e-ISSN: 2550-1569

Available online at
https://myjms.mohe.gov.my/index.php/IJSMS

International Journal of Service Management and Sustainability
11(1) 2026, 37 – 56.

International Journal of Service Management and Sustainability (IJSMSust)

The interplay of profiling, social engineering tactics, and situational factors in shaping cybersecurity awareness

Haiqal Shazrin Anuar[1*], Mohd Norhisham Razali@Ghazali[2], Marlita Mat Yusof[3]

[1,2,3]*Faculty of Business and Management, Universiti Teknologi MARA Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia*

ARTICLE INFO

Article history:
Received 16 December 2025
Revised 27 January 2026
Accepted 4 February 2026
Online first
Published 31 March 2026

Keywords:
Social Engineering
Cybersecurity Awareness
Psychological
Victim Profiling
Situational Factors
Protection Motivation Theory

DOI: 10.24191/ijsms.v11i1.24238

Citation in APA:
Anuar, H.S., Razali, M.N., & Mat Yusof, M. (2026). The Interplay of Profiling, Social Engineering Tactics, and Situational Factors in Shaping Cybersecurity Awareness. *International Journal of Service Management and Sustainability, 11*(1), 37 – 56.

ABSTRACT

The rapid expansion of the internet has contributed to a rise in cybercrime, scams, and various emerging threats. The current social engineering framework focuses on technical defences and general risks, but fails to address the psychological tactics of social engineering or the diverse demographic and psychological profiles of victims. To address this gap, this study aims to refine the awareness framework by integrating an analysis of social engineering factors and victim profiles to better measure cybersecurity awareness. The objectives of this study are to identify the most prevalent victim profiles using cluster analysis and examine social engineering factors affecting cybersecurity awareness; and test the moderating role of situational factors in the relationship between social engineering factors and cybersecurity awareness. A structured online survey measuring attack experiences and cybersecurity awareness was distributed to 131 higher-education students in Malaysia. Data were analysed using multiple regression and K-means cluster analysis to identify patterns among the variables. A detailed analysis based on Protection Motivation Theory and Routine Activity Theory provided a more comprehensive explanation of cybersecurity awareness. The findings indicate that social engineering tactics are a major driver of cybersecurity awareness, while place of study and gender emerge as two significant variables in victim profiling. The refined awareness model incorporates psychological, demographic, and situational factors to provide a practical framework for enhancing an individual's defence system and developing an effective, focused cybersecurity awareness programme. These insights offer valuable guidance for policymakers in designing targeted cybersecurity education initiatives, persona-based training modules, and context-aware awareness campaigns for mitigating social engineering risks among vulnerable populations.

[1*] Corresponding author. *E-mail address*: haiqalanuar09@gmail.com

1. INTRODUCTION

The rapid spread of the internet in the modern age of technological advancement has brought about both possibilities and associated threats, such as breaches of privacy through cybercrimes, scams, and data breaches. Cyberattacks have already resulted in significant financial and informational losses, and attackers use social media like Facebook, Instagram, and Twitter to engage in malicious activities (Datta et al., 2020; Deora, 2021) Cybercrime, which includes theft, fraud, and hacking, has increased with the rising use of the internet; thus, the issue of data privacy, especially with sensitive financial data, has become a major concern (Bora, 2023; Omar et al., 2021). Although technology has brought many advantages, personal data protection has become increasingly challenging, and stronger cybersecurity measures are required. Social engineering is a form of human hacking that uses tactics such as phishing and vishing to induce victims to reveal sensitive data (Gomes et al., 2020). These frauds rely on psychological trust and interest, and make people of all demographics susceptible (Montañez et al., 2020). The scale of the problem is further supported by statistics that show a dramatic increase to 877,536 worldwide phishing attacks in 2024 alone (APWG, 2025).

Existing cybersecurity initiatives often lack focus on psychological manipulation and demographic threats, so they should implement specially designed awareness frameworks (Sulaiman et al., 2022; Zulkifli et al., 2024). Theoretical frameworks, Routine Activity Theory (RAT) and Protection Motivation Theory (PMT), show important gaps in explaining victim vulnerability; since RAT focuses on opportunistic crime, it fails to consider psychological motivators of manipulation (Holt & Bossler, 2008; Plachkinova et al., 2025), while PMT neglects the role of emotional and cognitive biases utilised by attackers (Jansen & Leukfeldt, 2016).

The current study builds on the independent use of RAT and PMT by combining these two theories into a single theoretical model that integrates victim persona profiling. This framework will explicitly test the role of situational factors as major determinants of vulnerability, or as moderators of psychological relationships, and thus refine the conceