 3*2*, each unique participant statement is typed only once, with all associated codes listed alongside it. This approach preserves the clarity of the analysis while enhancing the readability of the table.

Table 32 Single response with multiple themes

Excerpt from transcript	*Codes*
"In Malaysia, exposure to cyber security is still on minimal level especially within primary and secondary school students", #P29	Vulnerable Groups: Youngsters (VGY) Call for More Awareness (CMA)
"I hope government can provide initiative to send awareness to more people about the cyber security as we are moving fast in the modern world", #P34	Systemic & Government Role (SYS) Call for More Awareness (CMA)
"I think it is better for the knowledge of security is implemented in the education website of university, school and so on to avoid any unethical behaviour among the students", #P36	Vulnerable Groups: Youngsters (VGY) Education & Training (EDU)
"Cyber security is really important as it helps to protect my privacy and ensure my cyber life is safe and free from any scams and threats. It is important for kids and adults nowadays to be exposed to the cyber security program and have an awareness of it as it will build a cyber-safe generation in the future. Thank you and good luck for your study.", #P7	Vulnerable Groups: Elderly (VGE) Vulnerable Groups: Youngsters (VGY) Call for More Awareness (CMA)
"I usually detect scam by using google lens for pictures, CCID web and true caller. I realised that we lack of cybersecurity awareness as people around me tend to trust any people that try to scam them. I often need to remind them always as im always alert with the scammers.", #P15	Vulnerable Groups: Elderly (VGE) Call for More Awareness (CMA) Personal Practice (PRAC)
"Cyber security issues demand more attention from many authorities, including the government, employers, and families, because during these day, everyone is exposed to cyber fraud.", #P25	Systemic & Government Role (SYS) Call for More Awareness (CMA)

4.3.4.2. Thematic Analysis Findings

This section presents the first mention of the themes derived from the open-ended responses. The analysis of 54 responses yielded 76 code-able instances across the 11 themes. The frequency and proportion of each theme are presented in Table 33 and summarised in Figure 37.

The most prominent finding was a pervasive Call for More Awareness (CMA), which constituted over a third of all coded themes. This indicates a strong consensus among participants that current levels of cybersecurity awareness are insufficient. This result aligns with previous research conducted by Abdullah et al. (2018) , which emphasised that Malaysia's growing integration with ICT highlights the critical importance of widespread cybersecurity awareness.

A portion of the responses also highlighted specific Vulnerable Groups, with concerns for Youngsters (VGY) appearing only a few percentage points higher than for the Elderly (VGE). This was often coupled with calls for structured Education & Training (EDU) , which also represented a meaningful proportion of the themes. Participants suggested integrating cybersecurity into school curricula, an area highlighted in the literature as warranting further investigation (Rehman & Manickam, 2023), and creating targeted programmes for different demographics.

Furthermore, a Systemic & Government Role (SYS) was mentioned in a smaller proportion of responses. While infrequent, this indicates that some participants perceived a need for greater involvement from authorities and organisations. As discussed in Section 2.6.1, relevant authorities such as CyberSecurity Malaysia and MCMC have implemented cybersecurity initiatives; however, respondents expressed that these initiatives may not be reaching a broad enough segment of the public. A smaller subset of comments pointed to barriers, including the perceived Cost & Accessibility (BAC) and Knowledge & Complexity (BAK) of cybersecurity itself, which were mentioned infrequently but nonetheless suggest obstacles that deter proactive measures.

Table 33 Frequency and Proportion of Identified Themes

Themes	Codes	Frequency	Proportion
Call for More Awareness	CMA	27	36%
Vulnerable Groups: Elderly	VGE	7	9%
Vulnerable Groups: Youngsters	VGY	11	14%
Education & Training	EDU	8	11%
Systemic & Government Role	SYS	5	7%
Barriers: Cost & Accessibility	BAC	1	1%
Barriers: Knowledge & Complexity	BAK	3	4%
Positive Feedback/General Support	POS	8	10%
Negative Feedback/Critique	NEG	1	1%
Personal Practice	PRAC	3	4%
No Additional Info / N/A	N/A	2	3%
Total		76	100%

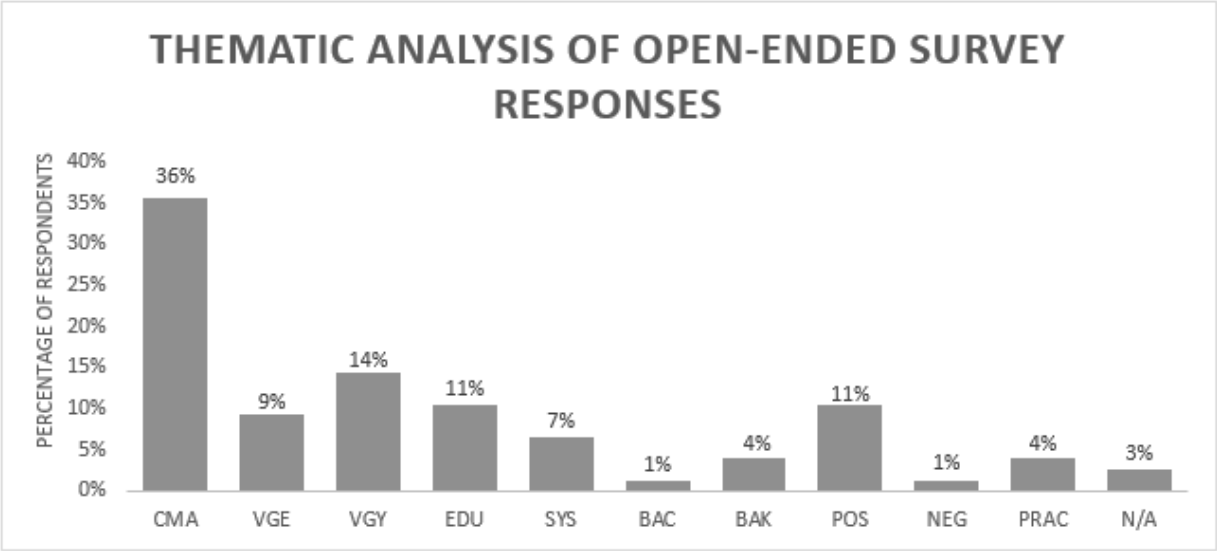


Figure 37 Thematic Analysis of Open-Ended Survey Responses

4.3.4.3. Bridge to Knowledge Domain from Quantitative Data

The findings from this thematic analysis provide a critical qualitative depth to the quantitative results.

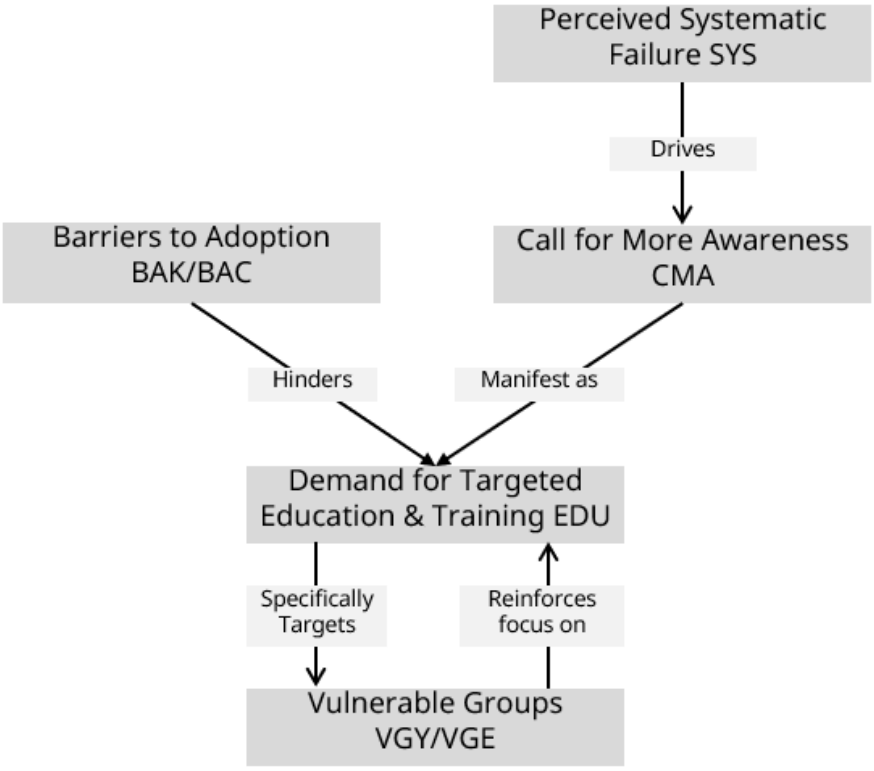


Figure 38 Relationship between themes

The conceptual model in Figure 38 offers a synthesised explanation, suggesting that cybersecurity application is a consequence of domain knowledge and education. The predominant call for awareness (CMA) directly correlates with the survey statistics, which indicated moderate to low engagement with certain cybersecurity practices (e.g., Human Security, Social Security). The identified focus on Vulnerable Groups (VGE, VGY) and Education (EDU) is discussed in relation to the demographic findings and the potential need for tailored intervention strategies in Section 5.3.

4.4. PHASE 2 ANALYSIS: Phishing Simulation Data

4.4.1. Data cleaning

The initial participant pool comprised N=765 individuals. As a mandatory prerequisite for inclusion in the phishing simulation phase, participants were requested to provide a valid and verifiable email address during the first phase. Cases that failed to meet this criterion, as such, those who did not provide an email address or those with technically invalid/unreachable addresses, were excluded from the subsequent campaign and the final analysis cohort. This pre-screening exclusion resulted in a final sample size of N=483 for the primary analysis of susceptibility to the three phishing email conditions. The non-participation at this stage is considered a Missing Completely at Random (MCAR) mechanism relative to the subsequent phishing outcomes, as it is based purely on technical compliance.

The analytical foundation for this chapter is the curated dataset, prepared as described in the Methods chapter, which was analysed using IBM SPSS Statistics. Crucially, the numerical values for the dependent variable (Experiment Status or ‘expstatus’), were decoded. This involved verifying and recoding the values within the variables themselves to ensure accurate representation of the experimental conditions. The primary outcome was modelled as an ordinal variable with four levels of escalating engagement, starting at the lowest level: '1': Email Sent, '2': Email Opened, '3': Link Clicked, and '4': Data Submitted. The distribution of cases across these ordinal levels is first examined descriptively, followed by inferential analyses to identify factors associated with progression to higher stages of susceptibility.

4.4.2. Descriptive Results of the Phishing Simulation

A cross-tabulation analysis was conducted to examine the distribution of participant responses across three different phishing campaign in Section 3.4 and the various email classifications. This initial descriptive analysis provides an overview of the data structure and

reveals key patterns in user susceptibility before inferential statistical testing. The row variable was the experiment number (‘ExperimentNo’), representing the three different phishing simulations, and the column variable was the experimental status (‘ExperimentalStatus’), which categorised participant interaction with the phishing email into one of four ordered levels, as explained in Table 34.

Table 34 Cross-Tabulation of Phishing Experiment Number by Participant Response Status

		ExperimentStatus				
		1	2	3	4	Total
Experiment No	1	1	3	22	139	165
	2	4	5	19	144	172
	3	0	4	19	123	146
Total		5	12	60	406	483

First, most participant interactions across all three experiments fell into the safest category, ‘Email Sent’ (Status 1), accounting for 406 out of 483 total responses (84.1%). This indicates a generally high level of security knowledge among the cohort. The email was sent using GoPhish tools to the participant's email address.

Second, the rate of the most severe compromise, 'Submitted Data' (Status 1), was consistently very low throughout the experiments. It was observed in only 5 instances out of 483 (1.0%), with no occurrences in the third experiment. The intermediate engagement levels of 'Clicked' (Status 2) and 'Opened' (Status 3) also represented small proportions of the total responses, at 2.5% (n=12) and 12.4% (n=60), respectively.

When examining the trends across the sequential experiments, the number of participants who exhibited 'No Interaction' (Status 4) remained the dominant response in each round, constituting 406 out of 483 total responses (84.1%). This indicates a generally high baseline level of security awareness among the cohort. However, a slight fluctuation in the total

number of participants per experiment is noted (165, 172, 146). The counts for the more severe responses, particularly 'Submitted Data' (Status 1) and 'Clicked' (Status 2) are low, suggesting high knowledge in cyber security.

Table 35 Case Processing Summary

	Decsription	N	Marginal Percentage
Experiment Status	Email Sent	406	84.1%
	Email Open	60	12.4%
	Clicked Link	12	2.5%
	Submitted Data	5	1.0%
Age	18-19	20	4.1%
	20-21	111	23.0%
	22-23	94	19.5%
	24-25	78	16.1%
	26	180	37.3%
Gender	Male	101	20.9%
	Female	377	78.1%
	Others	5	1.0%
LOEdu	High-School	25	5.2%
	Diploma	121	25.1%
	Degree	277	57.3%
	Masters	52	10.8%
	PhD	8	1.7%
Valid		483	100.0%
Total		765	

In summary, these descriptive results establish a baseline understanding of participant behaviour, characterising the sample as largely resilient to the phishing simulations but with a small, consistent proportion engaging in risky behaviours. This sets the foundation for the

formal hypothesis testing presented in the next section, which will determine if these observed differences across experiments are statistically significant.

4.4.3. Bridging the Data: Correlating Survey and Simulation Result

To test the hypothesis that the type of phishing email significantly predicts the level of participant cyber knowledge, a regression model was employed. This approach ensures robust analysis of both susceptibility in phishing and the outcome of overall variables. The Ordinal Logistic Regression (OLR), specifically the proportional odds model, was selected due to the inherently ordered nature of the variable. To test the hypothesis that the type of phishing email significantly predicts the level of participant cyber knowledge, an ordinal logistic regression was employed. Specifically, the proportional odds model was selected due to the inherently ordered nature of the outcome variable (phishing susceptibility). Phishing susceptibility, as operationalised in this study, is not a simple binary state but a hierarchical construct of escalating compromise severity (Taylor & Becker, 1998). The outcome variable, 'ExperimentalStatus', captures this inherent order, ranging from the least severe 'No Interaction' to the most severe 'Submitted Data'.

Table 35 shows the Cases Processing Summary highlighting the cases included in the analysis. The number of missing cases (n=282) primarily reflects the exclusion of participants who did not successfully enter the experimental phase, aligning with the listwise exclusion approach for non-compliance and invalid data (as noted in Section 4.4.1). The total sample size for the analysis (N=483) is correctly reflected in the descriptive results above. The high rate of no interaction in the phishing simulation was not anticipated but is consistent with some prior phishing simulation studies (Gordon et al., 2019; Rizzoni et al., 2022).

Model Fitting Information in Table 35 shows that there is a significant improvement in fit (<0.05) as compared to null model, hence, the model is showing a good fit. Meanwhile for

Goodness-of-Fit in Table 36 shows statistically significant improvement in fit over the null model, confirming that the phishing experiment, as a set, are meaningful for predicting the variables below.

Table 36 Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	358.363			
Final	337.670	20.693	11	0.037
Link function: Logit.				

Table 37 Goodness-of-Fit

	Chi-Square	df	Sig.
Pearson	649.104	580	0.024
Deviance	252.316	580	1.000
Link function: Logit.			

The pseudo-R-square values reported in Table 37 indicate the proportion of variance in phishing susceptibility explained by the demographic predictors. The Nagelkerke R^2 of 0.063 suggests that the model explains approximately 6.3% of the variance, which, while statistically significant, indicates that unmeasured factors (e.g., cognitive load, personality traits, contextual cues) account for the majority of variance in phishing susceptibility which a common finding in behavioural cybersecurity research (Clark et al., 2023; Kwak et al., 2020). For this research, there has been a 3.9 percent increase in the prediction of the moderator in the model (age, level of education and gender) based on the behaviour in comparison to the null model.

Table 38 Pseudo R-Square

Types of Pseudo R-Square	
Cox and Snell	0.042
Nagelkerke	0.063
McFadden	0.039
Link function: Logit.	

For Parameter Estimates, Table 38 shows an increase of youngsters' intention (β=-0.091; s.e.[d]=0.148; P-value=0.541) when there is lower phishing susceptibility. The Odds Ratios (O.R) quantify the change in the odds of a participant being in a higher category of susceptibility (i.e., 'Clicked Link' or 'Submitted Data') versus all lower categories, for a one-unit change in the predictor. The ordinal regression analysis revealed a complex picture regarding the demographic predictors of phishing susceptibility. The ordinal regression analysis revealed a statistically significant effect for gender; however, the extreme parameter estimates (e.g., Male: $\beta = -11.926$, $p < .001$; Female: $\beta = -13.070$, $p < .001$) and odds ratios of effectively zero suggest the presence of quasi-complete separation.

Quasi-complete separation occurs in logistic regression when a predictor variable perfectly predicts the outcome for most, but not all, cases. This phenomenon typically arises when there are zero cell counts, for example, when no participants from a particular gender group fall into the highest severity category (Clark et al., 2023). However, removing the parameter entirely would lose information. The standard solution (Clark et al., 2023) is to collapse categories or collect more balanced data. For this study, the gender results are reported with a cautionary note, and the 'Others' category is treated as the reference. Future research should recruit a larger and more balanced sample to enable stable estimation of gender effects.

In contrast, the effects of Age and Level of Education on compromise severity were not statistically significant. While point estimates indicated that younger age groups (e.g., 20-21 years: O.R = 1.52) and those with lower educational level (e.g., High School: O.R = 2.83) had

elevated odds of more severe susceptibility compared to their older (≥26 years) and PhD-holding counterparts, the confidence intervals for all categories crossed the null value (OR = 1.0) and p-values exceeded the .05 threshold. Therefore, after addressing the gender variable anomaly, no robust, significant demographic predictors of phishing compromise severity were identified in this model.

Table 39 Parameter Estimates and Odd Ratio

		β	O.R	S.E	Wald	df	Sig.	95% Confidence Interval Lower Bound	pper Bour
Location	Youngster's Intention	-0.091	0.913	0.148	0.374	1	0.541	-0.382	0.200
	18-19	0.384	1.468	0.697	0.304	1	0.581	-0.982	1.750
	20-21	0.417	1.517	0.363	1.316	1	0.251	-0.295	1.129
	22-23	0.201	1.223	0.371	0.294	1	0.588	-0.526	0.929
	24-25	-0.425	0.654	0.342	1.545	1	0.214	-1.096	0.245
	26	0[a]				0			
	Male	-11.926	0.000	0.418	813.034	1	0.000	-14.846	-13.206
	Female	-13.070	0.000	0.000		1		-15.170	-15.170
	Others	0[a]				0			
	High-School	1.039	2.826	1.145	0.824	1	0.364	-1.204	3.282
	Diploma	0.213	1.237	0.891	0.057	1	0.811	-1.533	1.959
	Degree	0.678	1.971	0.874	0.603	1	0.438	-1.035	2.392
	Masters	0.079	1.083	0.919	0.007	1	0.931	-1.721	1.880
	PhD	0[a]				0			

Link function: Logit.
a. This parameter is set to zero because it is redundant.

The columns in Table 38 represent:

- **β (Estimate)**: The log-odds coefficient for each predictor. Negative values indicate lower odds of higher severity; positive values indicate higher odds.
- **O.R. (Odds Ratio)**: Exp(β); the factor by which the odds of being in a higher severity category change for a one-unit increase in the predictor. An OR < 1 indicates lower odds; OR > 1 indicates higher odds.*

- **S.E.**: Standard error of the estimate.
- **Wald**: Chi-square test statistic for each predictor.
- **df**: Degrees of freedom.
- **Sig.**: p-value; values < 0.05 indicate statistical significance.*
- **95% Confidence Interval**: The range within which the true odds ratio is likely to fall with 95% confidence.*

For example, the odds ratio for '20-21 years' (O.R. = 1.517) suggests that participants aged 20-21 have approximately 1.5 times higher odds of being in a higher severity category compared to the reference age group (26+ years), but this result is not statistically significant (p = 0.251).

The proportional odds assumption, a prerequisite for the ordinal regression model, was assessed using the Test of Parallel Lines. The result in Table 39 was non-significant ($\chi^2(22) = 30.837$, $p = 0.100$), indicating that the assumption was not violated and fulfilled. This confirms that the effect of the predictor variables on moving between the ordered categories of phishing susceptibility was consistent across all threshold points in the model, thus validating the use of the ordinal logistic regression approach.

Table 40 Test of parallel lines

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Null Hypothes	337.670			
General	306.833[b]	30.837[c]	22	0.100

The ordinal regression analysis indicated that gender was a statistically significant predictor of phishing susceptibility. However, due to quasi-complete separation (discussed

above), the odds ratios for male (OR ≈ 0.000) and female (OR ≈ 0.000) participants were effectively zero relative to the reference category ('Others'). This suggests that, within this sample, no male or female participants fell into the highest severity categories (e.g., 'Data Submitted'), while a small number of participants in the 'Others' category did. Thus, the finding should be interpreted with caution, and the apparent 'lower odds' for male and female participants is an artefact of the sparse data distribution rather than a meaningful substantive finding. All other demographic variables (‘Age’ and ‘LOEdu’) are insignificant predictors of the level of phishing susceptibility.

4.5. Testing the Research Model and Hypotheses

We used IBM SPSS and SEM using SPSS AMOS Statistics for conducting statistical analyses, designed to streamline data management and processing for research. It allows survey data, often encoded numerically (e.g., 1 for "male", 2 for "female" and 3 for “others”), to be stored alongside descriptive labels for better readability and interpretation. SPSS supports multiple data formats, including files from database applications like Microsoft Access and spreadsheets like Microsoft Excel and Lotus 1-2-3. Additionally, it can import ASCII files and data created in earlier SPSS versions, offering versatility and seamless integration for data handling (Huizingh, 2007). In this study, each hypothesis was evaluated as either fully supported (if all criteria met) or not supported (if any criterion failed). This binary approach is consistent with standard hypothesis testing conventions.

4.5.1. Structural model assessment

A structural equation model generated through AMOS was used to test the relationship. A good-fitting model is accepted if the value of the CMIN/df is <5 (K. Wang et al., 2020), the goodness-of-fit (GFI) indices; the Tucker & Lewis (1973) index (TLI); the Confirmatory fit index (CFI) (Bentler, 1990) is > 0.90 (hair et al, 2010). In addition, an adequate-fitting model

was accepted in the AMOS computed value of the standardised root mean square residual (RMR) <0.05, and the root mean square error approximation (RMSEA) is between 0.05 and 0.08 (hair et al, 2010). The fit indices for the model shown in Table 40 fell within the acceptable range: CMIN/df = 3.345, goodness-of-fit (GFI) = .901, TLI = .904, CFI = .916, SRMR = .07, and RMSEA = .05.

The squared multiple correlation was 0.40 for youngsters' intention, this shows that 40% variance in youngsters' intention is accounted by youngsters' attitude, youngsters' social pressure and youngsters perceived control (Figure 39).

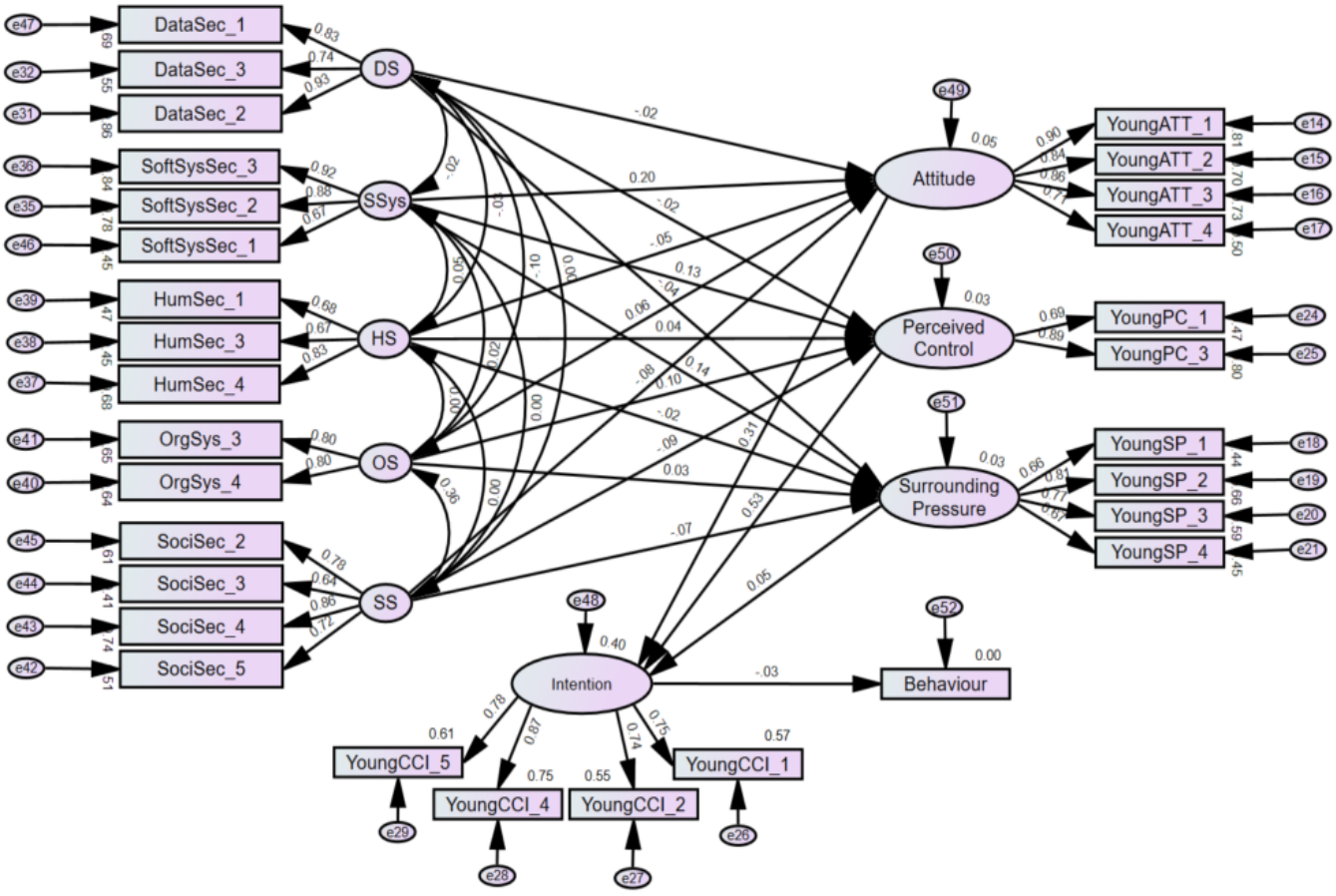


Figure 39 Square Multiple Correlation

The study assessed the influence of cyber knowledge domain, which is password security, software/system security, human security, organisation security on youngsters' intention. The influence of password security on attitude was negative and insignificant (b = -.021, t = -.413, p = .680). Hence, h_1 (Youngsters who hold a more positive attitude toward cybersecurity practices will demonstrate stronger intention to engage in secure online behaviour) was not supported. The influence of software/system security on attitude was positive and significant (b = .166, t = 5.106, p < .001) hence, h2 was supported.

Model fit indices and hypotheses results are presented in Table 40 and tested research model with result in Figure 40.

Each hypothesis in this study proposes a directional relationship between two constructs (e.g., "Software/System Security has a significant positive influence on Attitude"). The decision to support or reject a hypothesis is based on three criteria:

a) The direction of the relationship: The standardised estimate (β) must be positive (as hypothesised) or negative (if a negative relationship was hypothesised).
b) The statistical significanc: The p-value must be less than 0.05.
c) The t-value – The t-value must be greater than ±1.96 (for $p < 0.05$).

To illustrate, consider Hypothesis H6b: "Software/System Security has a significant positive influence on Attitude." The results showed a positive standardised estimate (β = 0.166), a t-value of 5.106 (well above ±1.96), and a p-value of < .001. Since all three criteria were satisfied; positive direction, statistical significance, and an adequate t-value; this hypothesis was marked as "Yes" (Supported) in Table 40.

Example: **Password Security → Attitude (H6a)**

In contrast, Hypothesis H6a: "Password Security has a significant positive influence on Attitude." The results showed a negative standardised estimate (β = -0.021), a t-value of -0.413

(within the range -1.96 to +1.96), and a p-value of 0.680 (well above 0.05). Since the direction was negative (opposite to the hypothesised positive relationship) and the result was not statistically significant, this hypothesis was marked as "No" (Not Supported) in Table 40.

Table 40 summarises all hypothesis testing results, and Figure 40 provides a visual representation of the significant paths in the structural model. Non-significant paths were also reported in Figure 40 for clarity from the beginning to the end of the research.

Table 41 Hypotheses result

Hypothesis	Path	Standardised Estimate (β)	t-value	p-value	Decision
H1	Attitude → Intention	0.253	8.597	< .001	Yes
H2	Subjective Norms (Surrounding Pressure	0.046	1.532	0.126	No
H3	Perceived Control → Intention	0.533	11.814	< .001	Yes
H4	Perceived Control → Behaviour	-0.013	-0.686	0.493	No
H5	Intention → Behaviour	-0.013	-0.686	0.493	No
H6a	Password Security → Attitude	-0.021	-0.413	0.68	No
H6b	Software/System Security → Attitude	0.166	5.106	< .001	Yes
H6c	Human Security → Attitude	-0.059	-1.089	0.276	No
H6d	Organisation Security → Attitude	0.065	1.353	0.176	No
H6e	Social Security → Attitude	-0.073	-1.432	0.152	No
H7a	Password Security → Subjective Norms	-0.048	-0.926	0.355	No
H7b	Software/System Security → Subjective	0.116	3.034	< .001	Yes
H7c	Human Security → Subjective Norms	-0.03	-0.541	0.588	No
H7d	Organisation Security → Subjective Nor	0.034	0.682	0.495	No
H7e	Social Security → Subjective Norms	-0.086	-1.766	0.077	No
H8a	Password Security → Perceived Contro	-0.017	-0.4	0.689	No
H8b	Software/System Security → Perceived	0.091	3.182	0.001	Yes
H8c	Human Security → Perceived Control	0.047	1.001	0.317	No
H8d	Organisation Security → Perceived Con	0.084	2.042	0.046	Yes
H8e	Social Security → Perceived Control	-0.078	-1.846	0.065	No

CMIN/df =3.345, the goodness-of-fit (GFI) = .901, TLI = .904, CFI = .916, SRMT = .07, and RMSEA = .05.

A hypothesis was considered supported if three conditions were met; (1) standardised estimate (β) was in the hypothesised direction (positive for all H6–H8); (2) the p-value was less than 0.05, and; (3) the t-value exceeded ±1.96. Non-significant paths ($p \geq 0.05$) and paths with estimates in the opposite direction to that hypothesised were considered not supported.

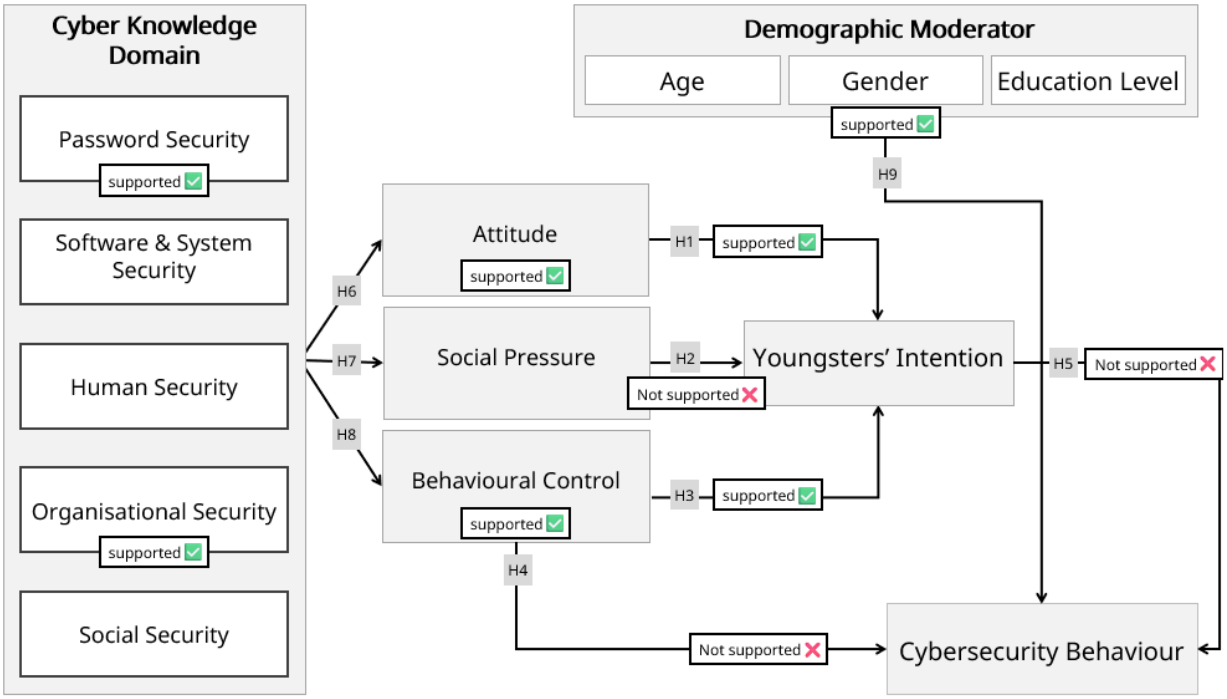


Figure 40 Tested research model result

This study highlights a disconnect where high cybersecurity intentions does not significantly predict cybersecurity behaviour (H5), check Figure 40 as above, this can be interpreted in two interconnected factors, one was during the execution of the phishing experiment and two is the conceptual scope in the experimental phase. As a high volume of participants, 84.1% missed or ignored the simulation (can be seen in Table 34), the behavioural outcome variable was absent. As intention cannot manifest if the phishing attempt is not encountered, this suggests that in real-world scenarios, the primary challenge isn't just a lack of intent, but a lack of situational engagement with the threat itself. Secondly, the research

model measured knowledge and intention within defined knowledge domains but omitted critical behavioural competencies. Since the research did not assess respondent's ability to detect deception, their knowledge of reporting protocols for suspicious emails, or their awareness of recovery steps post-breach creates a significant barrier between wanting to be secure and knowing how to act securely in a dynamic threat environment.

The limited interaction with the phishing emails suggests that simply ignoring a message may be a passive form of defence, however, this does not indicate whether the user correctly identified the email as deceptive or was aware of the appropriate reporting alternatives such as in Figure 17. The following 5.2.4 will address the ambiguity, whether 'ignore' an email constitutes an informed defence, while also addressing the missing behavioural components of proactive deception detection, incident reporting, and post click recovery and addressing the research recommendation (5.3), research limitation (6.4) and future work (6.5).

4.5.2. Correlation Between Demographic Differences to Actual Behaviour

H9: There is negative significant relationship between demographic and behaviour

Pearson product correlation was computed to assess demographic and behaviour (Table 38). There was a negative correlation between the variables (age r= -.379, p<.001; Gender r= -.298, p<.001; LOEdu r= -.404, p<.001) and actual behaviour, hence H9 was supported. The negative correlations indicate that as age and level of education increase, risky cybersecurity behaviour decreases. Similarly, the negative correlation with gender (where male = 1, female = 2) suggests that male participants exhibited lower levels of risky behaviour compared to female participants. In other words, older, more educated, and male participants were less likely to engage in risky actions (such as clicking phishing links or submitting data) during the phishing simulation.

Table 42 Correlation between demographic and behaviour

	Age	Gender	LOEdu	Behaviour
Age	1			
Gender	.265**	1		
LOEdu	.592**	.334**	1	
Behaviour	-.379**	-.298**	-.404**	1

**. Correlation is significant at the 0.01 level (2-tailed).

4.5.2.1. Age and Gender Effects on Cybersecurity Behaviour

To provide clarity and completeness regarding the role of demographic factors, a brief examination of age and gender effects is warranted. As shown in Table 41, age demonstrated a negative correlation with risky behaviour ($r = -.379$, $p < .001$). This finding suggests that older participants within the 18-26 age range exhibited greater caution during the phishing simulation compared to their younger counterparts. Specifically, participants aged 25-26 were less likely to click on phishing links or submit personal information than those aged 18-19.

Regarding gender, the negative correlation ($r = -.298$, $p < .001$) indicates that male participants (coded as 1) engaged in less risky behaviour than female participants (coded as 2). However, as noted in Section 4.4.3, the gender results should be interpreted with caution due to quasi-complete separation, which arose from the sparse distribution of outcomes across the small 'Others' category ($n = 15$). Future research with a more balanced gender representation is needed to confirm these preliminary findings.

4.6. Summary

This chapter presented the comprehensive findings derived from a sequential quantitative research design, encompassing data from a survey and three subsequent phishing

experiments conducted with 765 participants. The data analysis adhered to a rigorous four-step process, which included data preparation and screening, descriptive analysis, exploratory analysis, and final statistical analysis. The core of the chapter focused on testing the structural relationships between various security factors and user behavioural intentions. The results of the path analysis identified several significant relationships:

Software/System Security as a Key Driver: The most consistent and powerful predictor was the Software/System Security factor. It was found to have a highly significant positive influence on Attitude ($\beta = 0.166$, $p < 0.001$\$), Subjective Norms ($\beta = 0.116$, $p < 0.001$\$), and Perceived Control ($\beta = 0.091$, $p = 0.001$\$). This suggests that perceptions of robust technology security are fundamental to shaping internal beliefs, social pressure, and perceived ease of action regarding security behaviour. While organisational Security's Influence: Organisational Security demonstrated a significant, though moderate, positive impact solely on Perceived Control ($\beta = 0.084$, $p = 0.046$\$).

Attitude Predicts Intention: The path between Attitude and Intention was found to be the strongest in the model ($\beta = 0.253$, $p < 0.001$\$), confirming the central role of an individual's positive or negative feeling toward security behaviour in predicting their actual decision to engage in that behaviour.

Notably, several hypothesised paths were found to be statistically non-significant, including all tested relationships involving Password Security, Human Security, and Social Security (when predicting Attitude or Subjective Norms). This outcome suggests that the independent security factors, aside from Software/System Security, did not directly or meaningfully influence the users' pre-intention beliefs, norms, or control over their security actions in this context. The chapter concluded with a discussion bridging these quantitative findings to provide a holistic understanding of the data.

CHAPTER 5 DISCUSSION AND RECOMMENDATION

5.1. Introduction

This chapter provides a critical analysis and interpretation of the results presented in Chapter 4, situating them within the broader scholarly landscape outlined in the literature review (Chapter 2). The primary aim of this research was to investigate the significance of cyber knowledge and behaviour on youngsters in Malaysia. The key findings, derived from two sequential quantitative phases: a closed-ended questionnaire (Phase 1) of 765 youngsters followed by a phishing simulation (Phase 2), reveal a complex and nuanced picture.

The phase one data indicates a statistically significant positive correlation ($p < 0.01$) between cyber knowledge domains and youngsters' perceived behaviour with cybersecurity. However, and crucially, the phase two data provide essential context, revealing a concomitant intention behaviour and actual behaviour with cyber attacks such as phishing attack among youngsters.

This chapter will proceed to interpret these core findings where the cyber knowledge domain-behaviour paradox and the phenomenon of actual behaviour through these four research questions:

RQ1: How do different cybersecurity knowledge domains (password, software/system, human, organisational, and social security) predict Malaysian youngsters' self-reported cybersecurity behavioural intentions?

RQ2: To what extent do the Theory of Planned Behaviour constructs (Attitude, Surrounding Pressure, and Perceived Control) mediate the relationship between cybersecurity knowledge domains and behavioural intentions among Malaysian youngsters?

RQ3: How do demographic factors (gender, age, education level) and cybersecurity knowledge domains influence actual cybersecurity behaviour, as measured by susceptibility to phishing simulations?

RQ4: What discrepancies exist between Malaysian youngsters' self-reported cybersecurity intentions and their actual behaviour when faced with a simulated phishing attack?

In addition, this chapter will proceed to synthesise these results with existing theories in the recommendation section to suggest for future research avenues.

5.2. Interpretation of Findings in Relation to Research Questions

5.2.1. Research Question 1

How do different cybersecurity knowledge domains (password, software/system, human, organisational, and social security) predict Malaysian youngsters' self-reported cybersecurity behavioural intentions?

The findings from the structural equation model (SEM) provide a clear, albeit mixed, answer to this question. The analysis reveals that not all cybersecurity knowledge domains are equally significant predictors of youngsters' self-reported behavioural intentions (YoungCCI), as first reported in Section 4.3.2.9 (Table 23) , where the overall mean score was 5.87 out of 7.

Specifically, the path analysis indicates that Software/System Security had a statistically significant, positive influence on Attitude ($\beta = .166$, $p < .001$) and Perceived Control ($\beta = .091$, $p = .001$). This construct was initially described in Section 4.3.2.2 (Table 16), where it demonstrated an overall mean score of 3.29 out of 5, indicating moderate engagement among respondents.

Organisation Security also showed a significant, though weaker, positive influence on Perceived Control (β = .084, p = .046). This implies that awareness of organisational security measures, such as alerts from an IT helpdesk, contributes to youngsters' confidence in managing cybersecurity threats.

Conversely, Password Security, Human Security, and Social Security did not demonstrate significant direct paths to the TPB constructs of Attitude, Subjective Norms, or Perceived Control in the model. The negative, non-significant path from Password Security to Attitude (β = -.021, p = .680) was particularly noteworthy, indicating that knowledge of password best practices does not necessarily translate into a more positive cybersecurity attitude within this cohort.

Therefore, in answer to RQ1, Software/System Security is the strongest positive predictor of Malaysian youngsters' self-reported cybersecurity behavioural intentions, operating through its enhancement of their Attitude and Perceived Control. The other domains, particularly Human and Social Security, which had the lowest mean scores in the descriptive analysis, show no significant predictive power in the structural model.

5.2.2. Research Question 2

To what extent do the Theory of Planned Behaviour constructs (Attitude, Surrounding Pressure, and Perceived Control) mediate the relationship between cybersecurity knowledge domains and behavioural intentions among Malaysian youngsters?

The findings strongly support the role of TPB constructs as mediators, with Attitude and Perceived Control being particularly pivotal. The model's R^2 value of 0.40 for Youngsters' Intention indicates that these three constructs collectively explain 40% of the variance in cybersecurity behavioural intentions. The path analysis clarifies their distinct roles.

Attitude was a significant and positive direct predictor of Intention ($\beta = .253$, $p < .001$). As established in RQ1, this attitude is significantly shaped by knowledge in Software/System Security. Perceived Control was the strongest direct predictor of Intention ($\beta = .533$, $p < .001$). This construct is significantly bolstered by knowledge in both Software/System Security and Organisation Security. This indicates that youngsters who feel capable of implementing security measures (e.g., updating software) and who are supported by organisational systems are far more likely to form an intention to act cautiously. Surrounding Pressure (Subjective Norms) was the only TPB construct that did not significantly predict Intention ($\beta = .046$, $p = .126$). This suggests that social influences from family and friends, while present (as shown by the moderate mean score of YoungSP), are less impactful than an individual's own attitude and sense of control in driving their cybersecurity intentions.

In summary, for RQ2, the relationship between cybersecurity knowledge domains and behavioural intentions is significantly mediated by the TPB constructs, primarily through Perceived Control and secondarily through Attitude. Knowledge influences intention not directly, but by shaping these internal psychological factors. The model confirms that what youngsters know (specifically about software and systems) enhances what they feel they can do (perceived control) and their positive evaluation of cybersecurity (attitude), which in turn drives their intention to act securely.

5.2.3. Research Question 3

How do demographic factors (gender, age, education level) and cybersecurity knowledge domains influence actual cybersecurity behaviour, as measured by susceptibility to phishing simulations?

As reported in Section 4.4.2 (Table 34), the phishing simulation revealed that 84.1% of participants (n = 406 out of 483) had no interaction with the phishing email. The demographic analysis in Section 4.4.2 (Table 11 - Table 13) showed that the sample comprised 63.3% female and 34.8% male participants, with nearly half holding a bachelor's degree (46.5%).

While cybersecurity knowledge domains like system/software security helped shape positive intentions, however, it did not warrant of who would fall for the phishing attack. Outdated software and unpatched system vulnerabilities degrade device performance, creating a frustrating user experience. For the digitally native younger generation, whose daily lives are intertwined with social media, transportation apps, and mobile-first communication, the need for secure and updated systems is not just a technical issue but a crucial social and technological requirement (Pérez-Sánchez & Palacios, 2022; Stone, 2018).

The actual behaviour was more directly influenced by demographic factors such as age, level of education, and gender. Based on the findings of this study (see Section 4.4.2, Table 34), it is not accurate to claim that all youngsters pose reckless behaviour. Rather, the data indicate that younger participants within the 18-26 age range, specifically those aged 18-19 – demonstrated higher susceptibility to phishing attacks compared to older participants aged 25-26. This finding aligns with Ali & Rahman (2025) who found that younger adults are more prone to phishing attacks due to financial strain, impulsivity, and increased receptiveness to incentives. This is primarily the reason that most of the researchers acknowledged the fact that

the need of earliest education or awareness in cybersecurity is essential (Capellan et al., 2020; Chiou et al., 2021; Fleenor, Peker, & Cutts, 2019; Yeşem & Hillary, 2020).

In addition, Table 41, age ($r = -.379$, $p < .001$) and education ($r = -.404$, $p < .001$) were negatively correlated with risky behaviour, indicating that older and more educated participants were less likely to engage with phishing emails. Gender also showed a negative correlation ($r = -.298$, $p < .001$), with male participants exhibiting less risky behaviour than female participants. However, due to quasi-complete separation (see Section 4.4.3), the gender finding should be interpreted with caution; the 'Others' category was too small for reliable estimation. Despite this, the negative correlation suggests that, in this sample, male participants were less susceptible than female participants with a finding that warrants further investigation with larger, more balanced samples.

5.2.4. Research Question 4

What discrepancies exist between Malaysian youngsters' self-reported cybersecurity intentions and their actual behaviour when faced with a simulated phishing attack?

This research question addresses the core "intention-behaviour gap." The findings reveal a critical and clear discrepancy. High Self-Reported Intentions: In Phase 1, participants reported very high levels of cyber cautiousness intention (YoungCCI mean = 5.87/7, as reported in Section 4.3.2.9, Table 23) and positive attitudes (YoungATT mean = 6.10/7, Section 4.3.2.6, Table 20). In contrast, Phase 2 revealed that, across all three experiments combined (see Section 4.4.2, Table 34), 84.1% of participants (n = 406 out of 483) ignored the phishing email entirely. Among the remaining participants, 12.4% opened the email, 2.5% clicked the link, and 1.0% submitted data. This discrepancy between high self-reported intentions and low behavioural engagement indicates that, on average, participants did not translate their positive intentions into active vigilance.

They intended to behave securely. Contrasting Actual Behaviour: In Phase 2, despite these high intentions, a portion of the cohort still engaged in risky behaviour. While other respondents were resilient, 12.4% opened the phishing email, 2.5% clicked the link, and 1.0% submitted their data, this did not manifest the intention if the majority of the participants ignored the phishing email.

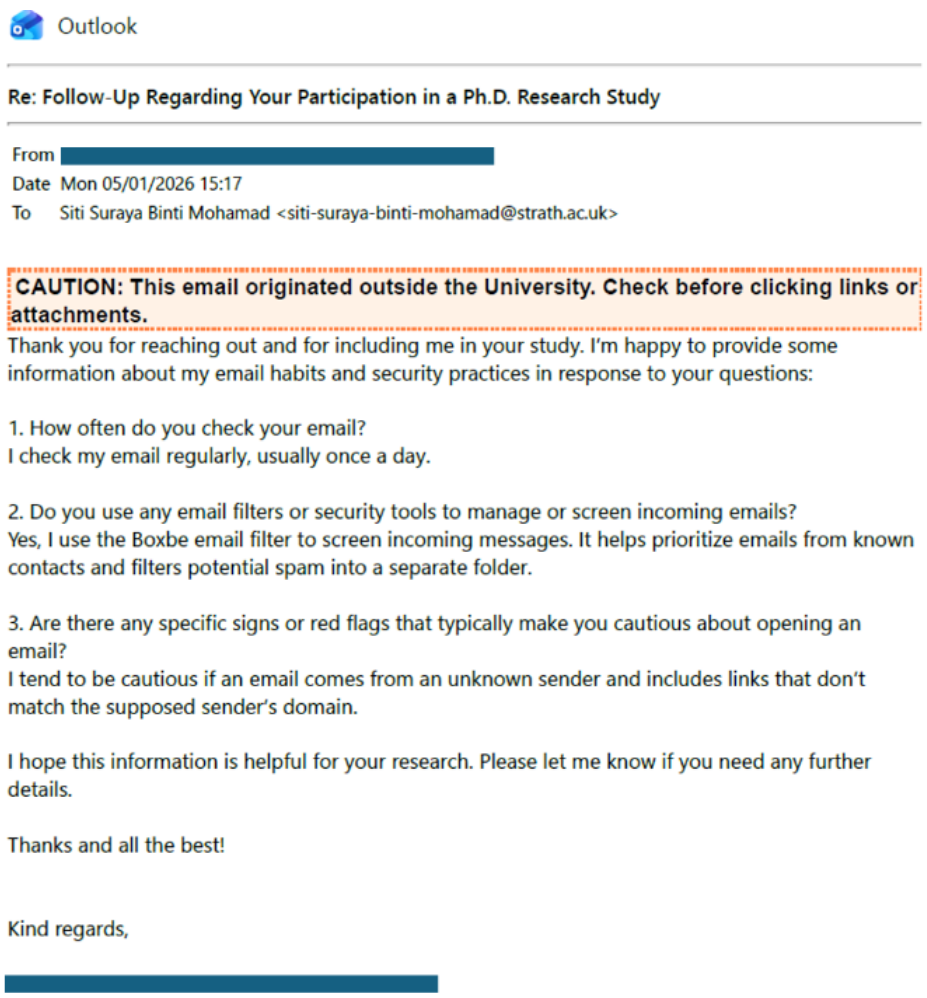
Platform-Constrained Vulnerabilities: A Discussion of Contextual Barriers to Phishing Detection and Response

One possible interpretation of the low engagement rate (84.1% no interaction) offered here as a speculative explanation rather than a quantitative finding. Is that email may not be the primary digital communication platform for many Malaysian youngsters, who increasingly favour instant messaging applications such as WhatsApp, Telegram, and Instagram. This phenomenon, which might be termed 'platform dormancy' , suggests that participants may have overlooked the phishing emails simply because they rarely check their email accounts, rather than because they actively identified the emails as malicious (Participant 1, appendix M). . the non-interaction rate itself is a meaningful finding: it suggests that passive avoidance such as ignoring suspicious emails, may be a common defence strategy among youngsters, rather than active identification of phishing cues.

However, this interpretation remains speculative and cannot be quantitatively validated with the current data. It is presented here as a potential avenue for future research rather than a definitive conclusion. Future studies should directly measure participants' primary communication platforms and email checking frequency to empirically test the 'platform dormancy' hypothesis

This observation aligns with Lee, Chern, and Azmir (2023) reports that mobile instant messaging (MIM) such as WhatsApp possesses distinct educational affordances that effectively

facilitates group, cooperative, and collaborative work. It is also said that WhatsApp is a practicable instructional strategy that enables successful study development in students (Indiran, Ismail, & Rashid, 2022).


Outlook

Re: Follow-Up Regarding Your Participation in a Ph.D. Research Study

From [redacted]
Date Mon 05/01/2026 15:17
To Siti Suraya Binti Mohamad <siti-suraya-binti-mohamad@strath.ac.uk>

CAUTION: This email originated outside the University. Check before clicking links or attachments.

Thank you for reaching out and for including me in your study. I'm happy to provide some information about my email habits and security practices in response to your questions:

1. How often do you check your email?
I check my email regularly, usually once a day.

2. Do you use any email filters or security tools to manage or screen incoming emails?
Yes, I use the Boxbe email filter to screen incoming messages. It helps prioritize emails from known contacts and filters potential spam into a separate folder.

3. Are there any specific signs or red flags that typically make you cautious about opening an email?
I tend to be cautious if an email comes from an unknown sender and includes links that don't match the supposed sender's domain.

I hope this information is helpful for your research. Please let me know if you need any further details.

Thanks and all the best!

Kind regards,

[redacted]

Figure 41 Example of participant feedback (single participant responding to three questions)

A salient insight from the qualitative email data was the participants' active reliance on automated email filtration systems. For instance, Participants 2 in Figure 41 explicitly referenced using tools like 'Boxbe', which operates to 'prioritise emails from known contacts' and sequester suspected spam, with the development of more sophisticated spam filtration systems has been growing (Magdy, Abouelseoud, & Mikhail, 2022). This practice substantiates

the key quantitative finding presented in Section 4.4, wherein Software/System Security emerged as a significant predictor of Perceived Control ($\beta = 0.091$, $p = 0.001$). The convergence of these data suggests that there is a sense of digital control among youngsters.

Thus, while participants exhibited resilience in this email-centric study, their susceptibility may be markedly higher on platforms characterised by greater habitual engagement and lower perceived risk, such as social media. This finding underscores the context-dependent nature of cybersecurity behaviours and suggests that apparent resilience may not translate across digital domains.

In the context of cybersecurity, resilience refers to an individual's ability to anticipate, withstand, recover from, and adapt to adverse cyber events such as phishing attacks, data breaches, or system compromises (Oner, Cetin, & Savas, 2025). Unlike mere awareness, which implies passive knowledge, resilience encompasses active defence behaviours, recovery from incidents, and the capacity to learn from past mistakes to strengthen future responses. In this study, resilience is operationalised as the participant's ability to resist the phishing simulation by not clicking links or submitting data.

This gap is evident when comparing the structural model with the phishing results. The model in Phase 1 showed a non-significant and negative path from Intention to actual Behaviour ($\beta = -.013$, $p = .493$). This means that the strong intentions reported in the survey did not translate into a measurable, protective effect against the real phishing attacks in the simulation. This finding is consistent with the intention-behaviour gap literature (Jenkins, Durcikova, & Nunamaker, 2021). Similarly, the negative path from Password Security to Attitude ($\beta = -0.021$) suggests that knowledge of password best practices does not necessarily translate into positive attitudes. Thematic analysis of open-ended responses provides a potential explanation for this gap. The predominant "Call for More Awareness" (36% of themes) and

mentions of "Barriers: Knowledge & Complexity" suggest that while youngsters have good intentions and some knowledge, they may lack the specific, applied skills or automatic vigilance needed to detect sophisticated phishing attempts in the moment. They know what they should do, but in a real-world scenario, this knowledge does not always manifest as correct behaviour, highlighting a deficit in situational awareness and capitalised safe practices.

5.3. Recommendations

Based on the analysis and findings, we acknowledged that it is essential to rather recommend an effective measure to closing the knowledge gap with youngsters' behaviour. The section below provides recommendations based on the relationship between cyber knowledge and behaviour.

5.3.1. Translating Early Cyber Knowledge into Lasting Security Intentions and Behaviour

Based on our findings we stated that knowledge acquisition, however comprehensive, cannot independently produce secure behavioural intentions or ensure the maintenance of long-term cybersecurity hygiene. As Damenu et al. (2025) observe, increased familiarity with ICT technologies can paradoxically lead to reduced risk perception, as children who experience the benefits of digital engagement tend to perceive these environments as less risky, fostering overconfidence and less cautious behaviour. This phenomenon aligns with broader evidence that while students may possess some cybersecurity awareness, their understanding is often superficial, resulting in a disconnect between knowledge and practice that leaves them vulnerable to online threats (Angela et al., 2025; Baraković & Baraković Husić, 2023; Cain et al., 2018; Xu & Li, 2025; Zwilling et al., 2022).

The cultivation of positive security intentions must therefore be recognised as a distinct and essential objective alongside knowledge transfer. The integration of cybersecurity

knowledge domains into early education is essential to address the critical global cyber threat. Evidence shows that visual, narrative-based curricula using accessible platforms like Scratch can effectively teach core concepts such as confidentiality, integrity, and authentication to K–12 students. Such approaches are not only engaging and comprehensible but also equitable, enabling scalable implementation across diverse socioeconomic settings (Pranathi et al., 2022). Furthermore, to improve user engagement, training must account for the difficulty of the content relative to the target group's existing knowledge base (Kuchar, Blazek, & Fujdiak, 2023). Malele (2023) demonstrate through their cloud-based cybersecurity framework for high school students that motivation is as determinant as background experience in shaping learning outcomes, with their adaptive assignments revealing that completion rates dropped when interactive tasks required sustained engagement, implying the need to reinforce interactions and motivational factors earlier in the learning process.

Similarly, research examining gamified cybersecurity education reveals that prior learning significantly contributes to increased student motivation, and that students with sustained or increased motivation exhibit positive correlations between motivation and subsequent learning outcomes (Qusa & Tarazi, 2021).

These findings establish motivation as a critical mediator between knowledge and intention behaviour. Translating this understanding into early curriculum design requires pedagogical approaches that deliberately foster intention behavioural commitment. The systematic literature review by Damenu et al. (2025) on cyber security educational games for children reveals evidence of positive learning outcomes across 91 games, yet critically identifies a lack of systematic design processes and methodological rigour in evaluating whether these outcomes translate to sustained behavioural change, with recommendation based on theory-informed game design approaches that combine bottom-up and top-down strategies to enhance educational impact from the systematic literature review by Damenu et al. (2025).

Based on these findings, the authors' recommendation for implementing gamified cybersecurity education in high schools was grounded in the observed positive correlation between motivation and learning outcomes.

Building on this, understanding specific knowledge domains, an issue debated in past studies, can significantly enhance the precision of safer cybersecurity (Qusa & Tarazi, 2021; Sharif & Ameen, 2020). The implications for early curriculum implementation across the five cybersecurity domains are clear. In password security, youngsters may learn the technical requirements of strong passwords but lack the intention to apply them consistently without motivational reinforcement that connects password practices to personal relevance.

For social security, awareness of privacy risks must be coupled with the cultivation of internalised norms around information sharing, moving beyond rule-following to positive-driven behaviour. 'Internalised norms', a finding from the thematic analysis of open-ended responses in this study (see Section 4.3.4, Table 31, and Figure 35), refer to participants' expressions of personal, self-adopted standards for cybersecurity behaviour that are not imposed by external rules or peer pressure but are genuinely accepted as personally important. For example, several participants stated that they 'personally believe' in the importance of cybersecurity, indicating internalisation rather than mere compliance.

Within organisational security, early exposure to concepts like reporting suspicious activity should be embedded peer-supported structures that normalise security-conscious behaviour as a shared responsibility.

In software security, understanding the importance of updates must be accompanied by the development of habits and routines that automate secure responses, reducing reliance on conscious intention alone. Within human security, the foundational domain encompassing cognitive resilience that the goal must be to develop not only knowledge but also the

metacognitive capacity to recognise manipulation and the motivational commitment to act on that recognition. As states, interactive platforms that move beyond passive learning by leveraging simulations of real-world digital scenarios can actively teach vital safety skills while building the confidence and motivation necessary for youngster to navigate digital environments safely (Bolun, Bulai, & Ciorbă, 2021).

Ultimately, embedding cybersecurity knowledge in early curricula is necessary but insufficient without parallel attention to the psychological and motivational mechanisms that translate knowledge into intention, and intention into consistent behaviour. The evidence presented here confirms that addressing the cybersecurity challenges facing youngsters requires a dual focus: (1) equipping them with domain-specific knowledge across all five security domains, and (2) fostering the internal motivations and peer-supported habits that transform that knowledge into resilient, self-sustaining secure behaviour

5.3.2. Mapping behaviour effects to a wider cybersecurity knowledge domain

The persistent knowledge-intention behaviour gap identified in this study underscores a fundamental limitation: Possessing cybersecurity knowledge does not automatically translate into secure behaviour. This phenomenon, often termed the "intention-behaviour gap" (Jenkins et al., 2021) or "knowing-doing gap" (Hsieh, 2025) has been extensively documented in cybersecurity research (Jenkins et al., 2021). Individuals may express strong positive intentions to follow security practices, yet these intentions frequently fail to materialise into consistent action (Ceran & Karataş, 2025). As Jenkins et al. (2021) explain, this inconsistency is particularly problematic in security contexts because a single failure to enact positive intentions, such as clicking a phishing link despite knowing the risks, could compromise an entire system. The presence of competing intentions, such as desire to minimise effort or complete tasks efficiently, often moderates and weakens the relationship between good intentions and actual security behaviour. Consequently, fostering genuine behavioural change

requires more than simply imparting cybersecurity knowledge; it necessitates cultivating strong and resilient security intentions that can withstand competing demands.

van Schaik & Renaud (2025) introduce Cognitive Dissonance Theory (CDT) to explain the failure to close the “knowledge-gap”. As such that when new security information contradicts a user's existing habits or beliefs, the resulting psychological discomfort (dissonance) can cause them to reject the new knowledge rather than change their behaviour. Thus, CDT is presented not as a tool for knowledge transfer, but as a critical barrier that must be understood and mitigated to foster genuine behavioural change. To add a similar point, hardiness personality traits; a personality construct characterised by commitment (viewing life events as interesting and meaningful), control (believing one can influence events through one's actions), and challenge (viewing change as an opportunity for growth rather than a threat), established habits may precipitate automated cognitive and behavioural responses, thus, to advance the behaviour will promote the likelihood of better understanding in cyber knowledge domain (Aigbefo et al., 2022). A complementary perspective is that the conceptualization and measurement of the security mindset (Holley, Garcia, & Bernd, 2023) as a malleable behavioural construct.

The analysis in this study reveals that merely assuming an investigation for parallel development between cyber knowledge domains and behavioural outcomes will not resolve security deficiencies, that prolonged cyber knowledge-intention behaviour gap requires a two-pronged approach, which is to harden technical control while at the same time sharpen human skills. These two must operate in synergy, for instance, providing phishing awareness training coupled with training for advanced email filtering, which both translate into consistent security practices.

5.3.3. Establishing effective techniques for training youngsters

In context, since we saw the tension between passive disengagement (missing the email) and an informed, and active defence (identifying the phishing attempt), it is crucial that the need for training that specifically drills youngsters on deception detection confidence such as dark patterns, and reporting efficacy such as knowing how to verify, report, or escalate a threat. Techniques used in phishing simulation play a pivotal role in maintaining effectivity of awareness, especially when we want to attract youngsters to be more resilient in cyberspace (Wright, Johnson, & Kitchens, 2023). Effective training has been proved to be effective in condition with gamification elements such as progress mechanics, player controls, problem solving, and an attachment story (Adams & Makramalla, 2015). Adams & Makramalla (2015) explained further of progress mechanics refer to visual or symbolic indicators of a user's advancement through a training programme, such as experience points (XP), level bars, achievement badges, or completion percentages. These mechanics provide learners with a clear sense of accomplishment and motivate continued engagement. An example from cybersecurity training is a phishing simulation that awards points for correctly identifying suspicious emails and displays a progress bar toward the next 'security awareness level.

Consequently, the results advocate for a strategic pivot in delivery channels from ineffective email to more integrated platforms. For Malaysian youngsters, embedding cybersecurity awareness within WhatsApp, a cornerstone of their digital communication practices, is proposed as a critical intervention to bridge the engagement gap. Moreover, the mode of delivery is of equal significance to the content. This investigation demonstrates that, for Malaysian youngsters, email is progressively less efficacious as a principal medium for awareness training, Farooq et al. (2024) and Zaharon, Ali, and Hasnan (2021) recommended the need for continuous education on evolving phishing tactics, as phishing or other social

engineering techniques will remain a persistent factor influencing how individuals interact on the internet (Xu & Rajivan, 2023).

In addition, to cultivate practical resilience, training should be expanded to include hands-on competencies to youngsters. This includes instructing youngsters on the proactive use of spam filters to detect and mitigate phishing attempts (Sarno, Gendron, & Volante, 2025). Technique reported by respondents in this study (see Figure 41) as a simple yet effective layer of defence, hence, training to strengthen email filtering systems as a foundational layer of defence represents a significant, scalable contribution to active deception detection (Mahalakshmi et al., 2025). Furthermore, programs should be designed to foster positive behavioural control, empowering users with clear, actionable steps for secure cyber practices rather than merely listing prohibitions. This shift from passive awareness to active skill-building is essential for translating knowledge into habitual, secure behaviour.

5.3.4. Updated Awareness from Agencies

Any organisations, be it from the government to private agencies must ensure that they have an updated requirement when they want to provide cybersecurity awareness. In Malaysia, the government agency for cybersecurity under The Ministry of Digital still uses an old password standard information poster that includes the statement to “Create password that have at least 8 characters with numbers and symbols” or “Change your password regularly, at least once every 3 months”, which has been outdated since 2017 as in Figure 42.

Figure 42: Poster from CyberSecurity Malaysia on Safe Password Guideline (CyberSecurity Malaysia, 2024, p. 1)

Based on NIST 800-63B an updated approach eliminated the complexity rules over technological augmentations such as password managers and robust multi-factor authentication (MFA), shifting focus from user-borne complexity to systemic defences against modern authentication threats (Temoshok et al., 2025).

Whereas in our research, we learned that the use of the most updated guideline will benefit the people in cyberspace, the critical infrastructures, and agencies be it from the public to private sector. We learnt the lesson with outdated data practices, which has been discussed in 2.6.

5.4. Summary

This chapter has provided a critical interpretation and discussion of the research findings, situating them within the context of the study's objectives and the broader theoretical framework. The analysis, grounded in the sequential quantitative data from Chapter 4, reveals a complex picture of cybersecurity awareness and practice among Malaysian youngsters. The core findings can be summarised as follows.

The relationship between each research question and its corresponding hypotheses is summarised below. **RQ1** (How do different cybersecurity knowledge domains predict self-reported behavioural intentions?) was addressed by hypotheses H6a–H6e (knowledge domains → Attitude), H7a–H7e (knowledge domains → Subjective Norms), and H8a–H8e (knowledge domains → Perceived Control). The results showed partial support: only Software/System Security significantly predicted Attitude (H6b), Subjective Norms (H7b), and Perceived Control (H8b), while Organisation Security significantly predicted Perceived Control (H8d). All other knowledge domain paths were not supported.

RQ2 (To what extent do the Theory of Planned Behaviour constructs mediate the relationship between knowledge domains and behavioural intentions?) was addressed by H1 (Attitude → Intention), H2 (Subjective Norms → Intention), and H3 (Perceived Control → Intention). The findings supported H1 and H3, confirming that Attitude and Perceived Control are significant predictors of behavioural intention. However, H2 was not supported, indicating that Subjective Norms (social pressure) did not significantly influence intention in this cohort.

RQ3 (How do demographic factors and cybersecurity knowledge domains influence actual cybersecurity behaviour?) was addressed by H4 (Perceived Control → Behaviour), H5 (Intention → Behaviour), and H9 (demographics → behaviour). The results supported H9, confirming that age, gender, and education level correlated with reduced risky behaviour.

However, H4 and H5 were not supported, indicating that neither perceived control nor intention significantly predicted actual phishing susceptibility.

RQ4 (What discrepancies exist between self-reported intentions and actual behaviour?) was addressed by comparing the survey results (Phase 1) with the phishing simulation outcomes (Phase 2). The key finding was a substantial intention-behaviour gap: despite high self-reported intentions (YoungCCI mean = 5.87/7), 84.1% of participants had no interaction with the phishing email, and among those who did engage, some clicked links or submitted data. This discrepancy suggests that intentions alone do not reliably translate into secure behaviour when individuals face a simulated phishing attack.

Collectively, these findings point to a "cyber knowledge domain-behaviour paradox": while youngsters possess varying levels of knowledge and strong intentions, this does not reliably translate into resilient real-world behaviour, particularly against social engineering attacks like phishing. The recommendations put forward from early education and updated awareness campaigns to engaging training techniques.

The next chapter will conclude the thesis by presenting an overview of the key findings, contributions of the study, future research, limitations of the study, and recommendations for future research.

CHAPTER 6 CONCLUSION

Our main findings can be summarised as: a) cyber knowledge has 5 specific domains called password security, software/system security, human security, organisation security, and social security and analysis shows specific domain is significant to youngster's behaviour in safe cyber practice; b) attitude, social pressure and perceived control have a significant impact on cyber intentions; and c) demographics. Therefore, mitigation strategies need to target these specific areas.

6.1. Research Limitations

Although this study had strengths, such as its depth of insights from 765 participants from a survey, it also had some limitations. Limitation included: the cohort of the study (ages 18-26), the high risk of a sampling bias from convenience sampling and access issues with phishing simulation campaigns.

First, the study focused specifically on youngsters aged 18-26 years. This strategic focus was initially justified by an identified research gap pertaining to this population segment within the Malaysian context, where individuals in this age range are transitioning from education to employment (or higher education). The examiner raises a valid point: this is not necessarily a limitation of external validity but rather a deliberate boundary condition of the study. The findings are representative of this specific age subsection and should not be generalised to older adults or younger adolescents without further research. Future studies should extend the age range to enable comparative analyses.

Second, the adoption of a convenience sampling strategy in Phase 1 was pragmatically necessary to facilitate participant recruitment via social media and collaborations with local universities and colleges. While this approach benefited the research by enabling access to a large and diverse sample (N = 765), it inherently carries a heightened risk of sampling bias.

This methodological choice may systematically underrepresent populations with limited digital connectivity or internet access. To mitigate this constraint, demographic variations within the sample were critically examined, and Phase 2 employed a stratified random sampling technique to validate the initial findings. Although this approach was pragmatically necessary to facilitate participant recruitment, it inherently carries a heightened risk of sampling bias (Golzar, Noor, & Tajik, 2022).

Lastly, our third limitation of this study was encountered during the execution of the phishing simulation campaign. At first this research developed a website, initially to simulate a legitimate phishing attack on the participants. The initial methodology involved deploying a simulated phishing website, developed using Wix.com, accompanied by a corresponding domain email address. However, this platform was persistently flagged (Figure 43), as we developed three different website and domain addresses to mimic legitimate phishing attack and deactivated by automated security systems within 48 hours of deployment (Figure 44).

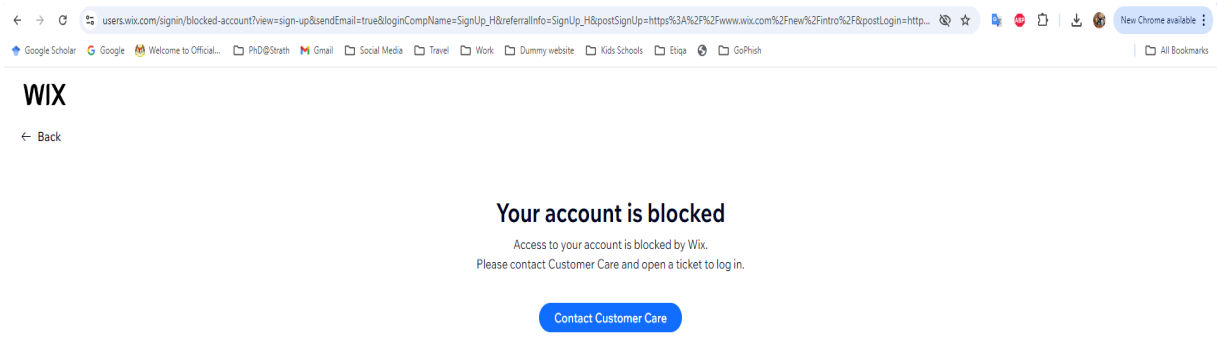


Figure 43 Flagged for phishing activity

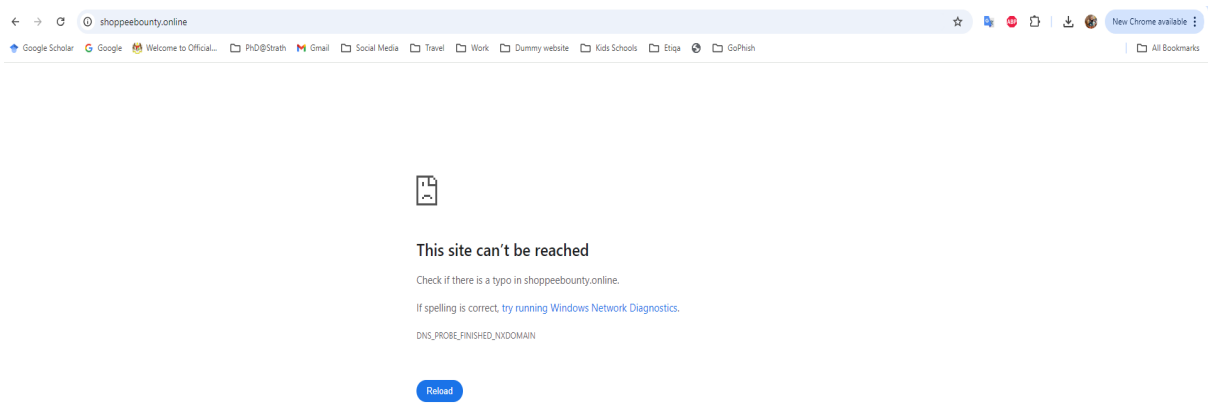


Figure 44 Website cannot be reached

Consequently, an alternative approach was necessitated, utilising the PhishMe phishing toolkit (see Figure 26, pg.95). This adaptation resulted in a simulation that was potentially less sophisticated than intended, as it precluded the use of a custom domain, potentially making the phishing emails more discernible to participants. Despite this challenge, the campaign was successfully administered across three iterations, each incorporating recognised phishing cues.

6.2. Theoretical Contributions

This study makes three primary theoretical contributions:

a) **Domain-specific knowledge framework**: The research moves beyond treating 'cybersecurity knowledge' as a monolithic construct by proposing and validating a multi-domain knowledge framework encompassing Password, Software/System, Human, Organisational, and Social Security.

b) **Identification of the most potent predictors**: The findings reveal that Software/System Security and Organisational Security were the most significant positive predictors of behavioural intentions, operating through their influence on Attitude and Perceived Control (see Section 4.5.1, Table 40).

c) **Demographic moderation**: Among demographic factors, educational level (rather than age or gender) emerged as the most significant moderator, with higher education correlating with both greater knowledge and, paradoxically, higher susceptibility to sophisticated phishing attempts in some cases (see Section 4.5.2, Table 41).

6.3. Methodological Contribution

From a methodological standpoint, this research makes a significant contribution through its sequential mixed-methods design. The integration of a large-scale quantitative survey (N=765) with a controlled phishing simulation (N=483) sets a rigorous precedent for measuring cybersecurity behaviour. This approach overcomes the limitations of reliance on self-reported data, which is often plagued by social desirability bias, by providing an objective behavioural outcome measure.

While the TPB has been widely applied in cybersecurity contexts, this research provides a nuanced understanding of the specific mediating roles of its constructs: Attitude, Subjective Norms, and Perceived Control within a non-Western, youngster-centric sample. The findings clarify which TPB constructs are most influential (Perceived Control and Attitude) and which are not (Subjective Norms) in predicting cybersecurity intentions among Malaysian youngsters.

6.4. Practical and Policy Contributions

The practical implications of this research are immediate and substantial. For cybersecurity educators and awareness campaigns in Malaysia and similar contexts, the findings provide an evidence-based roadmap for intervention. The identified weakness in Human and Social Security knowledge domains dictates a strategic pivot in awareness content, moving beyond technical advice towards critical thinking, social engineering recognition, and

psychological resilience training. The findings argue for a pivot in cybersecurity awareness strategies while moving away from generic, one-size-fits-all training towards targeted, experiential, and simulation-based approaches integrated into educational curricula.

For policymakers, particularly agencies like CyberSecurity Malaysia and the Ministry of Education, the study offers a critical, evidence-based assessment of current initiatives. The finding that outdated password guidelines are still being promoted serves as a direct call to action for the systematic updating of national cybersecurity resources based on international best practices (e.g., NIST guidelines). The strong theme from the qualitative data calling for more awareness, coupled with the empirical evidence of knowledge gaps, provides a powerful mandate for increasing investment and refining the targeting of national cybersecurity education programmes, suggesting they should be embedded "at the earliest curriculum" as highlighted in the discussion in chapter 5.

Finally, by identifying that demographic factors are poor predictors of behaviour compared to knowledge and psychological constructs, the research argues for a move away from demographic stereotypes in cybersecurity profiling. This suggests that resources should be focused on universal, knowledge-based interventions that are accessible to all youngsters, regardless of gender or educational background, while being sophisticated enough to address the specific psychological barriers identified.

6.5. Future Work

This research provides a clear and valuable roadmap for subsequent research by: utilise secure, institutional-grade platforms to develop more ecologically-valid and sophisticated phishing models that avoid premature takedowns, expand its demographic and geographic scope, investigating the human-technical interplay in deception detection, and applying multi-method approaches to provide deeper explanatory power.

A key focus for future endeavours is to augment the methodological rigour of phishing simulations. Future research may employ safe, institutional-grade systems, potentially established in partnership with government entities like CyberSecurity Malaysia and the Malaysian Communications and Multimedia Commission (MCMC). Such collaborations would enable the development of more ecologically valid and advanced phishing models that are ethically implemented and shielded against premature takedowns, thereby maintaining their research integrity.

The term 'ecologically valid' refers to the degree to which research findings can be generalised to real-world settings. In the context of phishing simulations, an ecologically valid design would closely mirror actual phishing attacks that users encounter in their daily lives including realistic sender addresses, convincing website clones, and authentic urgency cues, rather than simplified or easily identifiable fake emails.

'Premature takedowns' refer to the automated or manual removal of simulated phishing websites by security services, hosting providers, or browsers before the research data collection is complete. As noted in Section 6.4 (Research Limitations) and illustrated in Figure 43 and Figure 44 (pg. 177), three different websites developed for this study were deactivated by automated security systems within 48 hours of deployment. This disrupted the research and necessitated an alternative approach using the GoPhish toolkit.

Furthermore, the finding in Figure 41, pg. 161 suggest an investigation for future research in the interplay between automated technical controls and active human deception detection. Future studies should examine how improved email filtering systems, to reduce the 'noise' of low-effort phishing attempts, impact a user's ability to engage with and accurately identify sophisticated scams. In addition, beyond deception detection, research is needed to evaluate the reporting behaviours of youngsters, whether they know how to alert the authorities as discussed in 2.7, and their capability in recovery efficacy if they clicked on a link. It is hypothesised that by minimising exposure to crude attacks, strengthening email filtering systems could allow users to focus cognitive resources on more deceptive campaigns, thereby making active deception detection a more measurable and reliable behavioural outcome for executing proper incident response protocols. This delineates the respective and complementary roles of technological and human resilience in a layered defence strategy.

To improve the generalisability of these findings, subsequent studies should broaden the demographic and geographic scope. Utilising stratified random sampling to encompass a wider range of age groups, socioeconomic status, and digital literacy levels would enable comparative analyses to ascertain whether the factors influencing phishing susceptibility are exclusive to a youngster demographic or prevalent across the entire population. Extending this research to different cultural and national contexts might help disentangle culturally unique behaviours from universal cognitive security risks. Specifically, specialised study is needed on populations systematically underrepresented in cybersecurity studies, such as persons with poor internet connectivity, to build equitable and comprehensive public cybersecurity policy.

Beyond these immediate extensions, embracing multi-method techniques would provide deeper explanatory power. Integrating qualitative methodologies, such as in-depth interviews following simulations, could reveal the cognitive and behavioural rationale underlying participants' behaviours, expanding beyond what they did to explain why.

Ultimately, a combination of more realistic simulations, diverse and representative sampling, and mixed-method designs will be critical for furthering a holistic understanding of phishing vulnerability and for designing more effective countermeasures.

6.6. In Summary

Mapping the Personal Landscape: Development and Growth in Academia

The completion of this thesis marks a significant transformation in my professional trajectory, representing a deliberate pivot from a seven-year career in the cybersecurity industry to the academic research. This academic path was initiated by industry gained from analysing phishing campaigns deployed during my professional experience. The experience uncovered a clear imperative for a future-proof Malaysia's digital security, moving beyond immediate defence mechanisms to build a robust, research-informed foundation. Undertaking a PhD was thus a strategic commitment to bridge the critical gap between industry practice and scholarly inquiry, equipping myself to contribute at a more systemic level to the nation's cyber resilience.

This academic passage was navigated alongside considerable personal and professional responsibilities, including early parenthood and a full-time role in the financial sector. This confluence of roles, while challenging, proved to be a profound catalyst for growth. It necessitated the development of advanced skills in rigorous time management, strategic prioritisation, and resilient project execution. More significantly, it forged a unique scholarly identity, one that synthesises the pragmatic, problem-solving orientation of an industry practitioner with the methodological discipline and theoretical depth required of a researcher.

The experience of balancing these multifaceted responsibilities has also generated a vital intellectual insight: the great significance of broadening the academic landscape. The route of a practitioner-researcher, while frequently complicated, brings vital views that can strengthen the relevance and effectiveness of cybersecurity studies. By describing this journey,

this thesis contributes to a broader discourse on cultivating diversity within academia, advocating for frameworks that support non-linear pathways and the integration of professional skills. Ultimately, this process has not only resulted in a corpus of research but has also fundamentally influenced my capacity to serve as a bridge between industry and academia, dedicated to bolstering Malaysia's cybersecurity landscape for the future.

References

Abadla, R., Alseiari, A., Alheili, A., Daoud, M. S., & Al-Mimi, H. M. (2023). Intelligent Phishing Email Detection with Multi-Feature Analysis (IPED-MFA). *Paper presented at the International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS)*, Valencia, Spain.

Abdullah, A. S., & Mohd, M. (2019, 25-26 September). Spear Phishing Simulation in Critical Sector: Telecommunication and Defense Sub-sector. *Paper presented at the International Conference on Cybersecurity (ICoCSec)*, Negeri Sembilan, Malaysia.

Abdullah, F., Mohamad, N. S., & Yunos, Z. (2018). Safeguarding Malaysia's Cyberspace Against Cyber Threats: Contributions by Cybersecurity Malaysia. *OIC-CERT Journal of Cyber Security,* 1(1), 22-31.

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. *IEEE Access,* 9, 44928-44949. doi: 10.1109/access.2021.3066383

Abu-Nimeh, S. (2009). Chapter 6 - Phishing, SMishing, and Vishing. In K. Dunham (Ed.), *Mobile Malware Attacks and Defense* (1 ed., pp. 125-196). Boston: Syngress

Ackerman, P. (2021). Different Types of Cybersecurity Assessments. In (pp. 2-3). Retrieved from https://app-knovel-com.proxy.lib.strath.ac.uk/kn/resources/kt013H0P53/kpICEICS03/pdf

Adams, M., & Makramalla, M. (2015). Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. *Technology Innovation Management Review,* 5(1), 5-14. doi: 10.22215/timreview861

Adebowale, O. O., Adenubi, O. T., Adesokan, H. K., Oloye, A. A., Bankole, N. O., Fadipe, O. E., AyoAjayi, P. O., & Akinloye, A. K. (2021). SARS-CoV-2 (COVID-19 pandemic) in Nigeria: Multi-institutional survey of knowledge, practices and perception amongst undergraduate veterinary medical students. *Public Library of Science (PLoS) One,* 16, e0248189. doi: 10.1371/journal.pone.0248189

Ahmad, N., Mokhtar, U. A., Fauzi, W. F. P., Othman, Z. A., Yeop, Y. H., & Abdullah, S. N. H. S. (2018, 13-15 November). Cyber Security Situational Awareness among Parents. *Paper presented at the Cyber Resilience Conference (CRC)*, Putrajaya, Malaysia.

Ahmead, M., El Sharif, N., & Abuiram, I. (2024). Risky Online Behaviors and Cybercrime Awareness Among Undergraduate Students At Al Quds University: A Cross-Sectional Study. *Crime Science,* 13(1), 29-19. doi: 10.1186/s40163-024-00230-w

Ahmetoglu, H., & Das, R. (2022). A Comprehensive Review on Detection of Cyber-Attacks: Data Sets, Methods, Challenges, And Future Research Directions. *Internet of Things,* 20, 100615. doi: 10.1016/j.iot.2022.100615

Aigbefo, Q. A., Blount, Y., & Marrone, M. (2022). The Influence of Hardiness and Habit on Security Behaviour Intention. *Behaviour & Information Technology,* 41(6), 1151-1170. doi: 10.1080/0144929x.2020.1856928

Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. In J. Kuhl & J. Beckmann (Eds.), *Action-Control: From Cognition to Behavior* (Third ed., pp. 11-39). New York: Springer

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes,* 50(2), 179-211. doi: 10.1016/0749-5978(91)90020-T

Ajzen, I. (2005). Attitudes, Personality and Behaviour: Open University Press.

Ajzen, I. (Producer). (2019). Theory of Planned Behavior Diagram. Retrieved from https://people.umass.edu/aizen/tpb.diag.html, Date Accessed 12 April 2022

Ajzen, I. (2024). Theory of Reasoned Action. Retrieved from https://people.umass.edu/aizen/tra.html, Date Accessed 17 November 2024

Akande, O. N., Gbenle, O., Abikoye, O. C., Jimoh, R. G., Akande, H. B., Balogun, A. O., & Fatokun, A. (2023). SMSPROTECT: An Automatic Smishing Detection Mobile Application. *ICT Express,* 9(2), 168-176. doi: 10.1016/j.icte.2022.05.009

Akati, J., & Conrad, M. (2021). Anti-Tailgating Solution Using Biometric Authentication, Motion Sensors and Image Recognition. *Paper presented at the 2021 International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Cloud and Big Data Computing, International Conference on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, Falerna, Italy.

Akhyari, N., Abdullah, A. R., & Rashid, A. H. M. (2018). The Significance of Main Constructs of Theory of Planned Behavior in Recent Information Security Policy Compliance Behavior Study: A Comparison Among Top Three Behavioral Theories. *International Journal of Engineering and Technology,* 7(2.29), 737-741. doi: 10.14419/ijet.v7i2.29.14008

Akther, T., & Nur, T. (2022). A model of factors influencing COVID-19 vaccine acceptance: A synthesis of the theory of reasoned action, conspiracy theory belief, awareness, perceived usefulness, and perceived ease of use. *Public Library of Science (PLoS) One,* 17(1), e0261869-e0261869. doi: 10.1371/journal.pone.0261869

Al-Hodiany, Z. M. (2023). Review on the Social Media Management Techniques Against Kids Harmful Information. In W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, & A. Emara (Eds.), *Kids Cybersecurity Using Computational Intelligence Techniques* (Vol. 1080, pp. 51-67). Cham: Springer International Publishing. Retrieved from 10.1007/978-3-031-21199-7_4

Al-Husseini, S. J. (2023). Social capital and individual motivations for information sharing: A theory of reasoned action perspective. *Journal of Information Science,* 49(6), 1493-1505. doi: 10.1177/01655515211060532

Al-Saggaf, Y., & Maclean, J. (2024). Smartphone Privacy and Cyber Safety among Australian Adolescents: Gender Differences. *Information (Basel),* 15. doi: 10.3390/info15100604

Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet,* 12(10), 168. doi: 10.3390/fi12100168

Albladi, S. M., & Weir, G. R. S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity,* 3(1), 1-19. doi: 10.1186/s42400-020-00047-5

Aldawood, H., & Skinner, G. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet,* 11(3), 73. doi: 10.3390/fi11030073

Alexei, A., & Alexei, A. (2023). The Difference Between Cyber Security Vs. Information Security. *Journal of Engineering Science (Chişinău),* 29(4), 72-83. doi: 10.52326/jes.utm.2022.29(4).08

Ali, A. N. B. M., & Rahman, S. H. A. (2025). Analyzing Cybersecurity Risk with a Phishing Simulation Website. *Paper presented at the Proceedings of the 2024 9th International Conference on Cloud Computing and Internet of Things*, Hanoi, Vietnam.

Alqahtani, S. I., Yafooz, W. M. S., Alsaeedi, A., Syed, L., & Alluhaibi, R. (2023). Children's Safety on YouTube: A Systematic Review. *Applied Sciences,* 13. doi: 10.3390/app13064044

Althobaiti, K., & Alsufyani, N. (2024). A review of organization-oriented phishing research. *PeerJ Computer Science,* 10, 1-44. doi: 10.7717/peerj-cs.2487

Alzahrani, K., Hall-Phillips, A., & Zeng, A. Z. (2019). Applying the theory of reasoned action to understanding consumers' intention to adopt hybrid electric vehicles in Saudi Arabia. *Transportation,* 46(1), 199-215. doi: 10.1007/s11116-017-9801-3

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly,* 34(3), 613-643. doi: 10.2307/25750694

Angela, S., Huda, M. M., & Rusdiyan, R. D. (2025). Analysis of Cybersecurity Awareness Among Social Media Users Among Teenagers Using Exploratory Factor Analysis (EFA) & Confirmatory Factor Analysis (CFA) Methods. *Journal of Electrical Engineering and Computer,* 7(2), 301-311. doi: 10.33650/jeecom.v7i2.11407

ANSecurity. (2025). Healthcare Disruption: NHS Scotland Hit. *Latest UK cyber attacks: A wake-up call for 2025.* Retrieved from https://www.ansecurity.com/latest-uk-cyber-attacks-a-wake-up-call-for-2025/, Date Accessed 12 July 2025

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior,* 69, 437-443. doi: 10.1016/j.chb.2016.12.040

Anwar, M. J., Ali, S. M., Leghari, M. A., & Tariq, J. (2015). *Oral Hygiene Knowledge and Source of Information Among 12 To 16 Years' Old Karachi School Children* (10128700). Retrieved from https://link.gale.com/apps/doc/A423411891/AONE Date Accessed 17 March 2025

Ariffin, M. R. K., & Letchumanan, M. (2020). Status of Cybersecurity Awareness Level in Malaysia. In K. Daimi & G. Francia Iii (Eds.), *Innovations in Cybersecurity Education* (pp. 343-359). doi:10.1007/978-3-030-50244-7_17

Ashfaq, S., Chandre, P., Pathan, S., Mande, U., Nimbalkar, M., & Mahalle, P. (2024). Defending Against Vishing Attacks: A Comprehensive Review for Prevention and Mitigation Techniques. *Paper presented at the Cyber Security and Digital Forensics 2024*, Singapore.

Askew, K., Buckner, J. E., Taing, M. U., Ilie, A., Bauer, J. A., & Coovert, M. D. (2019). Erratum to "Explaining Cyberloafing: The Role of the Theory of Planned Behavior" [Computers in Human Behavior 36C 510–519]. *Computers in Human Behavior,* 90, 284. doi: 10.1016/j.chb.2018.09.019

Athena Information Solutions. (2022). Unifi Business Suite now includes eCommerce hub, cloud storage, and cyber security. *Communications Today*. https://www.proquest.com/trade-journals/unifi-business-suite-now-includes-ecommerce-hub/docview/2653327841/se-2, Date Accessed 13 November 2024

Awuah, A. G., & Hayfron-Acquah, J. B. (2022). QR Code security: mitigating the issue of quishing (QR Code Phishing). *International Journal of Computer Applications,* 184(33), 34-39. doi: 10.5120/ijca2022922425

Azmin, H., & Serota, E. (2024). How Malaysia is regulating the rise in cybersecurity threats. Retrieved from FTI Consulting Strategic Communication website: https://fticommunications.com/how-malaysia-is-regulating-the-rise-in-cybersecurity-threats/, Date Accessed July 29,2024

Babbie, E. R. (2008). The Basics of Social Research (4th [International Student Edition] ed.). Belmont, California: Thomson/Wadsworth.

Bailar, B. A., & Lanphier, C. M. (1978). Pilot-Study to Develop Survey Methods to Assess Survey Practices. *The American Statistician,* 32(4), 130-132. doi: 10.2307/2682939

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security,* 1(2), 176-198. doi: 10.1017/eis.2016.8

Bank, D. (2005, August 17). 'Spear Phishing' Tests Educate People About Online Scams. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/SB112424042313615131. Date Accessed 12 June 2025

Baraković, S., & Baraković Husić, J. (2023). Cyber Hygiene Knowledge, Awareness, And Behavioural Practices of University Students. *Information Security Journal: A Global Perspective,* 32(5), 347-370. doi: 10.1080/19393555.2022.2088428

Barbera, J., Naibert, N., Komperda, R., & Pentecost, T. C. (2021). Clarity on Cronbach's Alpha Use. *Journal of Chemical Education,* 98(2), 257-258. doi: 10.1021/acs.jchemed.0c00183

Bareja, D. O. (2021). By Failing to Prepare, You Are Preparing to Fail. In A. Bhardwaj & V. Sapra (Eds.), *Security Incidents & Response Against Cyber Attacks* (pp. 13-29). Cham: Springer International Publishing. Retrieved from 10.1007/978-3-030-69174-5_1

Barela, J., Gasiba, T. E., Suppan, S. R., Berges, M., & Beckers, K. (2019, 23-27 September). When Interactive Graphic Storytelling Fails. *Paper presented at the 27th International Requirements Engineering Conference Workshops (REW)*, Jeju Island, South Korea.

Bauer, S., & Bernroider, E. W. N. (2017). From Information Security Awareness to Reasoned Compliant Action: Analyzing Information Security Policy Compliance in a Large Banking Organization. *Association for Computing Machinary for Advances in Information Systems,* 48(SIGMIS Database), 44–68. doi: 10.1145/3130515.3130519

Bawaba, A. (2014). Malaysia,Sri Lanka : DIALOG AXIATA flourishes ICT infrastructure through US $115m investment. *MENA Report*. Retrieved from https://link.gale.com/apps/doc/A363540870/AONE. Date Accessed 3 November 2025

Baxter, R. J. (2016). Applying Basic Gamification Techniques to IT Compliance Training: Evidence from the Lab and Field. *Journal of Information Systems,* 30(3), 119-134. doi: 10.2308/isys-51341

Beach, D. A. (1989). Identifying the Random Responder. *Journal of Psychology,* 123(1), 101-103. doi: 10.1080/00223980.1989.10542966

Bello, M. B., Ahmad, B. A., Auwal, M. N., & Jamal, F. (2025). Emerging Trends in Phishing: A Look at Smishing, Vishing, Quishing. *International Journal of Technology Emerging Research,* 1, 274-289. doi: 10.64823/ijter.2503033

Bentler, P. M. (1990). Comparative fit indexes in structural models. *Psychological Bulletin,* 107(2), 238-246. doi: 10.1037/0033-2909.107.2.238

Bernama. (2024). Dewan Negara passes Cyber Security Bill 2024. https://api.nst.com.my/news/nation/2024/04/1034050/dewan-negara-passes-cyber-security-bill-2024, Date Accessed 28 July 2024

Beskow, D. M., & Carley, K. M. (2019). Social Cybersecurity: An Emerging National Security Requirement. *Military Review, 99,* 117-127.

Bhanderi, D., Kavathiya, M., Bhut, T., Kaur, H., & Mehta, M. (2023, 15-17 March). Impact of Two-Factor Authentication on User Convenience and Security. *Paper presented at the 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India.

Blancaflor, E. B., Abaleta, R. M., Achacoso, L. M. D. L., Amper, A. C. C., & Ampiloquio, P. I. R. (2025). Emerging Threat: The Use of AI Voice Cloning Software and Services to Deceive Victims Through Phone Conversations and its Potential Effects on the Filipino Population. *Paper presented at the Proceeding of the 2024 5th Asia Service Sciences and Software Engineering Conference*, Tokyo, Japan.

Blancaflor, E. B., Alfonso, A. B., Banganay, K. N. U., Cruz, G. A. B. D., Fernandez, K. E., & Santos, S. A. M. (2021, 7-10 March). Let's Go Phishing: A Phishing Awareness Campaign Using Smishing, Email Phishing, and Social Media Phishing Tools. *Paper presented at the Proceedings of the 11th Annual International Conference on Industrial Engineering and Operations Management*, Singapore.

Boise State University. (2025, 15 October). Boise State University : Stay alert to 'quishing' and other threats during National Cybersecurity Awareness Month. *News Bites - Private Companies*. Retrieved from https://www.proquest.com/wire-feeds/boise-state-university-stay-alert-quishing-other/docview/3260778099/se-2?accountid=14116. Date Accessed 17 December 2025

Bolun, I., Bulai, R., & Ciorbă, D. (2021). Support of Education in Cybersecurity. *Pro Publico Bono - Magyar Kozigazgatas,* (1), 128-147. doi: 10.32575/ppb.2021.1.8

Bonneau, J. (2012, 20-23 May). The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. *Paper presented at the Symposium on Security and Privacy*, San Francisco, USA.

Bonsaksen, T., Kleppang, A. L., & Steigen, A. M. (2024). Cyberbullying Among Adolescents in Norway: Time Trends and Factors Associated with Perpetration and Victimization. *Behavioral Sciences, 14*. 10.3390/bs14111043, Date Accessed 8 December 2025

Bordonaba-Juste, M. V. (2020). Generational differences in valuing usefulness, privacy and security negative experiences for paying for cloud services. *Information Systems & e-Business Management,* 18(1), 35-61. doi: 10.1007/s10257-020-00462-8

Bossauer, P., Neifer, T., Stevens, G., & Pakusch, C. (2020). Trust versus privacy: Using connected car data in peer-to-peer carsharing. *Paper presented at the Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, Honolulu, Hawai'i, USA.

Boulton, C. (2016, 1 December 2021). Whaling emerges as major cybersecurity threat. *Business And Economics-Computer Applications*. Retrieved from https://www.proquest.com/trade-journals/whaling-emerges-as-major-cybersecurity-threat/docview/1783205110/se-2?accountid=14116. Date Accessed 7 October 2024

Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring Age and Gender Differences in ICT Cybersecurity Behaviour. *Human Behavior and Emerging Technologies,* 2022(1), 2693080. doi: 10.1155/2022/2693080

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology,* 3(2), 77-101. doi: 10.1191/1478088706qp063oa

Brewer, J., & Hunter, A. (1989). Multimethod Research: A Synthesis of Styles. Newbury Park, California: Sage Publications.

Brewer, J., & Hunter, A. (2006). Foundations of multimethod research: Synthesizing styles. Thousand Oaks, California: Sage Publications.

Browne, M. W., & Cudeck, R. (1992). Alternative Ways of Assessing Model Fit. *Sociological Methods and Research,* 21(2), 230-258. doi: 10.1177/0049124192021002005

Brush, A. J. B., & Inkpen, K. M. (2007, 16-19 September). Yours, mine and ours? sharing and use of technology in domestic environments. *Paper presented at the 9th International Conference on Ubiquitous Computing*, Berlin, Heidelberg.

Bujang, M. A., Omar, E. D., & Baharum, N. A. (2018). A Review on Sample Size Determination for Cronbach's Alpha Test: A Simple Guide for Researchers. *The Malaysian Journal of Medical Sciences: MJMS,* 25(6), 85-99. doi: 10.21315/mjms2018.25.6.9

Bullock, J. A., Haddow, G. D., & Coppola, D. P. (2018). Cybersecurity and Critical Infrastructure Protection. In J. A. Bullock, G. D. Haddow, & D. P. Coppola (Eds.), *Introduction to Homeland Security (Fourth Edition)* (pp. 189-226). doi:10.1016/b978-0-12-804465-0.00008-x

Burcu, B., Hasan, C., & Izak, B. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly,* 34(3), 523-548. doi: 10.2307/25750690

Burns, S., & Roberts, L. (2013). Applying the Theory of Planned Behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety,* 15(1), 48-64. doi: 10.1057/cpcs.2012.13

Byrne, D. (2022). A worked example of Braun and Clarke's approach to reflexive thematic analysis. *Quality and Quantity,* 56, 1391+. doi: 10.1007/s11135-021-01182-y

Byun, H., Kim, J., Jeong, Y., Byoungjin, S., Gong, S., & Lee, C. (2024). A Security Analysis of Cryptocurrency Wallets against Password Brute-Force Attacks. *Scholarly Journal,* 13(13), 2433. doi: 10.3390/electronics13132433

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications,* 42, 36-45. doi: 10.1016/j.jisa.2018.08.002

Cains, M. G., Liberty, F., Taber, D., King, Z., & Henshel, D. S. (2022). Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis,* 42(8), 1643-1669. doi: 10.1111/risa.13687

Campbell, C. C. (2019). Solutions for counteracting human deception in social engineering attacks. [Human deception in social engineering attacks]. *Information Technology & People,* 32(5), 1130-1152. doi: 10.1108/ITP-12-2017-0422

Capellan, K., Condado, M., Morais, I., & Morreale, P. (2020). Analyzing Cybersecurity Understanding Using a Brain Computer Interface. *Paper presented at the HCI for Cybersecurity, Privacy and Trust*, Copenhagen, Denmark.

Carle, N., & Ophoff, J. (2024). Using Visual Cues to Enhance Phishing Education for Children. *Paper presented at the 16th IFIP WG 11.8 World Conference on Information Security Education on Information Security Education Challenges in the Digital Age*, Edinburgh, United Kingdom.

Carley, K. M. (2020). Social Cybersecurity: An Emerging Science. *Computer Mathematics Organ Theory,* 26(4), 365-381. doi: 10.1007/s10588-020-09322-9

CE Noticias Financieras. (2024a). Quishing, the technique that uses QR codes to steal information from you. *CE Noticias Financieras*. Retrieved from https://www.proquest.com/wire-feeds/quishing-technique-that-uses-qr-codes-steal/docview/2937219553/se-2. Date Accessed 23 April 2025

CE Noticias Financieras. (2024b, 28 February). Whaling: when CEOs in Peru are targeted by hackers. *CE Noticias Financieras*. Retrieved from https://www.proquest.com/wire-feeds/whaling-when-ceos-peru-are-targeted-hackers/docview/2933318311/se-2. Date Accessed 27 June 2024

Central Intelligence Agency. (2021). CIA The World Factbook. From Central Intelligence Agency https://www.cia.gov/the-world-factbook, Retrieved 12 February 2023

Ceran, O., & Karataş, S. (2025). What Influences Human Behaviour to Follow Their Intentions When It Comes to Cybersecurity? *Asian Journal of Social Psychology,* 28(4), 1-21. doi: doi.org/10.1111/ajsp.70050

Chapagain, D., Kshetri, N., Aryal, B., & Dhakal, B. (2024). SEAtech: Deception Techniques in Social Engineering Attacks: An Analysis of Emerging Trends and Countermeasures. http://arxiv.org/abs/2408.02092, Date Accessed 27 June 2025

Chatchalermpun, S., & Daengsi, T. (2021). Improving cybersecurity awareness using phishing attack simulation. *IOP conference series. Materials Science and Engineering,* 1088(1), 12015. doi: 10.1088/1757-899x/1088/1/012015

Chen, M.-F. (2016). Extending the theory of planned behavior model to explain people's energy savings and carbon reduction behavioral intentions to mitigate climate change in Taiwan–moral obligation matters. *Journal of Cleaner Production,* 112, 1746-1753. doi: 10.1016/j.jclepro.2015.07.043

Chiew, K. L., & Pieprzyk, J. (2010, 2021/03/15). Estimating Hidden Message Length in Binary Image Embedded by Using Boundary Pixels Steganography. *Paper presented at the Proceedings of the 5th International Conference on Availability, Reliability and Security*, Krakow, Poland.

Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications,* 106, 1-20. doi: 10.1016/j.eswa.2018.03.050

Chiou, Y.-M., Barnes, T., Jelenewicz, S. M., Mouza, C., & Shen, C.-C. (2021). Teacher Views on Storytelling-based Cybersecurity Education with Social Robots. *Paper presented at the Proceedings of the 20th Annual ACM Interaction Design and Children Conference*, Athens, Greece.

Choi, K.-S., Cho, S., & Lee, J. R. (2019). Impacts of online risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimization among Korean youth: Application of cyber-routine activities theory with latent class analysis. *Computers in Human Behavior,* 100, 1-10. doi: 10.1016/j.chb.2019.06.007

Chong, M.-T., Puah, C.-H., & Teh, C.-S. (2025). Digital policy initiatives and infrastructure in Malaysia: driving economic and financial growth through the Digital Economy Performance Indicator. *International Journal of Social Economics*. doi: 10.1108/IJSE-10-2024-0826

CISA. (2014). Cybersecurity Definition. In *Glossary*. National Initiative for Cybersecurity Careers and Studies: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary Date Accessed 8 August 2021

Claes, F., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research,* Vol.18 (3)(1), p.375-381. doi: 10.2307/3151312

Clark, R. G., Blanchard, W., Hui, F. K. C., Tian, R., & Woods, H. (2023). Dealing with complete separation and quasi-complete separation in logistic regression for linguistic data. *Research Methods in Applied Linguistics,* 2(1), 100044. doi: 10.1016/j.rmal.2023.100044

Claudia, L., & Erika, P. (2025). A Thesaurus for the Cybersecurity Domain to Specialized Knowledge Management and Indexing Operations. *Paper presented at the Advances in Social Networks Analysis and Mining*, Niagara Falls, ON, Canada.

Cloud&More. (2025). Top Cyber Attack on UK Businesses 2025. Retrieved from https://cloudandmore.co.uk/biggest-uk-cyber-attacks-2025/, Date Accessed 12 June 2025

Cochran, W. G. (1977). Sampling techniques (3rd ed.). Wiley: Wiley.

Corradini, I., & Nardelli, E. (2020). Social Engineering and the Value of Data: The Need of Specific Awareness Programs. *Paper presented at the Advances in Human Factors in Cybersecurity*, Washington D.C., USA.

Cranfield, D., Tick, A., Venter, I. M., Blignaut, R. J., & Renaud, K. (2021). Higher Education Students' Perceptions of Online Learning during COVID-19—A Comparative Study. *Education Sciences,* 11(8), 403. doi: 10.3390/educsci11080403

Creswell, J. W. (2018). Research design : qualitative, quantitative, and mixed methods approaches (Fifth edition.. ed.): Thousand Oaks, California : SAGE Publications, Inc.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika,* 16(3), 297-334. doi: 10.1007/bf02310555

Cuyugan, M. J. R., & Rey, W. P. (2024, 16-18 August). Beyond the Firewall: Strategies in Securing Remote Work Environment. *Paper presented at the 14th International Conference on Software Technology and Engineering (ICSTE)*, Macau, China.

CyberSAFE Malaysia (2017, 15 October). Keep our Women and Children CyberSAFE [CyberSecurity Malaysia]. Retrieved from https://www.facebook.com/watch/?v=1597157987025749

CyberSecurity Malaysia (Producer). (2023). Mid-Year Report- Threat Landscape. [.Png] Retrieved from https://www.cybersecurity.my/data/content_files/26/2511.pdf, Date Accessed 3 July 2024

CyberSecurity Malaysia (Producer). (2024). Protecting Your Password. Retrieved from https://www.cybersafe.my/pdf/youth/jpg/Protecting-Your-Password-Poster.jpg, Date Accessed 3 July 2024

Damenu, T. K., Gökbay, İ. Z., Covaci, A., & Li, S. (2025). Cyber Security Educational Games for Children: A Systematic Literature Review. *ACM Journal,* 1, 1-38. doi: 10.48550/arXiv.2508.17414

Dance, N. (2019, 21 February). New Study Finds Millennials Concerned About Privacy, But Lax On Security: 91% Take Responsibility For Own Data Security and 92% Believe Two-Factor Authentication (2FA) Keeps Data More Secure. *PR Newswire*.

David, A. B., & Carmi, E. (2025). Dark Cycles: Social Engineering and Political Chatbots in Netanyahu's 2019 Election Campaigns. *International Journal of Communication,* 19, 592-616.

Davis, T. P., Yimam, A. K., Kalam, M. A., Tolossa, A. D., Kanwagi, R., Bauler, S., Kulathungam, L., & Larson, H. (2022). Behavioural Determinants of COVID-19-Vaccine Acceptance in Rural Areas of Six Lower-and Middle-Income Countries. *Vaccines (Basel),* 10(2), 214. doi: 10.3390/vaccines10020214

Dawson, J. F. (2017). Analysing Quantitative Survey Data for Business and Management Students (1 ed.). London: London: SAGE Publications, Limited.
Denning, D. E. R. (1982). Cryptography and data security (Vol. 112): Addison-Wesley Reading.
Department of Statistics Malaysia. (2019). Household Income, Expenditure and Basic Amenities Survey (HIES/BA) 2019. From Ministry of Economy https://www.dosm.gov.my/portal-main/release-content/household-income-&-basic-amenities-survey-report-2019, Retrieved 15 May 2021
Department of Statistics Malaysia. (2021). Demographic Statistics Fourth Quarter 2020, Malaysia. From Ministry of Economy https://www.dosm.gov.my/portal-main/release-content/demographic-statistics-fourth-quarter-2020-malaysia, Retrieved 15 May 2021
Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys,* 54(8), 1-35. doi: 10.1145/3469886
Devasis, P., Prasanna Kumar, S., Nitin, S. G., Mangesh, M. G., Hla Myo, T., Rajeswari, R., & Sabyasachi, P. (2022). Security, Privacy, Risk, and Safety Toward 5G Green Network (5G-GN). In *Cyber Security and Network Security* (pp. 193-216): Wiley Date Accessed 27 June 2023
Divakarla, U., & Chandrasekaran, K. (2023). Predicting Phishing Emails and Websites to Fight Cybersecurity Threats Using Machine Learning Algorithms. *Paper presented at the 3rd International Conference on Smart Generation Computing, Communication (SMART GENCON)*, Bangalore, India.
Dodge, R. C., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers and Security,* 26(1), 73-80. doi: 10.1016/j.cose.2006.10.009
Donalds, C., & Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management,* 51, 102056. doi: 10.1016/j.ijinfomgt.2019.102056
Dzidzah, E., Owusu Kwateng, K., & Asante, B. K. (2020). Security behaviour of mobile financial service users. *Information and Computer Security,* 28(5), 719-741. doi: 10.1108/ics-02-2020-0021
Emanuela, A. R., Cristina, B. A., & Luminița, S. (2024, 27-28 June). AI and Prompt Engineering: The New Weapons of Social Engineering Attacks. *Paper presented at the 2024 16th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Iasi, Romania.
Fabian, K., Smith, E. T., Smith, S., & Bratton, A. (2023). Signalling new opportunities? An analysis of UK job adverts for degree apprenticeships. *Higher Education, Skills and Work - Based Learning,* 13(2), 299-314. doi: 10.1108/HESWBL-02-2022-0037
Fam, C. (Producer). (2025). Malaysia records 2.98 million scam calls last year, 82.81% increase from 2023. Retrieved from https://asianews.network/malaysia-records-2-98-million-scam-calls-last-year-82-81-increase-from-2023, Date Accessed 5 May 2026
Farhana, K. F., Fahmie, R. S. I., & Wan, Z. W. F. (2021, 21 July). Does the theory of planned behavior and perceived enjoyment give a big impact on online purchase intention among Gen-Y in east coast Malaysia? *Paper presented at the 8th International Conference on Advanced Materials Engineering & Technology (ICAMET)*, Langkawi, Malaysia.
Farooq, A., Dahabiyeh, L., & Javed, Y. (2024). When WhatsApp changed its privacy policy: explaining WhatsApp discontinuation using an enablers-inhibitors' perspective. *Online Information Review,* 48(1), 22-42. doi: 10.1108/OIR-04-2022-0232
Fatima, R., Fareed, M. M. S., Ullah, S., Ahmad, G., & Mahmood, S. (2024). An Optimized Approach for Detection and Classification of Spam Email's Using Ensemble Methods. *Wireless Personal Communications,* 139(1), 347-373. doi: 10.1007/s11277-024-11628-9
Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical

investigation on Malaysian Universities. *Journal of Physics. Conference Series,* 1339(1), 12098. doi: 10.1088/1742-6596/1339/1/012098
Felker, G. (2025). Malaysia's ICT sector policymaking: toward a developmental network state. *The Pacific Review,* 38(2), 338-369. doi: 10.1080/09512748.2024.2382104
Fink, A. (2002). How to Sample in Surveys. In The survey kit (2 ed.). Los Angeles: SAGE Publications. doi:10.4135/9781412984478
Fink, A. (2003). How to manage, analyze and interpret survey data (2nd ed. ed.). Thousand Oaks, California: Sage.
Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior : an introduction to theory and research: Addison-Wesley.
Fishbein, M., & Ajzen, I. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs: Englewood Cliffs : Prentice-Hall.
Fishbein, M., & Ajzen, I. (2011). Predicting And Changing Behaviour: The Reasoned Action Approach: Psychology Press.
Fleenor, H., Peker, Y., & Cutts, E. (2019, 27-2 March). Collaboration: Developing and Piloting a Cybersecurity Curriculum for Middle School. *Paper presented at the 50th ACM Technical Symposium on Computer Science Education*, Minneapolis, MN, USA.
Frank, I., & Eweniyi, O. (2013). Approach To Cyber Security Issues in Nigeria: Challenges and Solution. *International Journal of Cognitive Research in Science, Engineering and Education,* 1(1), 100-110.
Freminville, M. D. (2020). Best Practices of the Board of Directors (1 ed.). USA: Wiley Data and Cybersecurity.
Fujifilm. (2021). FUJIFILM Europe GmbH statement on June 2021 ransomware attack on FUJIFILM Corporation. https://www.fujifilm.com/lv/en/news/statement-on-june-2021-ransomware-attack, Date Accessed 10 January 2023
Furnell, S. (2005). Why users cannot use security. *Computers & Security,* 24(4), 274-279. doi: 10.1016/j.cose.2005.04.003
Gainsbury, S. M., Russell, A., Hing, N., Wood, R., Lubman, D. I., & Blaszczynski, A. (2014). The prevalence and determinants of problem gambling in Australia: Assessing the impact of interactive gambling and new technologies. *Psychology of Addictive Behaviors,* 28(3), 769-780. doi: 10.1037/a0036207
Gallegos-Segovia, P. L., Bravo-Torres, J. F., Larios-Rosillo, V. M., Vintimilla-Tapia, P. E., Yuquilima-Albarado, I. F., & Jara-Saltos, J. D. (2017, 18-20 October). Social engineering as an attack vector for ransomware. *Paper presented at the CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*, Pucon, Chile.
Gardner, B. (2014). What Is a Security Awareness Program? In B. Gardner & V. Thomas (Eds.), *Building an Information Security Awareness Program* (pp. 1-8). Boston: Syngress
Gaspard, L. (2020). Australian high school students and their Internet use : perceptions of opportunities versus 'problematic situations'. *Children Australia,* 45(1), 54-63. doi: 10.1017/cha.2020.2
Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *TQM Journal,* 23(4), 367-376. doi: 10.1108/17542731111139455
Golzar, J., Noor, S., & Tajik, O. (2022). Convenience Sampling. *International Journal of Education & Language Studies,* 1(2), 72-77. doi: 10.22034/ijels.2022.162981
Gonzalez, C. (2018, 12 Spetember). Phishing attempts among the dark triad: Patterns of attack and vulnerability, Report. *Computer Weekly News,* p. 728. Retrieved from https://link.gale.com/apps/doc/A553523705/GBIB. Date Accessed 16 January 2026
Gordon, W. J., Wright, A., Glynn, R. J., Kadakia, J., Mazzone, C., Leinbach, E., & Landman, A. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare

system. *Journal of the American Medical Informatics Association,* 26(6), 547-552. doi: 10.1093/jamia/ocz005
Gorsuch, R. L. (1997). Exploratory Factor Analysis: Its Role in Item Analysis. *Journal of Personality Assessment,* 68(3), 532-560. doi: 10.1207/s15327752jpa6803_5
Grant, H., Aashish, S., Mobin, J., Vern, P., & Wagner, D. (2017). Detecting credential spearphishing in enterprise settings. *Paper presented at the 26th USENIX Security Symposium* Vancouver, Canada.
Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. *Paper presented at the Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Montreal QC, Canada.
Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Toward a Conceptual Framework for Mixed-Method Evaluation Designs. *Educational Evaluation and Policy Analysis,* 11(3), 255-274. doi: 10.2307/1163620
Guitton, M. J. (2020). Cyberpsychology research and COVID-19. *Computers in Human Behavior,* 111, 106357. doi: 10.1016/j.chb.2020.106357
Gummer, T., Roßmann, J., & Silber, H. (2021). Using Instructed Response Items as Attention Checks in Web Surveys: Properties and Implementation. *Sociological Methods and Research,* 50(1), 238-264. doi: 10.1177/0049124118769083
Gusev, A. (2022). Domestic Private Banking Solutions Can Be Quite Successful as an Effective Protection Against Whaling-Style Cyber-Attacks Which Are Used as A Basis for More Complex Targeted Phishing. *Procedia Computer Science,* 213, 391-399. doi: 10.1016/j.procs.2022.11.083
Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon,* 3(7), e00346. doi: 10.1016/j.heliyon.2017.e00346
Hafner, L., Wutz, F., Pöhn, D., & Hommel, W. (2023, 29 August). TASEP: A Collaborative Social Engineering Tabletop Role-Playing Game to Prevent Successful Social Engineering Attacks. *Paper presented at the Proceedings of the 18th International Conference on Availability, Reliability and Security*, Benevento, Italy.
Hair, J. F. (2009). Multivariate data analysis : a global perspective (7th ed. ed.). Upper Saddle River, N.J. Harlow: Upper Saddle River, N.J. Harlow : Pearson Education.
Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security,* 73, 102-113. doi: 10.1016/j.cose.2017.10.008
Hawamleh, A. M. A., Alorfi, A. S. M., Al-Gasawneh, J. A., & Al-Rawashdeh, G. (2020). Cyber security and ethical hacking: The importance of protecting user data. *Solid State Technology,* 63(5), 7894-7899.
He, J., & Zhu, Y. (2014). Social Engineering/Phishing. In R. Alhajj & J. Rokne (Eds.), *Encyclopedia of Social Network Analysis and Mining* (pp. 1777-1783). New York, NY: Springer New York
Hendrik, L. E. E. (2018). *From Fishing to Phishing.* (Doctor of Philosophy PhD Thesis), University of Twente, Institute on Digital Society, Enschede, The Netherlands. Retrieved from https://ris.utwente.nl/ws/portalfiles/portal/23838012/thesis_E_Lastdrager.pdf, Date Accessed 29 March 2023
Hill, Z., Tawiah-Agyemang, C., Manu, A., Okyere, E., & Kirkwood, B. R. (2010). Keeping newborns warm: beliefs, practices and potential for behaviour change in rural Ghana. *Tropical Medicine and International Health,* 15(10), 1118-1124. doi: 10.1111/j.1365-3156.2010.02593.x
Hitomi, K. (2010). Operationalising human security: A brief review of the United Nations. *Paper presented at the New Perspectives on Human Security*, Sheffield, United Kingdom.

Hoheisel, R., van Capelleveen, G., Sarmah, D. K., & Junger, M. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. *Computers & Security,* 128, 103158. doi: 10.1016/j.cose.2023.103158

Holbrook, M., Sheng, S., Kumaraguru, P., Cagnoni, A., & Downs, J. (2010, 10-15 April). Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. *Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Atlanta, Georgia, USA.

Holley, B., Garcia, D., & Bernd, J. (2023). Teaching Cybersecurity: Introducing the Security Mindset. *Paper presented at the Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 2*, Toronto ON, Canada.

Hoong, R. (2021). Self control and smartphone use: An experimental study of soft commitment devices. *European Economic Review,* 140, 103924. doi: 10.1016/j.euroecorev.2021.103924

Howe, A. E., Ray, I., Roberts, M., Urbanska, M., & Byrne, Z. (2012, 20-23 May). The Psychology of Security for the Home Computer User. *Paper presented at the IEEE Symposium on Security and Privacy*, San Francisco, CA, USA.

Hsieh, H.-S. (2025). Applying a self-activation change approach to modify university students' environmental awareness and behavior. *Environment, Development and Sustainability,* 1, 1-19. doi: 10.1007/s10668-025-06226-z

Huizingh, E. (2007). The use of SPSS in statistical research. In E. Huizingh (Ed.), *Applied Statistics with SPSS* (pp. 6-23). London, United Kingdom: SAGE Publications

Hun, T. W. (2025). Minimum wage throughout Malaysia aligned from 1 August 2025. https://www.skrine.com/insights/alerts/july-2025/minimum-wage-throughout-malaysia-aligned-from-1-au, Date Accessed 7 November 2025

Hunter, A., & Brewer, J. (2006). Foundations of Multimethod Research: A Synthesizing Styles. Thousand Oaks, Calif.: Sage Publications.

Hurley, M. (2014). Cleaning a Data Set to Make Ready for Analysis. *Sage Research Methods Cases Part 1*. doi: 10.4135/978144627305014537966

Huxley, K. (2020). Data cleaning. In P. Atkinson, S. Delamont, A. Cernat, J. W. Sakshaug, & R. A. Williams (Eds.). London: SAGE Research Methods Foundations. Retrieved from 10.4135/9781526421036842861

Iannarelli, J. G., & O'Shaughnessy, M. (2015). The Threats of Today and Tomorrow. In J. G. Iannarelli & M. O'Shaughnessy (Eds.), *Information Governance and Security* (pp. 13-27). Boston: Butterworth-Heinemann

Indiran, D., Ismail, H. H., & Rashid, R. A. (2022). Exploring opportunities and challenges of using WhatsApp in teaching reading: A Malaysian rural primary school context. *Creative Education,* 13(5), 1689-1709. doi: 10.4236/ce.2022.135107

Inho, H. (2021). A Study on Improving Information Security Compliance of Organization Insider. [조직 내부자의 정보보안 준수 향상에 대한 연구]. *Journal of The Korean Society of Industry Convergence,* 24(4), 421-434. doi: 10.21289/ksic.2021.24.4.421

International Telecommunication Union. (2008). *ITU-T X.1205: Overview of cybersecurity*. Retrieved from International Telecommunication Union https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx Date Accessed 8 August 2021

Ion, I., Reeder, R., & Consolvo, S. (2015, 22-24 July). "... No one can hack my mind": Comparing Expert and Non-Expert Security Practices. *Paper presented at the Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, Ottawa, Canada.

Jackson, D. (2023, 2023 Sep 12). MGM Resorts cyberattack hobbles Las Vegas Strip operations. *Urgent Communications*. Retrieved from https://www.proquest.com/trade-journals/mgm-resorts-cyberattack-hobbles-las-vegas-strip/docview/3126354897/se-2

Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems,* 28(1), 66-82. doi: 10.1016/j.jsis.2018.09.003

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences,* 10(1), 33. doi: 10.1186/s13673-020-00237-7

Jarvie, C., & Renaud, K. (2024). Online Age Verification: Government Legislation, Supplier Responsibilization, and Public Perceptions. *Children (Basel),* 11(9), 1068. doi: 10.3390/children11091068

Jenkins, J., Durcikova, A., & Nunamaker, J. F., Jr. (2021). Mitigating the Security Intention-Behavior Gap: The Moderating Role of Required Effort on the Intention-Behavior Relationship. *Journal of the Association for Information Systems,* 22(1), 246-272. doi: doi.org/10.17705/1jais.00660

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems,* 34(2), 597-626. doi: 10.1080/07421222.2017.1334499

Jimmieson, N. L., Peach, M., & White, K. M. (2008). Utilizing the Theory of Planned Behavior to Inform Change Management: An Investigation of Employee Intentions to Support Organizational Change. *The Journal of Applied Behavioral Science,* 44(2), 237-262. doi: 10.1177/0021886307312773

Jinyin, P., Jiale, W., Jiawei, C., Geng, L., Hongqing, X., Yang, L., Qing, Z., Xiaozhen, W., & Yiping, Z. (2025). Mobile phone addiction was the mediator and physical activity was the moderator between bullying victimization and sleep quality. *Bio Medical Central Public Health,* 25(1), 1577-1513. doi: 10.1186/s12889-025-22813-1

Joisten, K., Thiemer, N., Renner, T., Janssen, A., & Scheffler, A. (2022, 22-24 March). Focusing on the Ethical Challenges of Data Breaches and Applications. *Paper presented at the International Conference on Assured Autonomy (ICAA)*, Fajardo, PR, USA.

Jones, K. S., Armstrong, M. E., Tornblad, M. K., & Namin, A. S. (2021). How social engineers use persuasion principles during vishing attacks. *Information and Computer Security,* 29(2), 314-331. doi: 10.1108/ICS-07-2020-0113

Jones, K. S., Siami, N. A., & Armstrong, M. E. (2018). The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals. *ACM Transactions on Computing Education,* 18(3), 1-12. doi: 10.1145/3152893

Jose, C. J., & Rajasree, M. S. (2020). Implicit Continuous User Authentication Using Swipe Actions on Mobile Touch Screen with ANN Classifier. In L. A. Kumar, L. S. Jayashree, & R. Manimegalai (Eds.), *Proceedings of International Conference on Artificial Intelligence, Smart Grid and Smart City Applications* (pp. 353-363). Switzerland: Springer International Publishing AG

KaaliÌ, K., Özkal, E. D., & DemiÌrer, Ü. i. (2025). Validity and reliability study of the dental students of attitudes towards online learning scale. *BMC Medical Education,* 25. doi: 10.1186/s12909-025-08296-z

Kamarudin, N. K., Hasani, N. N. M., Ruslan, R., Ramle, R., & Zukri, N. H. A. (2018). The Performance Analysis of Malware Attack. *Journal of Computing Research and Innovation,* 3(4), 19-24. doi: 10.24191/jcrinn.v3i4.72

Kamruzzaman, A., Thakur, K., Ismat, S., Ali, M. L., Huang, K., & Thakur, H. N. (2023, 8-11 March). Social Engineering Incidents and Preventions. *Paper presented at the 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA.

Kautonen, T., van Gelderen, M., & Fink, M. (2015). Robustness of the Theory of Planned Behavior in Predicting Entrepreneurial Intentions and Actions. *Entrepreneurship Theory and Practice,* 39(3), 655-674. doi: 10.1111/etap.12056

Keerthi, K. B. S., Sunil, V., Chengappa, K. T., & Basavaraju, S. (2025, 17-19 Dec. 2025). Proactive Defense Against Quishing: Integrating Predictive Analytics and Dynamic Analysis for Intelligent Threat Detection. *Paper presented at the 4th International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, Salem, India.

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. *International Journal of Information Security,* 24(3), 119. doi: 10.1007/s10207-025-01032-0

Khan, M., Zehui, B., & Copeland, J. A. (2012). Software updates as a security metric: Passive identification of update trends and effect on machine infection. *Paper presented at the IEEE Military Communications Conference*, New York.

Khanzadeh, S., Neto, E. C. P., Iqbal, S., Alalfi, M., & Buffett, S. (2025). An exploratory study on domain knowledge infusion in deep learning for automated threat defense. *International Journal of Information Security,* 24(1), 71. doi: 10.1007/s10207-025-00987-4

Kianpour, M., Kowalski, S. J., & Øverby, H. (2022). Advancing the concept of cybersecurity as a public good. *Simulation Modelling Practice and Theory,* 116, 102493. doi: 10.1016/j.simpat.2022.102493

Kim, S. H., Yang, K. H., & Park, S. (2014). An Integrative Behavioral Model of Information Security Policy Compliance. *Scientific World Journal*. doi: 10.1155/2014/463870

Köhler, D., Pünter, W., & Meinel, C. (2024). How Users Investigate Phishing Emails that Lack Traditional Phishing Cues. *Paper presented at the 22nd International Conference on Applied Cryptography and Network Security, ACNS*, Abu Dhabi, United Arab Emirates.

Köse, Ö. B., & Doğan, A. (2019). The Relationship between Social Media Addiction and Self-Esteem among Turkish University Students. *Addicta : The Turkish Journal on Addictions,* 6(1), 175-190. doi: 10.15805/addicta.2019.6.1.0036

Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Access,* 8, 125140-125148. doi: 10.1109/ACCESS.2020.3007867

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security,* 28(7), 509-520. doi: 10.1016/j.cose.2009.04.006

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications,* 22, 113-122. doi: 10.1016/j.jisa.2014.09.005

Kuchar, K., Blazek, P., & Fujdiak, R. (2023). From Playground to Battleground: Cyber Range Training for Industrial Cybersecurity Education. *Paper presented at the International Conference on Communication and Network Security (ICCNS)*, New York, USA.

Kumar, R. (2018). Research methodology : a step-by-step guide for beginners (Fifth ed.). Los Angeles: SAGE.

Kushner, D. (2013). The real story of stuxnet. *IEEE Spectrum,* 50(3), 48-53. doi: 10.1109/MSPEC.2013.6471059

Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A. (2020). Why do users not report spear phishing emails? *Telematics and Informatics,* 48, 101343. doi: 10.1016/j.tele.2020.101343

Lahcen, R. A. M., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity,* 3(1), 2-3. doi: 10.1186/s42400-020-00050-w

Lakoff, G. (1987). Women, fire, and dangerous things : what categories reveal about the mind. Chicago: Chicago : University of Chicago Press.

Lakshmi, N. T., Skandarsini, R. R., & Ida, S. J. (2023, 01-02 November). Enhancing Cybersecurity: A Multilayered Approach to Phishing Website Detection Using Machine Learning. *Paper presented at the 2023 International Conference on Research Methodologies in Knowledge*

Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), Chennai, India.

Le, X. C. (2022). The diffusion of mobile QR-code payment: an empirical evaluation for a pandemic. *Asia - Pacific Journal of Business Administration,* 14(4), 617-636. doi: 10.1108/APJBA-07-2021-0329

Lee, C. E., Chern, H. H., & Azmir, D. A. (2023). WhatsApp Use in a Higher Education Learning Environment: Perspective of Students of a Malaysian Private University on Academic Performance and Team Effectiveness. *Education Sciences,* 13. doi: 10.3390/educsci13030244

Lee, C. S., & Chua, Y. T. (2024). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime and Delinquency,* 70(9), 2250-2277. doi: 10.1177/00111287231180093

Leonov, P. Y., Vorobyev, A. V., Ezhova, A. A., Kotelyanets, O. S., Zavalishina, A. K., & Morozov, N. V. (2021, 13-14 May). The Main Social Engineering Techniques Aimed at Hacking Information Systems. *Paper presented at the Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, Yekaterinburg, Russia.

Leskin, A. (2025, 5 May 2026). Cybersecurity: How Malaysian SMEs are tackling increased network attacks. *The Edge Malaysia*. Retrieved from https://theedgemalaysia.com/node/748656

Lévesque, F. L., Chiasson, S., Somayaji, A., & Fernandez, J. M. (2018). Technological and Human Factors of Malware Attacks: A Computer Security Clinical Trial Approach. *ACM Transactions on Privacy and Security (TOPS),* 21(4), Article 18. doi: 10.1145/3210311

Lévesque, F. L., Fernandez, J. M., & Batchelder, D. (2017). Age and gender as independent risk factors for malware victimisation. *Paper presented at the Electronic Visualisation and the Arts (EVA 2017)*, London, United Kingdom.

Lewis-Beck, M. S. (2004). The Sage encyclopedia of social science research methods. Thousand Oaks, Calif.: Sage.

Li-tze, H., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal,* 6(1), 1-55. doi: 10.1080/10705519909540118

Li, C., Wu, Y., Yuan, X., Sun, Z., Wang, W., Li, X., & Gong, L. (2018). Detection and defense of DDoS attack–based on deep learning in OpenFlow-based SDN. *International Journal of Communication Systems,* 31(5), e3497. doi: 10.1002/dac.3497

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. Date Accessed 19 November 2025

Lin, C. Y., Tseng, Y. H., Lin, M. L., & Hou, W. L. (2021). Factors Related to Intentions to Commit Dating Violence Among Taiwanese University Students: Application of The Extended Theory of Planned Behaviour. *International Journal of Environmental Research and Public Health,* 18(4), 1-14. doi: 10.3390/ijerph18041956

Liobikiene, G., Mandravickaite, J., & Bernatoniene, J. (2016). Theory of planned behavior approach to understand the green purchasing behavior in the EU: A cross-cultural study. *Ecological Economics,* 125, 38-46. doi: 10.1016/j.ecolecon.2016.02.008

Löffler, E., Schneider, B., Zanwar, T., & Asprion, P. M. (2021). CySecEscape 2.0—A Virtual Escape Room To Raise Cybersecurity Awareness. *International Journal of Serious Games,* 8(1), 59-70. doi: 10.17083/ijsg.v8i1.413

Longtchi, T., & Xu, S. (2025, 14–16 August). Characterizing the Evolution of Psychological Tactics and Techniques Exploited by Malicious Emails. *Paper presented at the Science of Cyber Security*, Copenhagen, Denmark.

Lorenz, B., Kikkas, K., & Osula, K. (2019, 21-25 July). Factors of Socially Engineering Citizens in Critical Situations. *Paper presented at the Advances in Human Factors in Cybersecurity*, Orlando, Florida, USA.

Luiijf, E., Besseling, K., & de Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures,* 9(1-2), 3-31. doi: 10.1504/ijcis.2013.051608

Magdy, S., Abouelseoud, Y., & Mikhail, M. (2022). Efficient spam and phishing emails filtering based on deep learning. *Computer Networks,* 206, 108826. doi: 10.1016/j.comnet.2022.108826

Mahalakshmi, S., Pansy, D. L., & Thejashree, V. M. (2025, 28-29 March). Smart Email Filtering Against Phishing Attacks. *Paper presented at the International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)*, Chennai, India.

Mahidin, M. U. (Producer). (2021). Current Population Estimates, Malaysia, 2021. *Population size and annual population growth rate, age structure*. Retrieved from https://www.dosm.gov.my/v1/index.php, Date Accessed 29 June 2022

Maitland, N., & Lynch, J. (2020). Social Media, Ethics, And the Privacy Paradox. *Journal of Internet Law,* 23(9), 3-14. doi: 10.5772/intechopen.90906

Malaysian National Security Council. (2020). *Malaysia Cyber Security Strategy 2020-2024*. Perdana Putra, Putrajaya, Malaysia: Malaysian National Security Council (NSC) Retrieved from https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf. Date Accessed 28 July 2024

Malele, V. (2023). Cybersecurity Cloud-Based Online Learning: A Literature Review Approach. *Journal of Information Systems and Informatics,* 5(4), 1623-1632. doi: 10.51519/journalisi.v5i4.583

Mao, J., Li, P., Li, K., Wei, T., & Liang, Z. (2013, 09-11 September). BaitAlarm: Detecting Phishing Sites Using Similarity in Fundamental Visual Features. *Paper presented at the 5th International Conference on Intelligent Networking and Collaborative Systems*, Xi'an, China.

Marchal, N., Xu, R., Elasmar, R., Iason, G., Goldberg, B., & Isaac, W. (2024). Generative AI Misuse: A Taxonomy of Tactics and Insights from Real-World Data. http://arxiv.org/abs/2406.13843, Date Accessed 17 December 2025

Martti, L. (2020). Cyber Security Capacity Building: Cyber Security Education in Finnish Universities. 221-231,XV. Date Accessed 16 June 2020

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *ACM Journals,* 3, 81-112. doi: 10.1145/3359183

Maurer, T. I. M., & Morgus, R. (2014). *Compilation of Existing Cybersecurity and Information Security Related Definitions*. Retrieved from New America Foundation http://www.jstor.org/stable/resrep10487.6 Date Accessed 5 June 2025

Mayer, S., Bekavac, L. J. L., & Strecker, J. (2024). QR-Code Integrity by Design. *Paper presented at the CHI Conference on Human Factors in Computing Systems*, Honolulu, USA.

McGuire, C. F. (2015). TIM Lecture Series - The Expanding Cybersecurity Threat. *Technology Innovation Management Review,* 5(3), 56-48.

McNeish, D. (2018). Thanks coefficient alpha, we'll take it from here. *Psychological Methods,* 23(3), 412-433. doi: 10.1037/met0000144

Meadows, J. J., & Sambasivam, S. (2023). Mandatory Gamified Security Awareness Training Impacts on Texas Public Middle School Students: a Qualitative Study. *Issues in Informing Science & Information Technology, 20*, 67+. Date Accessed 8 December 2023

Meng, S., Wang, L., Wang, S., Wang, K., Xiao, X., Bai, G., & Wang, H. (2023, 11-15 September). Wemint:Tainting Sensitive Data Leaks in WeChat Mini-Programs. *Paper presented at the 38th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, Luxembourg, Luxembourg.

Merritt, M., Hansche, S., Ellis, B., Sanchez-Cherry, K., Snyder, J. N., & Donald, W. (2024). Building a Cybersecurity and Privacy Learning Program. *U.S. Department of Commence*. doi: 10.6028/NIST.SP.800-50r1

Mittapalli, J. S., Ojha, S., & T, S. (2021). Phishing Attack Detection using Python and Machine Learning. *Paper presented at the 5th International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India.

Mohamed, N., Taherdoost, H., & Khashan, O. A. (2025). A Review of AI in Spear Phishing Defense: Detecting and Thwarting Advanced Email Threats. *Paper presented at the EAI 3rd International Conference on Smart Technologies and Innovation Management*, Vancouver, Canada.

Mohammadinezhad, S., & Ahmadvand, M. (2020). Modeling the internal processes of farmers' water conflicts in arid and semi-arid regions: Extending the theory of planned behavior. *Journal of Hydrology (Amsterdam),* 580, 124241. doi: 10.1016/j.jhydrol.2019.124241

Montañez, R., Golob, E., & Xu, S. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology,* 11, 1755-1755. doi: 10.3389/fpsyg.2020.01755

Morgan, E., Thomas, M., Jing, C., & Jeremiah, S. (2023). SMiShing Attack Vector: Surveying End-User Behavior, Experience, and Knowledge. *Paper presented at the Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Liverpool, UK.

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014, 13-14 August). Social engineering attack framework. *Paper presented at the Information Security for South Africa*, Johannesburg, South Africa.

Mtair, A.-H. A. (2023). Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures. *International Journal of Advanced Computer Science*. doi: 10.14569/IJACSA.2023.0140292

Muller, L. P. (2024). Cybersecurity in practice: The vigilant logic of kill chains and threat construction. *European Journal of International Security,* 10(2), 231–251. doi: 10.1017/eis.2024.27

Murtaza, A. S., Pak, W., & Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences,* 12(12), 6042. doi: 10.3390/app12126042

Mwagwabi, F., & Jiow, J. H. (2021). Compliance with security guidelines in teenagers: the conflicting role of peer influence and personal norms. *Australasian Journal of Information Systems,* 25. doi: 10.3127/ajis.v25i0.2953

Nafees, T., Coull, N., Ferguson, R. I., & Sampson, A. (2017, 3-5 July). Idea-Caution Before Exploitation: The Use of Cybersecurity Domain Knowledge to Educate Software Engineers Against Software Vulnerabilities. *Paper presented at the Engineering Secure Software and Systems*, Bonn, Germany.

Nagyfejeo, E., & von Solms, B. (2020). Why Do National Cybersecurity Awareness Programmes Often Fail? *International Journal of Information Security and Cybercrime (IJISC),* 9(2), 18-27. doi: 10.19107/IJISC.2020.02.03

Nájera, P., Abad, F. J., & Sorrel, M. A. (2025). Is exploratory factor analysis always to be preferred? A systematic comparison of factor analytic techniques throughout the confirmatory–exploratory continuum. *Psychological Methods,* 30(1), 16-39. doi: 10.1037/met0000579

Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. *Computers & Security,* 132, 103387. doi: 10.1016/j.cose.2023.103387

National Cyber Security Agency. (2024). *Malaysia's Cyber Security Act 2024 (Act 854)*. Malaysia Retrieved from https://www.nacsa.gov.my/act854.php. Date Accessed 28 July 2024

Neil, L., Haney, J. M., Buchanan, K., & Healy, C. (2023). Analyzing Cybersecurity Definitions for Non-experts. In N. Clarke & S. Furnell (Eds.), (Vol. 674, pp. 391-404). Switzerland: Springer

Nevin, P., Renaud, K., & Finney, G. (2022). Slow down and frown to improve phishing detection. *Computer Fraud and Security*. doi: 10.12968/s1361-3723(22)70593-3

Neyazi, T. A. (2020). Digital propaganda, political bots and polarized politics in India. *Asian Journal of Communication,* 30(1), 39-57. doi: 10.1080/01292986.2019.1699938

Nicholson, J., Javed, Y., Dixon, M., Coventry, L., Ajayi, O. D., & Anderson, P. (2020, 07-11 September). Investigating Teenagers' Ability to Detect Phishing Messages. *Paper presented at the European Symposium on Security and Privacy (EuroS&PW)*, Genoa, Italy.

Nick, P. (Producer). (2022). Antivirus Apps: Need antivirus protection? Here are six of the best. *MacFormat*. [Article] Retrieved from https://link.gale.com/apps/doc/A700296685/ITOF?u=ustrath&sid=bookmark-ITOF&xid=38a55669, Date Accessed 5 October 2025

Normand, L. M., Paternò, F., & Winckler, M. (2014). Public policies and multilingualism in Human Computer Interaction (HCI). *Interactions, 21,* 70–73. Retrieved from 10.1145/2598608

Novak, A. N., & Vilceanu, M. O. (2019). "The internet is not pleased": twitter and the 2017 Equifax data breach. *The Communication Review,* 22(3), 196-221. doi: 10.1080/10714421.2019.1651595

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis. *International Journal of Qualitative Methods,* 16(1). doi: 10.1177/1609406917733847

Oh, S., Bae, Y., Thompson, I. A., & Im, Y. (2025). Uncovering the Dark Patterns of Phishing Emails: An Eye-Tracking Analysis. *IEEE Access,* 13, 197634-197644. doi: 10.1109/ACCESS.2025.3633616

Okazaki, S., Li, H., & Hirose, M. (2012). Benchmarking the Use of QR Code in Mobile Promotion. *Journal of Advertising Research,* 52(1), 102-117. doi: 10.2501/JAR-52-1-102-117

Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable Children and Youth Studies,* 8(4), 298-309. doi: 10.1080/17450128.2012.752119

Olifer, D., Goranin, N., Kaceniauskas, A., & Cenys, A. (2017). Controls-based approach for evaluation of information security standards implementation costs. *Technological and Economic Development of Economy (TEDE),* 23(1), 196-219. doi: 10.3846/20294913.2017.1280558

Oner, U., Cetin, O., & Savas, E. (2025). Human factors in phishing: Understanding susceptibility and resilience. 94, 104014. doi: 10.1016/j.csi.2025.104014

Onwuegbuche, F. C., Titung, R., Rantanen, E. M., Jurcut, A. D., Alm, C. O., & Pasquale, L. (2025). Securing the Weakest Link: Exploring Affective States Exploited in Phishing Emails With Large Language Models. *IEEE Access,* 13, 173460-173486. doi: 10.1109/ACCESS.2025.3615788

Ortiz, E., Reinerman-Jones, L., & Matthews, G. (2016, 27-31 July). Developing an Insider Threat Training Environment. *Paper presented at the AHFE 2016 International Conference on Human Factors in Cybersecurity*, Walt Disney World®, Florida, USA.

Oxford English Dictionary. (2025). Cybersecurity, n. In *Oxford University Press*. Retrieved from https://www.oed.com/dictionary/cybersecurity_n. Date Accessed 12 July 2024

Oyelami, J. O., & Azleena Mohd, K. (2020). Cyber Security Defence Policies: A Proposed Guidelines for Organisations Cyber Security Practices. *International Journal of Advanced Computer Science and Applications,* 11(8). doi: 10.14569/IJACSA.2020.0110817

Palmieri, M., Shortland, N., & McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. *Computers in Human Behavior,* 120, 106745. doi: 10.1016/j.chb.2021.106745

Pan, V. S.-H., Attar, R. W., Alhazmi, A. H., Alhazmi, A., Arya, V., Hsu, C.-H., & Alhomoud, A. (2025). AI-Powered Detection of Spear Phishing and Digital Arrest Attacks in E-Commerce. *International Journal on Semantic Web and Information Systems,* 21(1), 1-20. doi: 10.4018/IJSWIS.382475

Pangrazio, L., & Cardozo-Gaibisso, L. (2020). Beyond cybersafety: The need to develop social media literacies in pre-teens. *Digital Education Review,* (37), 49-63. doi: 10.1344/der.2020.37.49-63

Parsons, K., Butavicius, M., Pattinson, M., Calic, D., McCormac, A., & Jerram, C. (2016). Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails? http://arxiv.org/abs/1605.04717, Date Accessed 20 November 2025

Parthy, P. P., & Rajendran, G. (2019, 01-03 October). Identification and prevention of social engineering attacks on an enterprise. *Paper presented at the 2019 International Carnahan Conference on Security Technology (ICCST)*, Chennai, India.

Paul, A., Sharma, V., & Olukoya, O. (2024). SQL injection attack: Detection, prioritization & prevention. *Journal of Information Security and Applications,* 85, 103871. doi: 10.1016/j.jisa.2024.103871

Pérez-Sánchez, A., & Palacios, R. (2022). Evaluation of Local Security Event Management System vs. Standard Antivirus Software. *Applied Sciences,* 12(3), 1076. doi: 10.3390/app12031076

Pett, M., Lackey, N., & Sullivan, J. (2003). An Overview of Factor Analysis. In S. Robinson & K. Wiley (Eds.), Making Sense of Factor Analysis. Thousand Oaks, California: SAGE Publications, Inc. doi:10.4135/9781412984898

PhishLabs. (2016). PhishLabs 2016 Phishing Trends Intelligence Report: Hacking the Human, Exposes Thriving Phishing Underworld. https://link.gale.com/apps/doc/A445272059/GBIB, Retrieved 17 December 2025

Pienta, D., Jason Bennett, T., & Johnston, A. (2020). Protecting a whale in a sea of phish. *Journal of Information Technology,* 35(3), 214-231. doi: 10.1177/0268396220918594

Pitre, V., Joshi, A., & Das, S. (2023, 25-27 August). Blockchain and Machine Learning Based Approach to Prevent Phishing Attacks. *Paper presented at the 3rd Asian Conference on Innovation in Technology (ASIANCON)*, Ravat, India.

PopulationPyramid.net (Producer). (2025). Camparison of Population Pyramids. Retrieved from https://www.populationpyramid.net/, Date Accessed 12 November 2025

Pound, R. (1969). An introduction to the philosophy of law (First ed.). New York: Yale University Press.

Powell, N. (2021, 10 June). Southeast Asia eCommerce platform Lazada launches public bug bounty program with YesWeHack. *PR Newswire Europe Including UK Disclose*. Retrieved from https://www.proquest.com/wire-feeds/southeast-asia-ecommerce-platform-lazada-launches/docview/2539466086/se-2. Date Accessed 17 December 2025

Power, A. (2018). Cyberpsychology and Society: Current Perspectives (1 ed.): Milton: Routledge.

Pranathi, R., Sreekriti, S., Ashwin, J., Justin, M., Nathan, P., Sashank, N., & Seungeun, L. C. (2022). Designing a Visual Cryptography Curriculum for K-12 Education. *Paper presented at the 2023 IEEE Global Engineering Education Conference (EDUCON)*, Kuwait, Kuwait.

Prasad, D., Suhasini, S., Parthasarathy, B., & Praveen, J. (2024). Enhancing Internet Security: A Machine Learning-Based Browser Extension to Prevent Phishing Attacks. *Paper presented at the 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)*, Gautam Buddha Nagar, India.

Prior, S., & Renaud, K. (2022). The Impact of Financial Deprivation on Children's Cybersecurity Knowledge and Abilities. *Education and Information Technologies*. doi: 10.1007/s10639-022-10908-w

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction,* 30, 100343. doi: 10.1016/j.ijcci.2021.100343

Qusa, H., & Tarazi, J. (2021, 27-30 January). Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students. *Paper presented at the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, Nevada, USA.

Rachad, A. (2012). Interpreting Quantitative Data With IBM SPSS Statistics. In. doi:10.4135/9781526435439

Rader, M., & Rahman, S. (2015). Exploring Historical and Emerging Phishing Techniques and Mitigating the Associated Security Risks. *Cornell University Library*. doi: 10.48550/arxiv.1512.00082

Radke, K., Brereton, M., Mirisaee, S., Ghelawat, S., Boyd, C., & Nieto, J. G. (2011, 5-9 September). Tensions in developing a secure collective information practice-the case of agile ridesharing. *Paper presented at the Human-Computer Interaction–INTERACT 2011: 13th IFIP TC 13 International Conference*, Lisbon, Portugal.

Rahim, N. H. A., Hamid, S., & Kiah, M. L. M. (2019). Enhancement of Cybersecurity Awareness Program on Personal Data Protection Among Youngsters In Malaysia: An Assessment. *Malaysian Journal of Computer Science,* 32(3), 221-245. doi: 10.22452/mjcs.vol32no3.4

Rajeswari, C., & Rajeeth, P. S. (2025, 28-29 March). Artificial Intelligence in Phishing Detection and Analysis: A Foundational Review. *Paper presented at the International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)*, Chennai, India.

Ramakrishnan, K., Yasin, N. M., & Periasamy, J. (2022). Digital divide on cybersecurity awareness among the Malaysian higher learning institution students. *AIP Conference Proceedings,* 2472(1), 040022. doi: 10.1063/5.0092796

Ramanathan, V., & Wechsler, H. (2012). phishGILLNET--phishing detection methodology using probabilistic latent semantic analysis, AdaBoost, and co-training: [Doc 9]. *EURASIP Journal on Information Security,* 2012, 1-22. doi: 10.1186/1687-417X-2012-1

Ramluckan, T., van Niekerk, B., & Martins, I. (2020, Jun 2020). A Change Management Perspective to Implementing a Cyber Security Culture. *Paper presented at the European Conference on Cyber Warfare and Security*, Reading, United Kingdom.

Rana, N. P., Slade, E., Kitching, S., & Dwivedi, Y. K. (2019). The IT way of loafing in class: Extending the theory of planned behavior (TPB) to understand students' cyberslacking intentions. *Computers in Human Behavior,* 101, 114-123. doi: 10.1016/j.chb.2019.07.022

Redmiles, E. M., Kross, S., & Mazurek, M. L. (2016). How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior. *Paper presented at the Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Vienna, Austria.

Redmiles, E. M., Kross, S., & Mazurek, M. L. (2017). Where is the Digital Divide? A Survey of Security, Privacy, and Socioeconomics. *Paper presented at the Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, Denver, Colorado, USA.

Rehman, S., & Manickam, S. (2023). Towards a Cybersecurity Awareness Program for Non-Technical Audiences in Malaysia. In K. D. Strang & N. R. Vajjhala (Eds.), (pp. 85-97). doi:10.1201/9781003319887-6

ReliaQuest. (2023). Rising trend in 'quishing' attacks targets QR code users. *ICT Monitor Worldwide*. Retrieved from https://www.proquest.com/wire-feeds/rising-trend-quishing-attacks-targets-qr-code/docview/2889547446/se-2. Date Accessed 17 September 2024

Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal: Practice, Process and People*. doi: 10.1108/OCJ-03-2021-0004

Renaud, K., Otondo, R., & Warkentin, M. (2019). "This is the way 'I' create my passwords" ... does the endowment effect deter people from changing the way they create their passwords? *Computers & Security,* 82, 241-260. doi: 10.1016/j.cose.2018.12.018

Renaud, K., Searle, R., & Dupuis, M. (2021, 25 - 28 October). Shame in cyber security : effective behavior modification tool or counterproductive foil? *Paper presented at the NSPW '21: Proceedings of the 2021 New Security Paradigms Workshop*, Virtual Event USA.

Renaud, K., Sengul, C., Coopamootoo, K., Clift, B., Taylor, J., Springett, M., & Morrison, B. (2024). "We're Not That Gullible!" Revealing Dark Pattern Mental Models of 11-12-Year-Old Scottish Children. *ACM Transactions on Computer-Human Interaction,* 31(3), 1-41. doi: 10.1145/3660342

Renaud, K., van der Schyff, K., & MacDonald, S. (2023). Would US citizens accept cybersecurity deresponsibilization? Perhaps not. *Computers & Security,* 131, 103301. doi: 10.1016/j.cose.2023.103301

Renaud, K., & Weir, G. R. S. (2016, 2-4 August). Cybersecurity and the Unbearability of Uncertainty. *Paper presented at the 2016 Cybersecurity and Cyberforensics Conference (CCC)*, Amman Jordan.

Renaud, K., Zimmermann, V., Schürmann, T., & Böhm, C. (2021). Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications,* 8(1), 1-17. doi: 10.1057/s41599-021-00746-5

Revilla, L., Montoya, J., & Ramamoorthi, L. S. (2023, 23-27 October). Exploring Cybersecurity Awareness Among Students from Two Latin American Universities: An Empirical Analysis. *Paper presented at the World Engineering Education Forum - Global Engineering Deans Council (WEEF-GEDC)*, Monterrey, Mexico.

Reynolds, M. (2021). Staying Protected—The Individual. In M. Reynolds (Ed.), *The Art of Attack: Attacker Mindset for Security Professionals* (pp. 241-256). Hoboken, New Jersey, USA: John Wiley & Sons, Inc.

Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). Which factors predict susceptibility to phishing? An empirical study. *Computers & Security,* 136, 103558. doi: 10.1016/j.cose.2023.103558

Rich, T. (2018). You can trust me: a multimethod analysis of the Nigerian email scam. *Security Journal,* 31(1), 208-225. doi: 10.1057/s41284-017-0095-0

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2022). Phishing simulation exercise in a large hospital: A case study. *Digital Health,* 8. doi: 10.1177/20552076221081716

Robinson, O. C. (2022). Conducting thematic analysis on brief texts: The structured tabular approach. *Qualitative Psychology,* 9(2), 194-208. doi: 10.1037/qup0000189

Roger, A. G. (2021). Social Engineering Attacks. In C. Nachreiner & A. Cagnoni (Eds.), *Hacking Multifactor Authentication* (pp. 259-273). Indianapolis, Indiana, USA: Wiley

Roos, M. J., & Bauldry, S. (2021). Confirmatory Factor Analysis. In B. Entwisle (Ed.), *Confirmatory Factor Analysis*. Thousand Oaks, California: Sage Publications. Retrieved from 10.4135/9781071938959.n4

Rys, M., Ślusarek, A., & Zieliński, K. (2025). Caught Off Guard: When Experts Fall for Quishing, Is Awareness Enough? *Security and Privacy,* 8(1), e486. doi: 10.1002/spy2.486

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security,* 53, 65-78. doi: 10.1016/j.cose.2015.05.012

Saker-Clark, H. (2025, 21 May). Marks & Spencer blames 'human error' as cyber attack set to cost £300m. *Press Association*. Retrieved from https://www.proquest.com/wire-feeds/marks-amp-spencer-blames-human-error-as-cyber/docview/3206123613/se-2. Date Accessed 17 December 2025

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Scholarly Journal,* 11(4), 89-106. doi: 10.3390/fi11040089

Santini, R. M. (2021). When Machine Behavior Targets Future Voters: The Use of Social Bots to Test Narratives for Political Campaigns in Brazil. *International Journal of Communication,* 15, 1220-1244.

Sapkale, Y. (2024, 2 August 2024). Fraud Alert: Online Shopping Scams & Deceptive App Designs aka Dark Patterns. *Money Life*. Retrieved from https://link.gale.com/apps/doc/A803613641/GBIB

Sarno, D. M., Gendron, C., & Volante, W. G. (2025). Filtering Out the User?: Are Users Complacent with Phishing Emails Due to Automated Filters? *International Journal of Human–Computer Interaction,* 41(16), 9908-9917. doi: 10.1080/10447318.2024.2429759

Saudi, M. H., Saudi, M. M., Rahmana, A., & Husainiamer, M. A. (2021). Gaming Mobile Applications: Proof of Concept for Security Exploitation. *Turkish Journal of Computer and Mathematics Education,* 12(8), 1761-1766.

Saulsbery, G. (2021, 17 February). Panel: 90% of cyber attacks are occasioned by human error, and they're on the rise. *Trade Journal*. Retrieved from https://www.proquest.com/trade-journals/panel-90-cyber-attacks-are-occasioned-human-error/docview/2492145704/se-2. Date Accessed 17 November 2025

Schafer, J. H. (2020). International Information Power and Foreign Malign Influence in Cyberspace. *Paper presented at the International Conference on Cyber Warfare and Security*, Reading, United Kingdom.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards A More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law : JDFSL,* 12(2), 53-74. doi: 10.15394/jdfsl.2017.1476

Schreuder, H. T., Gregoire, T. G., & Weyer, J. P. (2001). For what applications can probability and non-probability sampling be used? *Environmental Monitoring and Assessment,* 66(3), 281-291. doi: 10.1023/a:1006316418865

Schultz, E. (2005). The human factor in security. *Computers & Security,* 24(6), 425-426. doi: 10.1016/j.cose.2005.07.002

Shah, P., & Agarwal, A. (2020). Cybersecurity behaviour of smartphone users in India: an empirical analysis. *Information and Computer Security,* 28(2), 293-318. doi: 10.1108/ics-04-2019-0041

Shahidah, H., Fauziah, A., Norizan, R., Noranifitri, M. N., Harliana, H., Syahid, M. A. A., Riki, R., Nizam, A., & Anuar, K. K. (2021). Level of Awareness of Social Media Users on Cyber Security: Case Study among Students of University Tun Hussein Onn Malaysia. *Turkish Journal of Computer and Mathematics Education,* 12(2), 694-698. doi: 10.17762/turcomat.v12i2.923

Shamon, H., & Berning, C. (2020). Attention Check Items and Instructions in Online Surveys with Incentivized and Non-Incentivized Samples: Boon or Bane for Data Quality? *Survey Research Methods Journal of the European Survey Research Association,* 14(1), 54-77. doi: 10.18148/srm/2020.v14i1.7374

Shamy, N. E., Xie, W., & Zhong, C. (2025). Smishing: Exploring How Different Persuasion Techniques Influence Users Emotions, Cognitions, and Identification Accuracy. In R. Riedl, G. R. Müller-Putz, F. D. Davis, J. vom Brocke, P.-M. Léger, & A. B. Randolph (Eds.), (Vol. 66, pp. 345-355). Cham: Cham: Springer Nature Switzerland

Shapiro, D. L. (2000). Using the Theory of Planned Behavior to Induce Problem Solving in Schools. *Negotiation Journal,* 16(2), 183-191. doi: 10.1111/j.1571-9979.2000.tb00212.x

Sharif, K. H., & Ameen, S. Y. (2020, 23-24 December). A Review of Security Awareness Approaches With Special Emphasis on Gamification. *Paper presented at the International Conference on Advanced Science and Engineering (ICOASE)*, Duhok, Iraq.

Shehata, A., & Eldakar, M. (2024). Social engineering awareness and resilience in Egypt: a quantitative exploration. *Library Hi Tech*. doi: 10.1108/lht-10-2023-0480

Shibli, A. M., Pritom, M. M. A., & Gupta, M. (2024, 29-30 April). AbuseGPT: Abuse of Generative AI ChatBots to Create Smishing Campaigns. *Paper presented at the 12th International Symposium on Digital Forensics and Security (ISDFS)*, San Antonio, TX, USA.

Siaw, Y.-L., Chua, K.-H., Ruckwongpatr, K., Tung, S. E. H., Gan, W. Y., Poon, W. C., Nadhiroh, S. R., Nurmala, I., Üztemur, S., Chen, I. H., Griffiths, M. D., & Lin, C.-Y. (2025). Psychometric Properties for the Malay Version of the Assessment of Criteria for Specific Internet-use Disorders

among Young Adults in Malaysia. *Asian Journal of Social Health and Behavior,* 8(3), 97+. doi: 10.4103/shb.shb_171_24

Sibi Chakkaravarthy, S., Sangeetha, D., & Vaidehi, V. (2019). A Survey on malware analysis and mitigation techniques. *Computer Science Review,* 32, 1-23. doi: 10.1016/j.cosrev.2019.01.002

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences,* 12(12), 6042. doi: 10.3390/app12126042

Sievert, M. (2021). The Cyberattack Against T-Mobile and Our Customers: What happened, and what we are doing about it. Retrieved from T-Mobile website: https://www.t-mobile.com/news/network/cyberattack-against-tmobile-and-our-customers, Date Accessed August 2, 2024

Sikos, L. F. (2023). Cybersecurity knowledge graphs. *Knowledge and Information Systems,* 65(9), 3511-3531. doi: 10.1007/s10115-023-01860-3

Skopik, F., Bonitz, A., Grantz, V., & Göhler, G. (2022). From scattered data to actionable knowledge: flexible cyber security reporting in the military domain. *International Journal of Information Security,* 21(6), 1323-1347. doi: 10.1007/s10207-022-00613-7

Smith, S., Smith, E. T., Fabian, K., Barr, M., Berg, T., Cutting, D., Paterson, J., Young, T., & Zarb, M. (2020, 21-24 October). Computing degree apprenticeships: An opportunity to address gender imbalance in the IT sector? *Paper presented at the IEEE Frontiers in Education Conference (FIE)*, Uppsala, Sweden.

Sparks, C. (2022, 4 April). UW System sends phishing simulations to students. *University Wire*. Retrieved from https://www.proquest.com/wire-feeds/uw-system-sends-phishing-simulations-students/docview/2647399069/se-2. Date Accessed 17 December 2025

Srinivasan, R., & Lohith, C. P. (2017). Pilot Study—Assessment of Validity and Reliability. In R. Srinivasan & C. P. Lohith (Eds.), *Strategic Marketing and Innovation for Indian MSMEs* (1 ed., pp. 43-49). Singapore: Springer Singapore Pte. Limited

Sten, M., Kristjan, K., Kaspar, J., & Olaf, M. (2019, June). Mixed Methods Research Approach and Experimental Procedure for Measuring Human Factors in Cybersecurity Using Phishing Simulations. *Paper presented at the 18th European Conference on Research Methodology for Business and Management Studies (ECRM 2019)* Johannesburg, South Africa.

Stevens, J. (2009). Applied multivariate statistics for the social sciences (5th ed. ed.): New York : Routledge.

Steves, M., Greene, K., & Theofanos, M. (2020). Categorizing human phishing difficulty: a Phish Scale. *Journal of Cybersecurity,* 6(1). doi: 10.1093/cybsec/tyaa009

Stone, J. (2018). How Companies Can Manage Cyber Risk Tied to Employees' Personal Devices. *WSJ Pro. Cyber Security*. https://www.proquest.com/trade-journals/how-companies-can-manage-cyber-risk-tied/docview/2171113175/se-2, Date Accessed 12 January 2023

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation Guidelines for IS Positivist Research. *Communications of the Association for Information Systems,* 13, 24. doi: 10.17705/1CAIS.01324

Stuart, L. M., Park, G., Talor, J. M., & Raskin, V. (2014, 24-26 June). On identifying phishing emails: Uncertainty in machine and human judgment. *Paper presented at the IEEE Conference on Norbert Wiener in the 21st Century (21CW)*, Boston, USA.

Subbulakshmi, T., Meghana, G., Sunkara, S. R. S., & Sai, V. S. (2025, 7-8 January). Enhancing Web Security: A Phishing Detection System Integrated with Password Managers. *Paper presented at the 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)*, Goathgaun, Nepal.

Sujata, M., Khor, K.-S., Ramayah, T., & Teoh, A. P. (2019). The role of social media on recycling behaviour. *Sustainable Production and Consumption,* 20, 365-374. doi: 10.1016/j.spc.2019.08.005

Sukhmani. (2017). Using theory of planned behavior in investigating agricultural waste management: Survey evidence from Northern India. *Vilakshan: The XIMB Journal of Management,* 14(2), 39-53.

Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. A. (2022). Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review. *Social Sciences (Basel),* 11(9), 386. doi: 10.3390/socsci11090386

Takanen, A., DeMott, J., Miller, C., & Kettunen, A. (2018). Fuzzing for software security testing and quality assurance (Second ed.). Boston, MA: Boston, MA : Artech House.

Talib, S., Clarke, N. L., & Furnell, S. M. (2010, 15-18 February). An analysis of information security awareness within home and work environments. *Paper presented at the 2010 International Conference on Availability, Reliability and Security*, Krakow, Poland.

Tam, L., Glassman, M., & Vandenwauver, M. (2010). The psychology of password management: a tradeoff between security and convenience. *Behaviour & Information Technology,* 29(3), 233-244. doi: 10.1080/01449290903121386

Tan, C.-S., Ooi, H.-Y., & Goh, Y.-N. (2017). A moral extension of the theory of planned behavior to predict consumers' purchase intention for energy-efficient household appliances in Malaysia. *Energy Policy,* 107, 459-471. doi: 10.1016/j.enpol.2017.05.027

Tang, C. F., & Rosidi, M. A. I. (2025). Investigating the effects of ICT infrastructure on Malaysia's economic growth: Insights from the Solow growth model. *Information Technology for Development,* 31(1), 124-139. doi: 10.1080/02681102.2024.2338527

Tayachi, A., Ouni, B., Mourad, A., & Erbad, A. (2025, 12-16 May). Quishing Attack Detection and Mitigation Using Machine Learning and Deep Learning for Malicious URL Identification. *Paper presented at the 2025 International Wireless Communications and Mobile Computing (IWCMC)*, Abu Dhabi, United Arab Emirates.

Taylor, G. W., & Becker, M. P. (1998). Increased efficiency of analyses: cumulative logistic regression vs ordinary logistic regression. *Community Dentistry and Oral Epidemiology,* 26(1), 1-6. doi: 10.1111/j.1600-0528.1998.tb01916.x

Te-Shun, C. (2019, 15-19 June). Multi-Learning Techniques for Enhancing Student Engagement in Cybersecurity Education. *Paper presented at the Association for Engineering Education (ASEE) Annual Conference & Exposition*, Tampa, Florida.

Temoshok, D., Lefkovitz, N., Galluzzo, R., Choong, Y.-Y., Regenscheid, A., Fenton, J. L., & Richer, J. P. (2025). Digital Identity Guidelines. From NIST Special Publication (SP) 10.6028/NIST.SP.800-63B-4, Retrieved 17 November 2025

Thao, M. P., & Tick, A. (2021). Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam. *Acta Polytechnica Hungarica,* 18(8), 67-89. doi: 10.12700/APH.18.8.2021.8.4

Thomas, V. (2014). Creating Simulated Phishing Attacks. In B. Gardner & V. Thomas (Eds.), *Building an Information Security Awareness Program* (pp. 95-107). Boston: Elsevier Inc

Thompson, B. (2004). Introduction to Factor Analysis. In B. Dan (Ed.), Exploratory and confirmatory factor analysis: Understanding concepts and applications (pp. 3-7). Washington, DC: American Psychological Association. doi:10.1037/10694-001

Thompson, J. (2025, 2 April). Adaptive Security Raises $43M from a16z and OpenAI Startup Fund to Combat AI-Powered Cyber Attacks Including Deepfakes, Vishing and Smishing. *PR Newswire*. Retrieved from https://www.proquest.com/wire-feeds/adaptive-security-raises-43m-a16z-openai-startup/docview/3185002990/se-2. Date Accessed 10 Novermber 2025

Tila, C. (2020). Age group distribution of internet users in Malaysia in 2020. From Malaysian Communications and Multimedia Commission https://www.statista.com/statistics/981334/malaysia-internet-users-age-group-distribution/, Retrieved 2 December 2025

Tiong, K. M., Cheng, M. Y., & Choong, C. K. (2022). The Roles Of ICT Telecommunication Infrastructure On Foreign Direct Investment In Malaysia. *Asian Academy of Management Journal,* 27(2), 1-20. doi: 10.21315/aamj2022.27.2.1

Toapanta, F., Rivadeneira, B., Tipantuña, C., & Guamán, D. (2024). AI-Driven Vishing Attacks: A Practical Approach. *Paper presented at the XXXII Conference on Electrical and Electronic Engineering*, Quito, Ecuador.

Tomičić, I. (2023, 22-26 May). Social Engineering Aspects of Email Phishing: an Overview and Taxonomy. *Paper presented at the 46th MIPRO ICT and Electronics Convention*, Opatija, Croatia.

Triantafyllopoulos, A., Spiesberger, A. A., Tsangko, I., Jing, X., Distler, V., Dietz, F., Alt, F., & Schuller, B. W. (2025). Vishing: Detecting social engineering in spoken communication — A first survey & urgent roadmap to address an emerging societal challenge. *Computer Speech & Language,* 94, 101802. doi: 10.1016/j.csl.2025.101802

Tucker, L. R., & Lewis, C. (1973). A reliability coefficient for maximum likelihood factor analysis. In Psychometrika (Vol. 38, pp. 1-10): Cambridge University Press. doi:10.1007/BF02291170

Uberti, D. (2020). Pentagon Must Improve Cyber Readiness, Watchdog Warns; Report says Defense Department has failed to meet multiple deadlines for cybersecurity initiatives. *WSJ Pro. Cyber Security*. https://www.proquest.com/trade-journals/pentagon-must-improve-cyber-readiness-watchdog/docview/2389560936/se-2, Date Accessed 15 April 2021

Ugwu, C., Ezema, M., Ome, U., Ofusori, L., Olebera, C., & Ukwandu, E. (2023). A Study on the Impact of Gender, Employment Status, and Academic Discipline on Cyber-Hygiene: A Case Study of University of Nigeria, Nsukka. In Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media (pp. 389-407): Singapore: Springer Nature Singapore. doi:10.1007/978-981-19-6414-5_22

van der Heijden, A., & Allodi, L. (2019). Cognitive Triaging of Phishing Attacks. http://arxiv.org/abs/1905.02162, Date Accessed 13 November 2021

van Schaik, P., & Renaud, K. (2025). SOK: Cognitive Dissonance in the Cybersecurity Domain. *Paper presented at the European Symposium on Usable Security (EuroUSEC)*, Manchester, United Kingdom.

van Steen, T. (2021). Successful Gamification of Cybersecurity Training. *CyberPsychology, Behavior & Social Networking,* 24(9), 593-599. doi: 10.1089/cyber.2020.0526

van Steen, T., & Deeleman, J. R. A. (2021). Successful Gamification of Cybersecurity Training. *Cyberpsychology Behavior and Social Networking,* 24(9), 593-598. doi: 10.1089/cyber.2020.0526

van Teijlingen, E. R., Rennie, A.-M., Hundley, V., & Graham, W. (2001). The importance of conducting and reporting pilot studies: the example of the Scottish Births Survey. *Journal of Advanced Nursing,* 34(3), 289-295. doi: 10.1046/j.1365-2648.2001.01757.x

Vanitha, J., Mallika, C., Hema, A., Parkavi, K., Shree, K. K. S., & Senthilkumar, S. (2024, 23-25 October). Detection System of Whaling Attack using Deep Learning Techniques. *Paper presented at the 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS)*, Erode, India.

Varshney, G., Kumawat, R., Varadharajan, V., Tupakula, U., & Gupta, C. (2024). Anti-phishing: A comprehensive perspective. *Expert Systems with Applications,* 238, 122199. doi: 10.1016/j.eswa.2023.122199

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as “the three R's”. *Heliyon: A Cell Press Journal,* 5(12). doi: 10.1016/j.heliyon.2019.e02855

Vikas, S., Kumar, V. T., Divya, T., Ravikant, Pranshul, S., & Shashank, S. (2025). Enhancing cybersecurity: A machine learning approach for phishing website detection. *Paper presented at the AIP Conference Proceedings*, Nitte, India.

Vishal, J., Bishwajeet, P., Laura, A., Pranav, S., Pushpanjali, P., & Damini, J. (2025, 7-9 March). A Comprehensive Usage of AI in Prevention of Social Engineering Attack. *Paper presented at the 14th International Conference on Communication Systems and Network Technologies (CSNT)*, Bhopal, India.

Walker, D. (2018, 11th October). WannaCry cost the NHS £92 million, report estimates. *IT Pro*. Retrieved from https://www.proquest.com/magazines/wannacry-cost-nhs-£92-million-report-estimates/docview/2118092438/se-2

Wang, K., Xu, Y., Wang, C., Tan, M., & Chen, P. (2020). A Corrected Goodness-of-Fit Index (CGFI) for Model Evaluation in Structural Equation Modeling. *Structural Equation Modeling: A Multidisciplinary Journal,* 27(5), 735-749. doi: 10.1080/10705511.2019.1695213

Wang, P. A. (2013). Assessment of Cybersecurity Knowledge and Behavior: An Anti-phishing Scenario. *Paper presented at the ICIMP 2013: The Eighth International Conference on Internet Monitoring and Protection, IARIA*, Rome, Italy.

Wang, S., Fan, J., Zhao, D., Yang, S., & Fu, Y. (2014). Predicting consumers’ intention to adopt hybrid electric vehicles: using an extended version of the theory of planned behavior model. *Transportation,* 43(1), 123-143. doi: 10.1007/s11116-014-9567-9

Wang, Z., Sun, L., & Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access,* 8, 85094-85115. doi: 10.1109/access.2020.2992807

Wang, Z., Zhu, H., & Sun, L. (2021). Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access,* 9, 11895-11910. doi: 10.1109/access.2021.3051633

Warren, P. (2018, 2018). Could a cyber attack cause a systemic impact in the financial sector? *Bank of England Quarterly Bulletin, 58,* 1-11.

Watson, H., Moju-Igbene, E., Kumari, A., & Das, S. (2020). "We Hold Each Other Accountable": Unpacking How Social Groups Approach Cybersecurity and Privacy Together. *Paper presented at the Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, New York, USA.

Weaver, G. A., Feddersen, B., Marla, L., Wei, D., Rose, A., & Van Moer, M. (2022). Estimating Economic Losses From Cyber-Attacks on Shipping Ports: An Optimization-Based Approach. *Transportation Research. Part C, Emerging Technologies,* 137, 103423. doi: 10.1016/j.trc.2021.103423

Welsh, S. (2020). Canva Security Incident – May 24 FAQs. https://www.canva.com/help/article/incident-may24, Date Accessed 7 June 2021

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Paper presented at the HCI for Cybersecurity, Privacy and Trust*, Virtual Event.

Wiafe, I., Koranteng, F. N., Wiafe, A., Obeng, E. N., & Yaokumah, W. (2020). The role of norms in information security policy compliance. *Information and Computer Security,* 28(5), 743-761. doi: 10.1108/ICS-08-2019-0095

Williams, E. J., & Polage, D. (2019). How persuasive is phishing email? The role of authentic design, influence and current events in email judgements. *Behaviour & Information Technology,* 38(2), 184-197. doi: 10.1080/0144929x.2018.1519599

Wilson, M., & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program (Standards and Guidelines). From National Institute of Standards and Technology

(NIST) https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf, Retrieved August 2021

Wolff, E. D., Growley, K. M., Lerner, M. O., Welling, M. B., Gruden, M. G., & Canter, J. (2021). Navigating the SolarWinds Supply Chain Attack. *The Procurement Lawyer,* 56(2), 3-28.

Wright, R. T., Johnson, S., & Kitchens, B. (2023). Phishing Susceptibility in Context: A Multilevel Information Processing Perspective on Deception Detection. *MIS Quarterly,* 47(2), 803-832. doi: 10.25300/MISQ/2022/16625

Wu, Y., Edwards, W. K., & Das, S. (2022, 22-26 May). SoK: Social Cybersecurity. *Paper presented at the IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA.

Wulandari, N., Adnan, M. S., & Wicaksono, C. B. (2022). Are You a Soft Target for Cyber Attack? Drivers of Susceptibility to Social Engineering-Based Cyber Attack (SECA): A Case Study of Mobile Messaging Application. *Human Behavior and Emerging Technologies,* 2022, 1-10. doi: 10.1155/2022/5738969

Wynn, C., Smith, L., & Killen, C. (2021). How Power Influences Behavior in Projects: A Theory of Planned Behavior Perspective. *Project Management Journal,* 52(6), 607-621. doi: 10.1177/87569728211052592

Xu, T., & Rajivan, P. (2023). Determining psycholinguistic features of deception in phishing messages. *Information and Computer Security,* 31(2), 199-220. doi: 10.1108/ICS-11-2021-0185

Xu, Y., & Li, H. (2025). Cybersecurity Matters for Primary School Students: A Scoping Review of the Trends, Challenges, and Opportunities. *IEEE Transactions on Learning Technologies,* 18, 513-529. doi: 10.1109/TLT.2025.3564610

Yaacob, W. M. Y. W., Haryani, Z. N., & Zahurin Ma, A. (2021). Identification of Factors Contributing to Online Game Addiction among Adolescents. *Journal of Information and Communication Technology,* 20(4), 565-597. doi: 10.32890/jict2021.20.4.5

Yeşem, K. P., & Hillary, F. (2020). Developing and Implementing a Cybersecurity Course for Middle School. *Paper presented at the National Cyber Summit (NCS) Research Track*, Huntsville, Alabama, USA.

Yi, J., Kim, W., He, D., Hu, H., & Huang, C. (2025). Exploration of the Social-Psychological factors associated with Drivers' engagement in protective cybersecurity behaviors: A TPB-based perspective. *Transportation Research Part F: Traffic Psychology and Behaviour,* 114, 69-85. doi: 10.1016/j.trf.2025.05.025

Yong, A. G., & Pearce, S. (2013). A Beginner's Guide to Factor Analysis: Focusing on Exploratory Factor Analysis. *Tutorials in Quantitative Methods for Psychology,* 9(2), 79-94. doi: 10.20982/tqmp.09.2.p079

Yulianto, S., Soewito, B., Gaol, F. L., & Kurniawan, A. (2025). Enhancing cybersecurity resilience through advanced red-teaming exercises and MITRE ATT&CK framework integration: A paradigm shift in cybersecurity assessment. *Cyber Security and Applications,* 3, 100077. doi: 10.1016/j.csa.2024.100077

Yunos, Z., Ahmad, R., Suid, S. H., & Ismail, Z. (2010, 23-25 August). Safeguarding Malaysia's critical national information infrastructure (CNII) against cyber terrorism: Towards development of a policy framework. *Paper presented at the 2010 Sixth International Conference on Information Assurance and Security*, Atlanta, USA.

Yusuf, S., Teimouri, M., Ibrahim, M. S., Ibrahim, N. Z. M., Nazri, S. M., & Victor, S. A. (2023). Let's Think They are Safe Online! A Malaysian Perspective on The Classification of Children's Cyber Risks. *Intellectual Discourse,* 31(1), 139-160. doi: 10.31436/id.v31i1.1864

Zaharon, N. F. M., Ali, M. M., & Hasnan, S. (2021). Factors affecting awareness of phishing among generation Y. *Asia-Pacific Management Accounting Journal (APMAJ),* 16(2), 410-444.

Zainudin, A. (2012). Research methodology and data analysis second edition. In. Universiti Teknologi MARA (UiTM) Press.

Zhang, Y.-Y., Chen, J.-J., Ye, H., & Volantin, L. (2020). Psychological effects of cognitive behavioral therapy on internet addiction in adolescents: A systematic review protocol. *Medicine (Baltimore),* 99(4), e18456. doi: 10.1097/md.0000000000018456

Zhao, X., Xu, W., Ma, J., & Gao, Y. (2018). The "PNE" driving simulator-based training model founded on the theory of planned behavior. *Cognition, Technology and Work,* 21(2), 287-300. doi: 10.1007/s10111-018-0517-8

Zimba, A., Mukupa, G., & Chama, V. (2024). On emergent mobile phone-based social engineering cyberattacks in developing countries: The case of the Zambian ICT sector. *African Journal of Science, Technology, Innovation and Development,* 16(6), 774-791. doi: 10.1080/20421338.2024.2387886

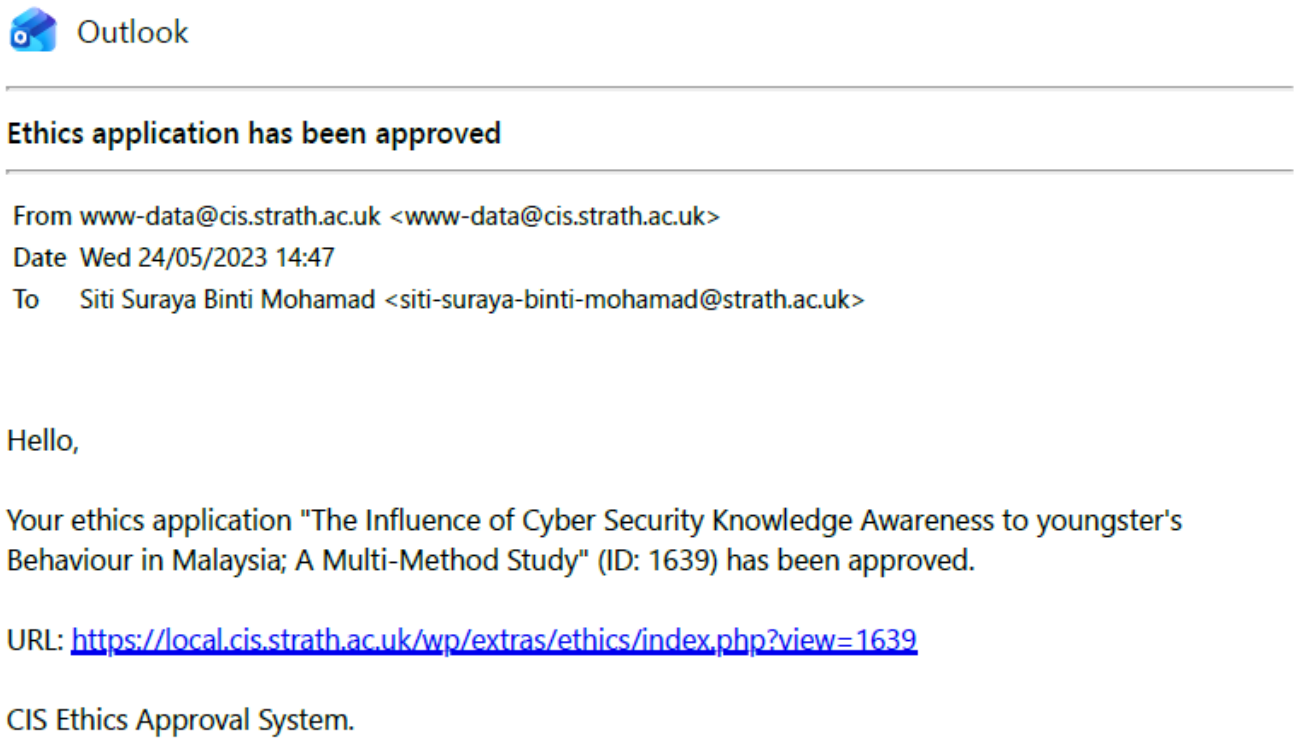
Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies,* 131, 169-187. doi: 10.1016/j.ijhcs.2019.05.005

Zojer, G. (2020). Moving the Human Being Into the Focus of Cybersecurity. In M. Salminen, G. Zojer, & K. Hossain (Eds.), *Digitalisation and Human Security: A Multi-Disciplinary Approach to Cybersecurity in the European High North* (pp. 353-363). Retrieved from 10.1007/978-3-030-48070-7_13

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems,* 62(1), 82-97. doi: 10.1080/08874417.2020.1712269

Appendix

A. First Phase Ethic Approval (ID:1639)



Outlook

Ethics application has been approved

From www-data@cis.strath.ac.uk <www-data@cis.strath.ac.uk>
Date Wed 24/05/2023 14:47
To Siti Suraya Binti Mohamad <siti-suraya-binti-mohamad@strath.ac.uk>

Hello,

Your ethics application "The Influence of Cyber Security Knowledge Awareness to youngster's Behaviour in Malaysia; A Multi-Method Study" (ID: 1639) has been approved.

URL: https://local.cis.strath.ac.uk/wp/extras/ethics/index.php?view=1639

CIS Ethics Approval System.

B. Consent form for survey

Consent Form for Survey

Name of department: Computer and Information Science
Title of the study: The Influence of Cyber Security Knowledge Awareness to youngster's Behaviour in Malaysia; A Multi-Method Study

- I confirm that I have read and understood the Participant Information Sheet for the above project and the researcher has answered any queries to my satisfaction.
- I confirm that I have read and understood the Privacy Notice for Participants in Research Projects and understand how my personal information will be used and what will happen to it (i.e. how it will be stored and for how long).
- I understand that my participation is voluntary and that I am free to withdraw from the project at any time, up to the point of completion, without having to give a reason and without any consequences.
- I understand that I can request the withdrawal from the study of some personal information and that whenever possible researchers will comply with my request. This includes the following personal data:
    - By continuing with this survey, you agree to provide your personal email address in order to proceed to the next question. Your email address will only be used for the purpose of this survey and will be kept confidential and secure. You have the right to withdraw at any time before submitting your email address, and you may choose not to complete the survey if you do not wish to provide your email address.
    - Your email address will only be used for this research purposes only and will be destroyed after the data has been collected.
- I understand that anonymised data (i.e. data that do not identify me personally) cannot be withdrawn once they have been included in the study.
- I understand that any information recorded in the research will remain confidential and no information that identifies me will be made publicly available.
- I consent to being a participant in the project.

Name:	
Signature of Participant:	Date:

C. Participant information sheet for survey

Participant Information Sheet for Survey

Name of department: Computer and Information science
Title of the study: The Influence of Cyber Security Knowledge Awareness to youngster's Behaviour in Malaysia; A Multi-Method Study

Introduction
My name is Siti Suraya Binti Mohamad, a PhD student at the University of Strathclyde in the department of Computer and Information Science. My supervisor is Dr. Karen Renaud, from the same department at the University of Strathclyde.

I would like to invite you to participate in this research survey. I am doing research in cyber security knowledge awareness to behavioural factors to youngsters in Malaysia. I would like to get the respondent for my survey from the youngsters in Malaysia, particularly from 18- to 26-year-olds.

Participation in this study is voluntary. Before you make any decision on participation, I would like to explain the research to you and what your participation will entail. Please read this information sheet and make sure you understand the content before proceeding or withdrawing from this study I am pleased to discuss this information sheet further with you if needed, in helping you decide to participate in this study or not (please see end of this information sheet for my contact details).

What is the purpose of this research?
It is proved that we use internet and electronic devices in our daily life. While cyber-attacks are now notably increased over the years, the complexity of cyber-attack has evolved to a more non-technical method, which is social engineering. Social engineering attack in cyber security has been the main topic for the biggest cyber threats world widely. With manipulation of scenarios to look legitimate to a native and active internet user, is the easiest modus operandi from the attacker.

There are significant proved from previous research that the lack of cyber security knowledge from the users has led to them behave poorly. In addition, it is uncertain that whether they will behave carefully if they have cyber security knowledge awareness. Current research indicated as the main threat in cyber security is youngsters, as they are the most active users in cyberspace, and possessed the highest number of people being the victim of it, especially in the phishing attack.

Hence, this study investigates cyber security knowledge awareness towards youngster's behaviour in Malaysia. This study investigates the attitude, subjective norms, perceived behavioural control, and intention in behavioural, and the connection of cyber security knowledge awareness to youngsters in Malaysia.

Do you have to take part?
No. this survey is voluntary, there are no obligation to participate or to finish the survey, should the respondents wish to withdraw up until the final submission of their responses and. The survey strictly confidential and anonymous.

What will you do in the project?
The survey will take approximately ten minutes maximum to completion. The survey will be active for seven days and between the time, participants can participate in the survey. The survey can be open via a link provided through their smartphones and laptop. The survey consisted of questionnaires that participants will answer.

Why have you been invited to take part?
You have been invited to take part of this study because the survey is intended for Malaysian youngsters between the age of 18 until 25 years old. Exclusion shall be made to people below 18 for legal issue and 25 above as the research aim to investigate youngsters.

What information is being collected in the project?
For the survey, there will be three sections of the questionnaire, each represent difference factor. The first section is the demographic background, second section will investigate the knowledge awareness and the last section will investigate the behavioural section. There will not be any right or wrong answer to the questions, and participants shall answer to the questions without anybody's possession. This is because, the researcher would like to investigate as accurate as possible based on their answer to the question. Not to mention that the respondent is required to provide their email address, as the survey analysis will be used for authorised phishing simulation later.

Please be aware that in order to proceed with the survey, respondents must provide a valid email address. Email address will only be used for the purpose of this research. We understand that some participants may be uncomfortable providing their email address, and therefore respondents have the right to withdraw at any time before submitting email address, and they may choose not to complete the survey if they do not wish to provide with email address. We take privacy and confidentiality seriously and will ensure that email address is kept confidential and secure. We will not share your email address with any third parties or use it for any purposes other than those outlined in this consent statement. The email address will be destroyed after we sent out the phishing simulation right after the survey.

Who will have access to the information?
Only below-mentioned researchers (Dr Karen Renaud, Siti Suraya Binti Mohamad) will have access to the data. It is possible that the data may be used by the below-mentioned researchers for other similar ethically approved research protocols, where the same standards of confidentiality will apply. The data will not be shared (unless approved by the academic main supervisor, Dr Karen Renaud).

Where will the information be stored and how long will it be kept for?
The collected data will be stored and kept for as long as it is required by involved researchers. After that, the data will be securely deleted. The collected data will be stored privately at a secured location within the University of Strathclyde Department of Computer and Information Sciences. The location will be provided by principal supervisor Dr. Karen Renaud. The location will be password protected and under the umbrella of University of Strathclyde network and data protection. Data analysed will be kept in the thesis.

What happens next?
If you are happy to be involved in this project, please read, and then complete the following consent form and then we can proceed to begin the experiment. Otherwise, we thank you for your time and attention.

Alternatively, if a potential respondent would like to participate or to find out more information about this research, they may contact the researcher. The researcher's contact details can be found below. Potential participants will be given a consent form to participate in the survey.

Researcher contact details:
If there is any need to contact the researchers, you can use any of the following means:

Name: Siti Suraya Binti Mohamad
Department: Computer and Information Sciences,
Email address: siti-suraya-binti-mohamad@strath.ac.uk
Address: The University of Strathclyde,
Livingstone Tower, LT 12-16
26 Richmond Street,
Glasgow, G1 1XH,
U.K.

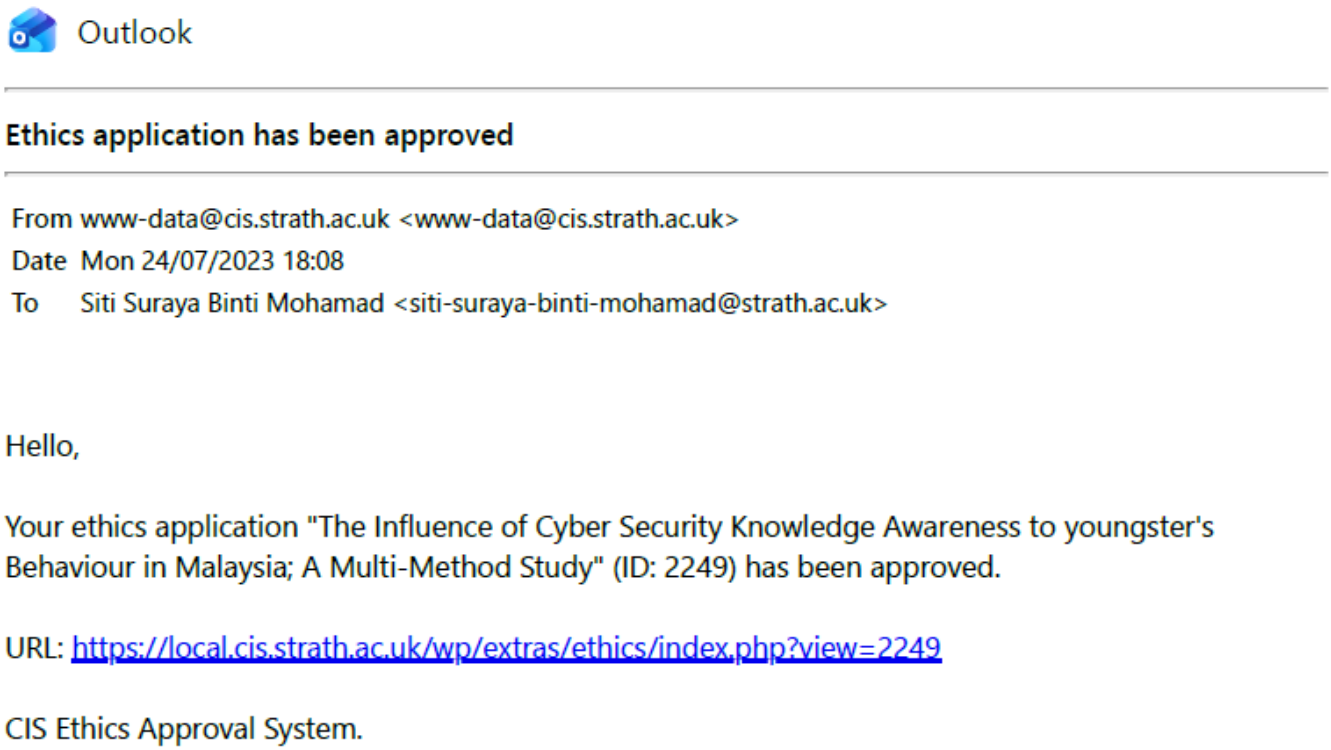
Academic Main Supervisor:
Name: Dr. Karen Renaud
Department: Department of Computer and Information Sciences
Address: 26 Richmond Street, Glasgow G1 1XH, Scotland, United Kingdom
Email: karen.renaud@strath.ac.uk

Chief Investigator details:
This research was granted ethical approval by Departmental Ethics Committee- Computer and Information Sciences. If you have any questions or concerns, before, during or after the investigation, or wish to contact an independent person to whom any questions may be directed or further information may be sought from, contact details are provided below:

Departmental Ethics Committee-Computer and Information Sciences
University of Strathclyde
Livingstone Tower
26 Richmond Street
Glasgow
G1 1XH
Scotland, United Kingdom

Phone Number- +44 141 548 3189
Email Address- ethics@cis.strath.ac.uk

D. Second Phase Ethic Approval (ID:2249)



Outlook

Ethics application has been approved

From www-data@cis.strath.ac.uk <www-data@cis.strath.ac.uk>
Date Mon 24/07/2023 18:08
To Siti Suraya Binti Mohamad <siti-suraya-binti-mohamad@strath.ac.uk>

Hello,

Your ethics application "The Influence of Cyber Security Knowledge Awareness to youngster's Behaviour in Malaysia; A Multi-Method Study" (ID: 2249) has been approved.

URL: https://local.cis.strath.ac.uk/wp/extras/ethics/index.php?view=2249

CIS Ethics Approval System.

E. Consent form for phishing email simulation

Consent Form for Phishing Simulation

Name of department: Computer and Information Science
Title of the study: The Influence of Cyber Security Knowledge Awareness to youngster's Behaviour in Malaysia; A Multi-Method Study

- I confirm that I have read and understood the Participant Information Sheet for the above project and the researcher has answered any queries to my satisfaction.
- I confirm that I have read and understood the Privacy Notice for Participants in Research Projects and understand how my personal information will be used and what will happen to it (i.e. how it will be stored and for how long).
- I understand that my participation is voluntary and that I am free to withdraw from the project at any time, up to the point of completion, without having to give a reason and without any consequences.
- I understand that I can request the withdrawal from the study of some personal information and that whenever possible researchers will comply with my request. Ensure that the data will only be used for this research purposes only and will be destroyed after the data has been collected, the following personal data as below:
    - Email address
    - IP addresses
    - Geolocation data
- I understand that anonymised data (i.e. data that do not identify me personally) cannot be withdrawn once they have been included in the study.
- I understand that any information recorded in the research will remain confidential and no information that identifies me will be made publicly available.
- I consent to being a participant in the project.

Name:	
Signature of Participant:	Date:

F. Participant information sheet for phishing email simulation

Participant Information Sheet for Phishing Simulation

Name of department: Computer and Information science
Title of the study: The Influence of Cyber Security Knowledge Awareness to youngster's Behaviour in Malaysia; A Multi-Method Study

Introduction
My name is Siti Suraya Binti Mohamad, a PhD student at the University of Strathclyde in the department of Computer and Information Science. My supervisor is Dr. Karen Renaud, from the same department at the University of Strathclyde.

I am doing research in cyber security knowledge awareness to behavioural factors to youngsters in Malaysia.

What is the purpose of this research?
The main objective of the research generally is to investigates cyber security knowledge awareness towards youngster's behaviour in Malaysia. While the primary objective of conducting phishing simulations is not to perpetrate deceitful people but rather to enhance their awareness and ability in identifying and appropriately responding to phishing attacks particularly. In this case in particular, to identify youth that are susceptible to phishing attack, to accurately find the comparison between both data gathered (first phase: survey and second phase: simulation).

The topic of social engineering attacks in the field of cyber security has garnered significant attention as one of the most prominent cyber threats on a global scale. The incidence of cyber-attacks has demonstrated a marked escalation over time, with the nature of these attacks evolving towards a less technical modality, namely social engineering. The most straightforward approach for an attacker is using manipulation in a manner that appears legitimate.

There are significant proved from the lack of cyber security awareness from the users has led to the increase of phishing attack. In addition, it is uncertain that whether they will behave carefully even if they have cyber security knowledge. Current research indicated the main threat in cyber security is youngsters, as they are the most active users in cyberspace, and possessed the highest number of people being the victim of it, especially in the phishing attack.

Do you have to take part?
Although your email address was obtained prior to the phishing simulation, it is crucial to acknowledge that your involvement in the simulation is still completely voluntary. The email address were collected through survey previously, where individuals willingly provided their contact information.

The importance of upholding participants' freedom of choice and securing their informed consent throughout the process is well acknowledged. Hence, we would like to ensure that your participation in this phishing simulation is completely voluntary. The participation of the user is highly valued and their willingness to engage in this educational exercise is greatly appreciated. The purpose of this exercise is to increase the user's awareness of phishing attacks and to improve the cybersecurity measures to youth in Malaysia, in particular.

In the event that you opt to refrain from participating in the simulation or decide to retract your consent, kindly inform us, and we will guarantee your exclusion from the simulation. We express our gratitude for your comprehension and eagerly anticipate your engagement, in the event that you choose to be involved.

What will you do in the project?
Since we used a simple random sampling technique, should a computer-generated picked participant's email address, the simulated phishing email will be distributed to the participants. It is recommended to diligently interact with the email based on your judgment. Observe various elements in the email, including the identity of the sender, the textual content of the email, the subject line, and any addition resources such as attachments or hyperlinks. If participants interact with the email, participants are directed to a simulated phishing landing page, however, we can assure that no confidential data will be collected.

Why have you been invited to take part?
Since the participants took part with the survey earlier on, where their email addresses were collected. Therefore, because of prior engagement in the survey, the email was included in the pool of potential participants for this phishing simulation. Simulation employed a technique known as simple random sampling in order to choose the participants.

This methodology ensured that each member of the designated population was afforded an equitable opportunity for selection. The objective of utilising this approach was to establish a heterogeneous and inclusive cohort of respondents, guaranteeing equitability and objectivity across the recruitment procedure.

The principal aim of our initiative is to furnish a worthwhile educational encounter that fosters an understanding of cybersecurity and facilitates the safeguarding of youth in Malaysia.

What information is being collected in the project?

- Addresses: The collection of email addresses of participants or targeted individuals is conducted for the purpose of disseminating phishing emails. However, we have collected all emails in our survey
- Email response data: Monitors the response to the phishing email, encompassing their engagement with what the phishing simulation design whether it is in hyperlinks, attachments, and disclosure of confidential data.
- IP addresses: The logging of IP addresses associated with participant interaction with phishing emails. This data aids in the identification of the participant's location or network.
- User agent information: The collection of user information, the web browser, is what we are planning to collect. The aforementioned data offers valuable insights regarding the technological and software preferences of the individuals involved. In addition, the reason why we would like to gather user's web browser is that it is assisting in the evaluation of the coherence of simulated phishing emails across diverse platforms.
- Geolocation data: This data assists in analysing the geographic distribution of participants and their response patterns.

Who will have access to the information?

Only below-mentioned researchers (Dr Karen Renaud, Siti Suraya Binti Mohamad) will have access to the data. It is possible that the data may be used by the below-mentioned researchers for other similar ethically approved research protocols, where the same standards of confidentiality will apply. The data will not be shared (unless approved by the academic main supervisor, Dr Karen Renaud).

Where will the information be stored and how long will it be kept for?

Data that have been collected will be stored and kept for as long as it is required by involved researchers. After that, the data will be securely deleted. The collected data will be stored privately at a secured location within the University of Strathclyde Department of Computer and Information Sciences. The location will be provided by principal supervisor Dr. Karen Renaud. The location will be password protected and under the umbrella of University of Strathclyde network and data protection. Data analysed will be kept in the thesis.

What happens next?

We thank you for your time and attention. Alternatively, if a potential respondent would like to participate/opt out or to find out more information about this research, they may contact the researcher. The researcher's contact details can be found below. Potential participants will be given a consent form to participate in the survey.

Researchers contact details:
If there is any need to contact the researchers, you can use any of the following means:

Name: Siti Suraya Binti Mohamad
Department: Computer and Information Sciences,
Email address: siti-suraya-binti-mohamad@strath.ac.uk
Address: The University of Strathclyde,
Livingstone Tower, LT 12-16
26 Richmond Street,
Glasgow, G1 1XH,
U.K.

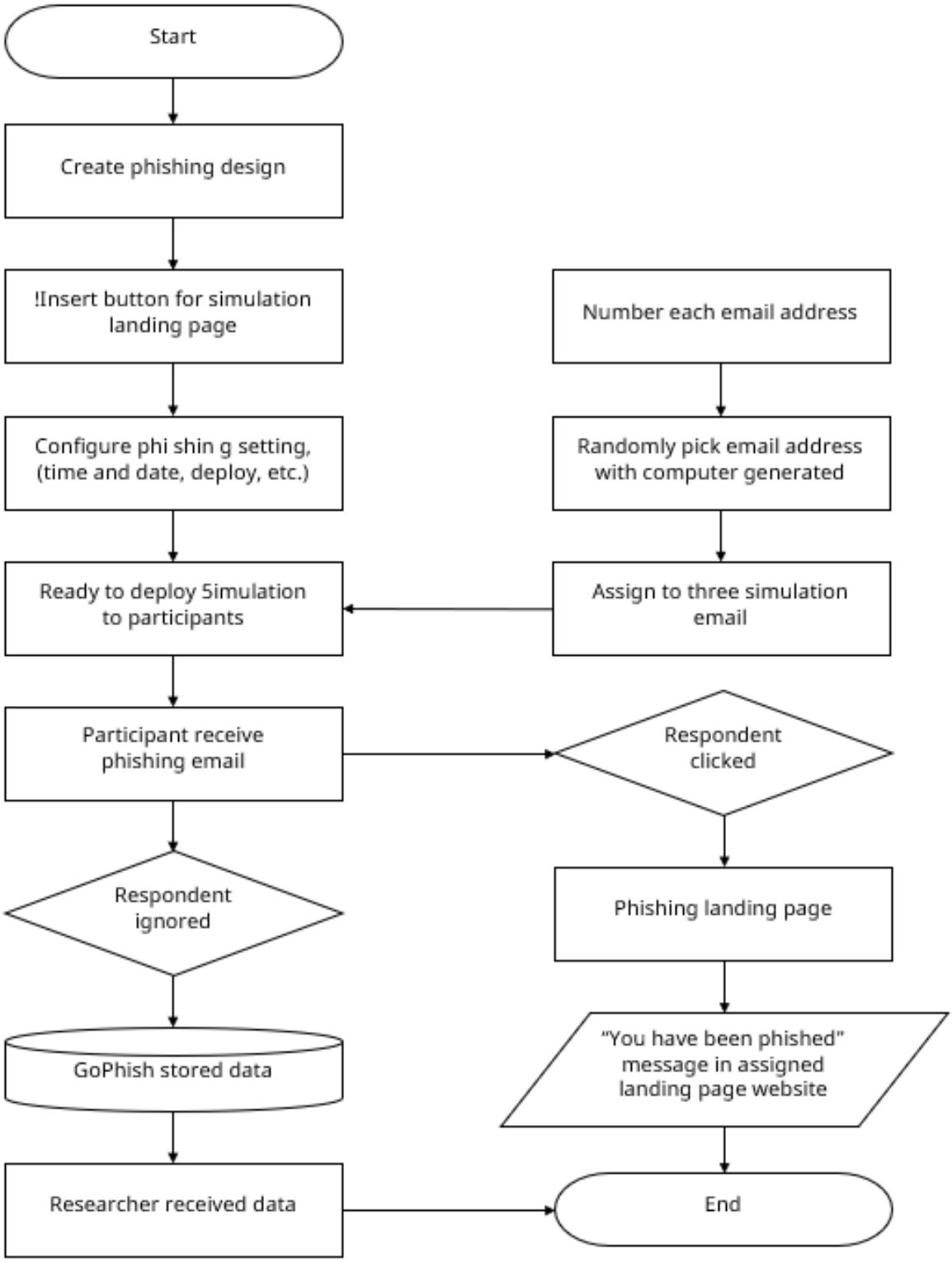
Academic Main Supervisor:
Name: Dr. Karen Renaud
Department: Department of Computer and Information Sciences
Address: 26 Richmond Street, Glasgow G1 1XH, Scotland, United Kingdom
Email: karen.renaud@strath.ac.uk

Chief Investigator details:
This research was granted ethical approval by Departmental Ethics Committee- Computer and Information Sciences. If you have any questions or concerns, before, during or after the investigation, or wish to contact an independent person to whom any questions may be directed or further information may be sought from, contact details are provided below:

Departmental Ethics Committee-Computer and Information Sciences
University of Strathclyde
Livingstone Tower
26 Richmond Street
Glasgow
G1 1XH
Scotland, United Kingdom

Phone Number- +44 141 548 3189
Email Address- ethics@cis.strath.ac.uk

G. Phishing simulation email flowchart



H. Qualtrics Survey

English (United Kingdom)

Participant Acknowledgement

Dear respondents:

I am doing academic research titled:
"The Influence of Cyber Security Knowledge Awareness to youngster's Behaviour in Malaysia; A Multi-Method Study"

You have been invited as a respondent for this study. Your sincere cooperation is crucial in determining the success of this study. In this study, I would like to access your perception concerning certain factors towards the effectiveness of cybersecurity awareness in Malaysia. Please read carefully all the instructions pertaining to every section and answer every question sincerely. There is no right or wrong answer.

The questions are classified into three sections:
Section A: Youngster's demographics background
Section B: Cybersecurity knowledge awareness practices
Section C: Youngster's behaviour
All responses provided will be treated with strict confidentiality and will be used for this academic research only. Thank you very much for your time and cooperation.

This survey is being conducted for Ph.D. research at the University of Strathclyde, United Kingdom. Should you have any questions about the study or you wish to receive a copy of the results, please contact the researcher via the address or email below:
siti--suraya-binti-mohamad@strath.ac.uk

Sincerely,
Ts. Siti Suraya Binti Mohamad
Department of Computer and Information Science
University of Strathclyde Glasgow, Scotland

A note on privacy This survey is anonymous. The record kept of your survey responses does not contain any identifying information about you unless a specific question in the survey has clearly asked for this. All answers will be treated confidentially and respondents will be anonymous during the collection, storage, and publication of research material. Once the survey has been taken offline, participant responses will be extracted, statistically analyzed, and published in a Ph.D. thesis, and may be used in a suitable academic journal. Your responses will be treated as confidential at all times and data will be presented in such a way that your identity cannot be connected with specific published data. This survey is designed for adult participation. **If you are under 18 years, please do not answer this survey**. Anyone 18 years old or above can take part in the survey and has the right to withdraw up until the final submission of their responses. **If you click 'Next', you confirm that you have read and understood the information given, understand that you are free to withdraw up until the point of submission of your responses, you are 18 years or above, and agree to take part in the study**.

Demographic background

Please provide your age

- ○ 18-19
- ○ 19-20
- ○ 21-22
- ○ 23-24
- ○ 25-26
- ○ Over 26

Kindly provide your gender

- ○ Male
- ○ Female
- ○ Prefer not to say

Kindly select your education background

- ○ High school
- ○ Diploma
- ○ Bachelors Degree
- ○ Masters degree
- ○ Doctoral degree

Kindly provide your email address (Please note that your provided email may receive an authorised phishing simulation at any time. No sensitive data will be collected.)

CSKA

Please respond to each of the following questions in the manner that best reflects your cyber security knowledge awareness practices. Please read the question carefully.

	Never	Sometimes	About half the time	Most of the time	Always
Do you use a password manager to keep track of your passwords? (E.g., 1Password, LastPass, Dashlane, etc)	○	○	○	○	○
How frequently do you use additional security measures to protect your online accounts (e.g., 2-step verification, etc) for at least one of the online accounts?	○	○	○	○	○
How often do you disclose confidential information (e.g. Identification Number (ID), credit card number, CVV number, etc)	○	○	○	○	○
How frequently do you include personal information such as your name, last name, date of birth, etc., when creating your passwords?	○	○	○	○	○
How often do you use a combination of uppercase and lowercase letters (e.g. aBc, ABC, or abc, etc), numbers (e.g., 123, etc), and special characters (e.g., !@+, etc) n your passwords?	○	○	○	○	○

Please respond to each of the following questions in the manner that best reflects your cyber security knowledge awareness practices. Please read the question carefully.

	Never	Sometimes	About half the time	Most of the time	Always
You update applications/systems to the latest version (e.g. operation systems (OS) , applications, etc.)	○	○	○	○	○
You use antivirus software (E.g. Microsoft defender, McAfee, Kaspersky, Norton, etc)	○	○	○	○	○
You clear Browser Cookies (e.g. username, password, bank account details, etc)	○	○	○	○	○
You use pop-up blocker (e.g., AdBlock, AdGuard, Opera Browser, etc.)	○	○	○	○	○
Your anti-virus software is up to date (e.g. manually or turned on automatic update)	○	○	○	○	○
If you're paying attention, click Sometimes	○	○	○	○	○

Please respond to each of the following questions in the manner that best reflects your cyber security knowledge awareness practices. Please read the question carefully.

	Never	Sometimes	About half the time	Most of the time	Always
How frequently do you enter your password after clicking on a link in an email and that link takes you to a website	○	○	○	○	○
Do you regularly check if the website you are visiting uses HTTPS?	○	○	○	○	○

	Never	Sometimes	About half the time	Most of the time	Always
How frequently do you look at the URL bar to verify your visit to the website?	○	○	○	○	○
Do you open emails or attachments from unknown sources	○	○	○	○	○
Do you visit websites you have not heard of?	○	○	○	○	○

Please respond to each of the following questions in the manner that best reflects your cyber security knowledge awareness practices. Please read the question carefully.

	Never	Sometimes	About half the time	Most of the time	Always
Organization organizes security talks	○	○	○	○	○
Organization constantly remind to practice computer security	○	○	○	○	○
Organization distributes security newsletters or articles	○	○	○	○	○
If you're paying attention, click Never	○	○	○	○	○
Organization's Information Technology helpdesk sends out alert messages/emails concerning security	○	○	○	○	○
Work device(s) is monitored by administrator	○	○	○	○	○

Please respond to each of the following questions in the manner that best reflects your cyber security knowledge awareness practices. Please read the question carefully.

	Never	Sometimes	About half the time	Most of the time	Always
Know how to report cybercrime (e.g. Cyber999, National Scam Response Centre (NSRC), Malaysian Communication and Multimedia Commission (MCMC), etc.)	○	○	○	○	○
Exposed to cyber security knowledge through past education (e.g. high school, universities, etc.)	○	○	○	○	○
Exposed to cyber security policy in Malaysia (e.g. Malaysia Cyber Security Strategy 2020-2024, National Cyber Security Policy in Malaysia, National Cyber Exercise in Malaysia, etc.)	○	○	○	○	○
Exposed to cyber security practices through government initiatives (e.g. Cyber Security and Awareness for Everyone (CyberSAFE), national cyber exercise in Malaysia, etc.)	○	○	○	○	○
Have ever encountered any cyber-attack(s)? (e.g. Phishing attack, malware and virus attack, ransomware attack, etc.)	○	○	○	○	○

TPB

Please answer each of following question that best describe your opinion. Some of the question may appear to be similar, but they do address somewhat different issues. Please read each question carefully.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
To me, cyber security knowledge awareness practices will affect cyber behavior	○	○	○	○	○	○	○
It is important to always behave accordingly in cyberspace	○	○	○	○	○	○	○
It is important to at all times to adhere to cybersecurity knowledge awareness	○	○	○	○	○	○	○
To me, I behave differently if I have cyber security knowledge awareness	○	○	○	○	○	○	○

Please answer each of following question that best describe your opinion. Some of the question may appear to be similar, but they do address somewhat different issues. Please read each question carefully.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
My family and friends think that cyber security knowledge awareness will affect cyber behavior	○	○	○	○	○	○	○
Most people around me obey to cybersecurity knowledge awareness	○	○	○	○	○	○	○
My surrounding think that I behave differently if I have cyber security knowledge awareness	○	○	○	○	○	○	○

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
Most people around me think that it is important to behave accordingly in cyberspace	○	○	○	○	○	○	○

Please answer each of following question that best describe your opinion. Some of the question may appear to be similar, but they do address somewhat different issues. Please read each question carefully.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
I find it easy to ensure that I always comply with the cybersecurity knowledge awareness	○	○	○	○	○	○	○
I find it easy to behave differently if I have cyber security knowledge	○	○	○	○	○	○	○
I find it easy to ensure I behave accordingly in cyberspace	○	○	○	○	○	○	○
Following cyber security knowledge awareness affecting my cyber behavior	○	○	○	○	○	○	○

Please answer each of following question that best describe your opinion. Some of the question may appear to be similar, but they do address somewhat different issues. Please read each question carefully.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
I expect to behave differently if I have cyber security knowledge	○	○	○	○	○	○	○

	Strongly disagree	Disagree	Somewhat disagree	Neither agree nor disagree	Somewhat agree	Agree	Strongly agree
I plan to always comply to cybersecurity knowledge awareness	○	○	○	○	○	○	○
If you're paying attention, click Disagree	○	○	○	○	○	○	○
I expect to follow cyber security knowledge awareness for my cyber behavior	○	○	○	○	○	○	○
I plan to always behave accordingly in cyberspace	○	○	○	○	○	○	○

Additional Information (e.g What do you think about cybersecurity in Malaysia)

https://www.qualtrics.com/powered-by-qualtrics

I. Codebook Portion

The codebook portions

Variable Label	Variable Name	Values: Level and Codes
Age	Age	1= "18" 2= "19-20" 3= "21-22" 4= "23-24" 5= "25-26" 6=" Over 26"
Gen	Gender	1=" Male" 2=" Female" 3=" Prefer not to say"
LOEdu	Level of education	1=" High school" 2= "Diploma" 3=" bachelor's degree" 4= "master's degree" 5= "Doctoral degree"
Email	Email	
Att1, Att2, Att3	Attention response	
PassSec1, PassSec2, PassSec3, DataSec4, PassSec5,	Password security	
SoftSysSec1, SoftSysSec2, SoftSysSec3, SoftSysSec4, SoftSysSec5,	Software/system security	
HumSec1, HumSec2, HumSec3, HumSec4, HumSec5,	Human security	1= "Never" 2= "Sometimes" 3= "About half the time" 4= "Most of the time" 5= "Always"
OrgSec1, OrgSec2, OrgSec3, OrgSe4, OrgSec5,	Organization security	
SocioSec1, SocioSec2, SocioSec3, SocioSec4, SocioSec5,	Social Security	
YoungATT1, YoungATT2, YoungATT3, YoungATT4,	Youngster's attitude	1=" Strongly disagree" 2= "Disagree" 3= "Somewhat disagree"

YoungSP1, YoungSP2, YoungSP3, YoungSP4,	Youngster's surrounding pressure	4=" Neither agree nor disagree" 5= "Somewhat agree" 6= "Agree" 7= "Strongly agree"
YoungPC1, YoungPC2, YoungPC3, YoungPC4,	Youngster's perceived control	
YoungCCI1, YoungCCI2, YoungCCI3, YoungCCI4,	Youngster's cyber cautiousness intention	
AddQue	Additional question	

J. Open ended answer

Participant's ID	Age Group	Gender	Education Level	Additional Information
P1	25-26	Male	Diploma	We need need to be exposed more about awareness in cybersecurity especially in our age where we use internet access all the time
P2	21-22	Male	Doctoral	We need to be exposed more to cybersecurity awareness because the amount of awareness that my surroundings and I received were still low.
P3	23-24	Female	Bachelor	Nothing to add on. But, I like the in between question to check our focus
P4	23-24	Female	Master D	Terima kasih atas info tersebut sangat berguna masa kini lebih berhati-hati penyebaran info tersebut.
P5	23-24	Female	Bachelor	I am working in the training industry which involves cybersecurity program areas. The organization that I worked for cater government & private agency on the cybersecurity awareness which also leads us to be exposed and alert to the cybersecurity activities. Since I have a basic cybersecurity knowledge, all passwords are changed to non dictionary/ no privacy information.
P6	19-20	Female	Bachelor	Please create more awareness on cyber security especially to elderly bcs most of them are lack on awareness about cyber security.
P7	25-26	Female	Bachelor	Please create more awareness on cyber security especially to elderly bcs most of them are lack on awareness about cyber security. Cyber security is really important as it helps to protect my privacy and ensure my cyber life is safe and free from any scams and threats. It is important for kids and adults nowadays to be exposed to the cyber security program and have an awareness of it as it will build a cyber-safe generation in the future. Thank you and good luck for your study.

				Cyber security is really important as it helps to protect my privacy and ensure my cyber life is safe and free from any scams and threats. It is important for kids and adults nowadays to be exposed to the cyber security program and have an awareness of it as it will build a cyber-safe generation in the future. Thank you and good luck for your study.
P8	25-26	Female	High Sch	I'm sorry if the answer given is not up to standard
P9	25-26	Female	Bachelor	Its important for everyone get well educated regarding cybersecurity as the crime increasing now. Its important for everyone get well educated regarding cybersecurity as the crime increasing now.
P10	18	Female	Diploma	Hi, i picked diploma but i'm actually a matriculation student hehe but my age correct la, goodluck in whatever you do and I strongly agree to implement strict security measure when dealing with internet access, may Allah ease everything 🩶
P11	21-22	Female	Bachelor	Good measure to highligh more about cyber security
P12	21-22	Female	Master D	Awareness and knowledge among teenagers/young generation is actually in a high phase compared to the old people/parents. They are exposed and become the target for the scammers especially from Facebook link or messenger.
P13	23-24	Male	Master D	Collecting email but not taking responsibility for the consequences is contradictory of your work. Collect data anonymously, not everything need email
P14	25-26	Female	Master D	Everything is good
P15	19-20	Female	Diploma	I usually detects for scam by using google lens for pictures, CCID web and true caller. I realised that we lack of cybersecurity awareness as ppl around me tend to trust any ppl that try to scam them. I often need to remind them always as im always alert with the scammers.

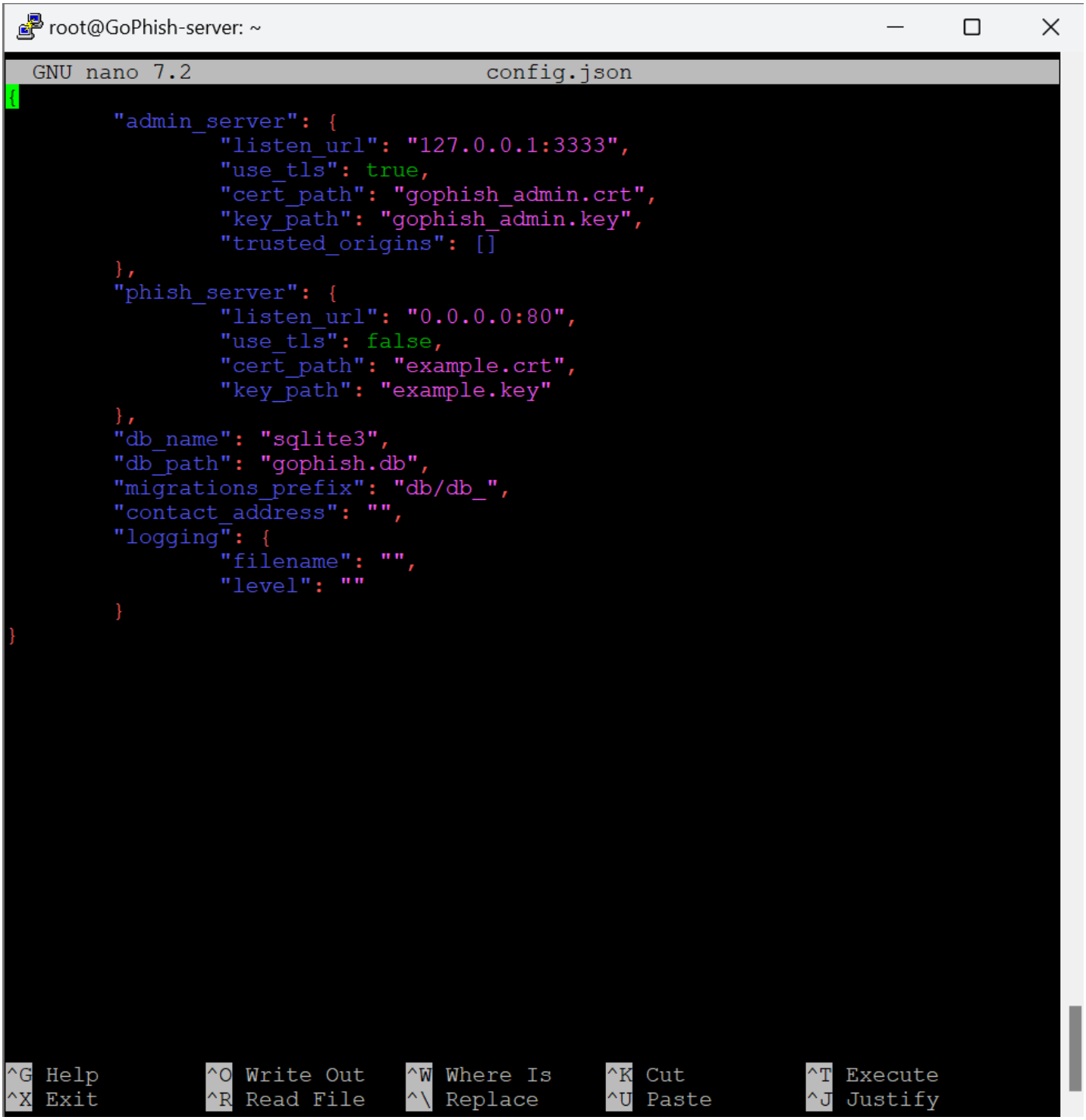
				I usually detects for scam by using google lens for pictures, CCID web and true caller. I realised that we lack of cybersecurity awareness as ppl around me tend to trust any ppl that try to scam them. I often need to remind them always as im always alert with the scammers.
P16	19-20	Female	Diploma	There's still some people even though with high education or good career old or young people still not aware about cyber security and easily got scammed by the scammers. Hope you can spread more awareness about cyber security There's still some people even though with high education or good career old or young people still not aware about cyber security and easily got scammed by the scammers. Hope you can spread more awareness about cyber security
P17	21-22	Female	Master D	I think one of the aspect that affect people to act accordingly towards cyber security are you need to spend lots of money to ensure its secure// gain security.
P18	25-26	Male	Bachelor	People online should be responsible for their actions on the internet, but the anonymity each individual have renders it impossible.
P19	25-26	Male	Bachelor	Goodluck with your survey!
P20	25-26	Female	Bachelor	Awareness on cyber security is still low tbh
P21	23-24	Male	Master D	Good for our enviroment
P22	23-24	Male	Bachelor	Cyber security awareness should be spread more to the elders through programs,infographic because they are the most fragile to pishing attacks etc Cyber security awareness should be spread more to the elders through programs,infographic because they are the most fragile to pishing attacks etc
P23	25-26	Female	Master D	I think cyber security is an important issue and deserve great attention

P24	23-24	Female	Bachelor	Awareness of cybersecurity is important to educate and train employees about the threats that lurk in cyberspace. They also need to know how to prevent such threats and what they must do in the event of a security incident.
P25	25-26	Female	Master D	Cyber security issues demand more attention from many authorities, including the government, employers, and families, because during these day, everyone is exposed to cyber fraud.
P26	25-26	Female	Master D	Cybersecurity is important as it can save us from scammers!
P27	21-22	Female	Master D	Most people don't really expose to cyber security
P28	19-20	Male	Bachelor	Need more enforcement and awareness on cybersecurity to community esp for elders Need more enforcement and awareness on cybersecurity to community esp for elders Need more enforcement and awareness on cybersecurity to community esp for elders
P29	25-26	Female	Bachelor	In Malaysia, exposure to cyber security is still on minimal level especially within primary and secondary school students. In Malaysia, exposure to cyber security is still on minimal level especially within primary and secondary school students.
P30	21-22	Female	Bachelor	More people are not sure what is cyber threat and how to minimise cyber threat
P31	25-26	Male	Bachelor	Hope citizen have more exposure into cyber security awareness
P32	25-26	Female	Doctoral	I hope more organisations aware about cyber security.
P33	19-20	Female	Bachelor	thank you for conducting this study. everyone need this kind of awareness.
P34	19-20	Male	Diploma	I hope government can provide initiative to send awareness to more people about the cyber security as we are moving fast in the modern world
p29				I hope government can provide initiative to send awareness to more people about the cyber security as we are moving fast in the modern world

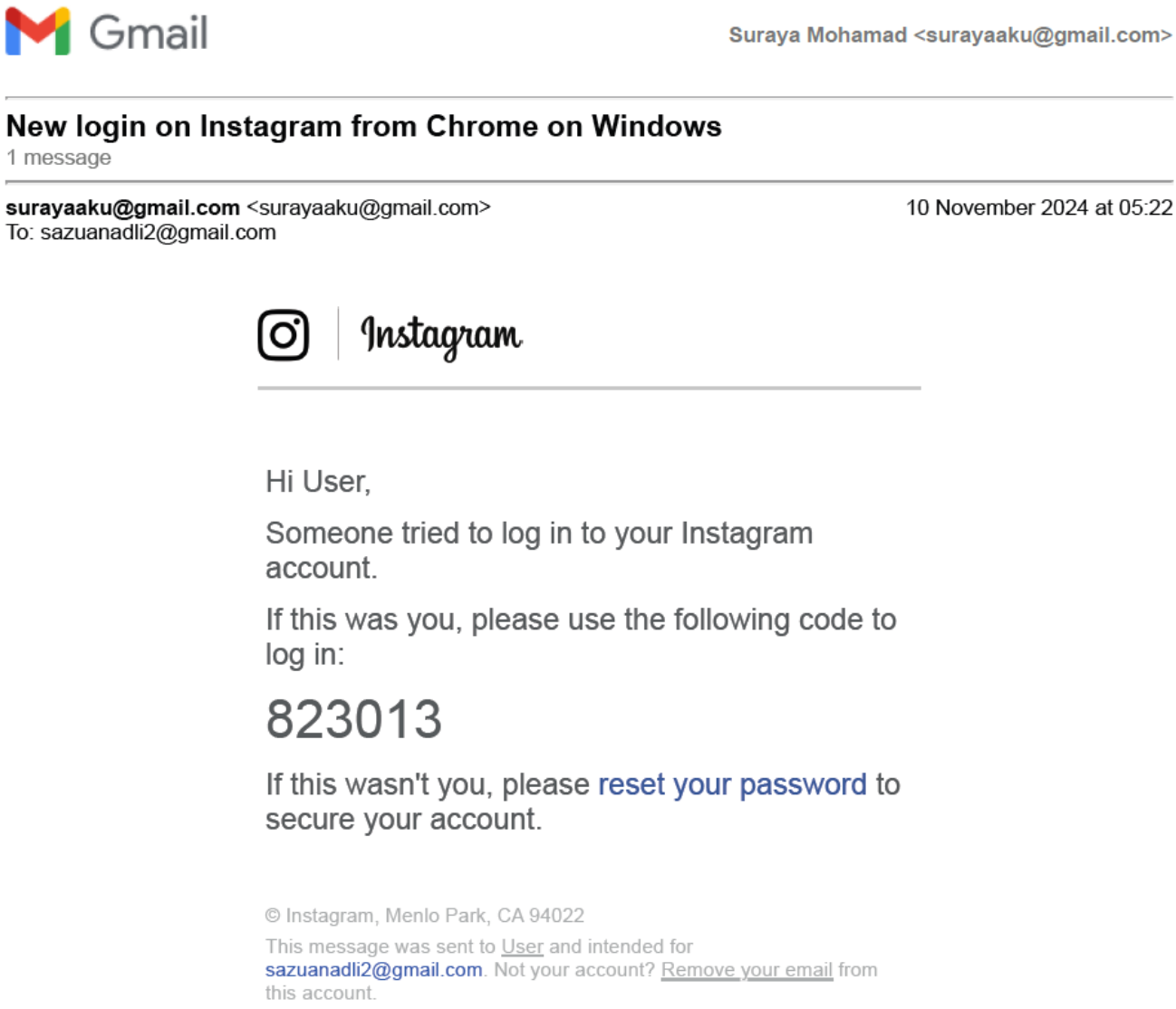
P35	19-20	Female	Bachelor	It seems like most of the authority haven't really focus on cybersecurity eg: government servant. No updated system, no end user monitoring, data leak here and there. It should start with them, the government.
P36	21-22	Female	Bachelor	I think it is better for the knowledge of security is implimented in the education website of university, school and so on to avoid any unethical behaviour among the students. I think it is better for the knowledge of security is implimented in the education website of university, school and so on to avoid any unethical behaviour among the students.
P37	23-24	Male	Bachelor	Cybersecurity is one of critical knowledge nowadays to avoid scammers etc
P38	18	Female	Diploma	I think cybersecurity awareness also important to children and elders as well I think cybersecurity awareness also important to children and elders as well
P39	23-24	Female	Bachelor	Security awareness are important to younger generation nowadays. Need to expose more information regarding security awareness to them to avoid any problems in future Security awareness are important to younger generation nowadays. Need to expose more information regarding security awareness to them to avoid any problems in future Security awareness are important to younger generation nowadays. Need to expose more information regarding security awareness to them to avoid any problems in future
P40	19-20	Female	Bachelor	Need more information of cyber security and free license for security for every devices.
P41	23-24	Female	Bachelor	No enforcement to strengthen cyber security expecially to teenagers No enforcement to strengthen cyber security expecially to teenagers No enforcement to strengthen cyber security expecially to teenagers

P42	25-26	Female	Master D	A proactive measures of cyber security awareness amongs children in school need to be conduct. This is because, children most likely to have gadget and smart phone to mingle around cyberspace with or without parents knowledge. Level of education will also affecting young adult to obey the rules in cyber space. A proactive measures of cyber security awareness amongs children in school need to be conduct. This is because, children most likely to have gadget and smart phone to mingle around cyberspace with or without parents knowledge. Level of education will also affecting young adult to obey the rules in cyber space.
P43	18	Male	Bachelor	Citizen in Malaysia do not have access to awareness in cybersecurity
P44	19-20	Female	Diploma	This is the age where we learn about cybersecurity
P45	18	Male	Bachelor	People sometimes do not know how to react to cybersecurity because they don't really know about it People sometimes do not know how to react to cybersecurity because they don't really know about it
P46	19-20	Male	Bachelor	No proper engagement in cybersecurity
P47	18	Female	Diploma	Cybersecurity is so hard to understand, I only know about update my laptop and my phone
P48	19-20	Male	Diploma	Good prospect to introduce cybersecurity even from high school Good prospect to introduce cybersecurity even from high school
P49	21-22	Female	Diploma	Never heard about cybersecurity awareness until I went to the university, should have more exposure from registered bodies Never heard about cybersecurity awareness until I went to the university, should have more exposure from registered bodies
P50	25-26	Female	Bachelor	Good for our generation if this is implemented from the very young age
P51	23-24	Male	Bachelor	We need more of cybersecurity in our country
P52	19-20	Male	Diploma	Good initiatives, expecially to kids and senior citizens Good initiatives, expecially to kids and senior citizens
P53	23-24	Male	Master D	The government does not expose us to cybersecurity The government does not expose us to cybersecurity
P54	25-26	Female	Bachelor	I only know that cyber-attack is legitimate when I was scam before

K. GoPhish server


root@GoPhish-server: ~
GNU nano 7.2 config.json
{
"admin_server": {
"listen_url": "127.0.0.1:3333",
"use_tls": true,
"cert_path": "gophish_admin.crt",
"key_path": "gophish_admin.key",
"trusted_origins": []
},
"phish_server": {
"listen_url": "0.0.0.0:80",
"use_tls": false,
"cert_path": "example.crt",
"key_path": "example.key"
},
"db_name": "sqlite3",
"db_path": "gophish.db",
"migrations_prefix": "db/db_",
"contact_address": "",
"logging": {
"filename": "",
"level": ""
}
}
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify

L. Three phishing email simulation



Urgent suspicious Activity on your Microsoft Account. UPDATE NOW. Inbox ×

S **sitisurayabm@gmail.com** 12:36 PM (12 minutes ago)

to me

Microsoft Account

Dear Siti Suraya,

Someone in Bogotá, Colombia, attempted to log into your account several times. If you believe this was fraudulent activity, please report it here.

If you do not believe this to be a fraudulent activity, you may ignore this message

Sincerely,

Suraya@Microsoft.com

New sign-in from Chrome OS

Hi Siti Suraya,
Your Google Account sitisurayabm@gmail.com was just used to sign in on Chrome OS.

sitisurayabm@gmail.com

Chrome OS
Tuesday, 25 November 2024 12:54 (British Summer Time)
Leeds, UK*

Don't recognise this activity? if you don't recognise this device click the following place:

click here

Review your recently used devices here

.

Why are we sending this? We take security very seriously, and we want to keep you in the loop on impotant actions in your account.
We were unable to determine whether you have used this browser or device with your account before. This can happen when you sign in for the first time on a new computer, phone, or browser, when you use your browser's incognito or private browsing mode clear your cookies, or when somebody else is accessing your account.

Best,
The Google Accounts team

*The location is approximate and determined by the IP address it was coming from.

M. Participants Feedback

Siti Suraya Binti Mohamad

From: [redacted]
Sent: 19 November 2025 01:32
To: Siti Suraya Binti Mohamad
Subject: Re: Follow-Up Regarding Your Participation in a Ph.D. Research Study

CAUTION: This email originated outside the University. Check before clicking links or attachments.

How often do you check your email?
This email account is dedicated solely to university projects, so I check it only when I am actively engaged in coursework or group assignments.

Do you use any email filters or security tools to manage or screen incoming emails?
No.

Are there any specific signs or red flags that typically make you cautious about opening an email? Red flags for me include emails offer unexpected rewards.

I hope my responses are useful for your analysis. Good luck with your Ph.D. research.

Sent from Yahoo Mail for iPad

On Friday, November 14, 2025, 6:57 AM, Siti Suraya Binti Mohamad <siti-suraya-binti-mohamad@strath.ac.uk> wrote:

> Dear Participants,
>
> I hope this message finds you well.
>
> You recently participated in a simulated phishing email study as part of my Ph.D. research on cybersecurity awareness. I sincerely appreciate your contribution to this important work.
>
> As part of my analysis, I am reaching out to participants who did not open the simulated phishing email. Your perspective is incredibly valuable, as it will help me better understand the factors influencing email interaction behavior. I would be grateful if you could take a moment to answer a few brief questions about your email habits and security practices:
>
> 1. How often do you check your email?
> 2. Do you use any email filters or security tools to manage or screen incoming emails? If so, could you briefly describe them?
> 3. Are there any specific signs or red flags that typically make you cautious about opening an email?

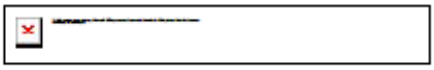
Your responses will remain completely confidential and will only be used for academic research purposes. This follow-up is entirely voluntary, and your decision to respond (or not) will not affect your standing in the study.

If you have any questions or concerns, please don't hesitate to reach out to me by replying to this email or my supervisor Dr Karen Renaud Here.

Thank you once again for your valuable participation and time.

Best regards,

Siti Suraya Binti Mohamad
Postgraduate Student
Computer and Information Sciences,
The University of Strathclyde,
Livingstone Tower, LT 12-17
26 Richmond Street,
Glasgow, G1 1XH,
U.K.
Tel: +44 7920 2555 61
Email: siti-suraya-binti-mohamad@strath.ac.uk
https://www.linkedin.com/in/sitisurayamohamad/



THE QUEEN'S ANNIVERSARY PRIZES
2019 & 2021
For Higher and Further Education

UNIVERSITY OF THE YEAR
2012 & 2019
Times Higher Education

SCOTTISH UNIVERSITY OF THE YEAR
2020
The Times & The Sunday Times

Outlook

Re: Follow-Up Regarding Your Participation in a Ph.D. Research Study

From [redacted]
Date Mon 05/01/2026 15:17
To Siti Suraya Binti Mohamad <siti-suraya-binti-mohamad@strath.ac.uk>

CAUTION: This email originated outside the University. Check before clicking links or attachments.

Thank you for reaching out and for including me in your study. I'm happy to provide some information about my email habits and security practices in response to your questions:

1. How often do you check your email?
I check my email regularly, usually once a day.

2. Do you use any email filters or security tools to manage or screen incoming emails?
Yes, I use the Boxbe email filter to screen incoming messages. It helps prioritize emails from known contacts and filters potential spam into a separate folder.

3. Are there any specific signs or red flags that typically make you cautious about opening an email?
I tend to be cautious if an email comes from an unknown sender and includes links that don't match the supposed sender's domain.

I hope this information is helpful for your research. Please let me know if you need any further details.

Thanks and all the best!

Kind regards,

[redacted]

On Friday, November 14, 2025, 6:57 AM, Siti Suraya Binti Mohamad <siti-suraya-binti-mohamad@strath.ac.uk> wrote: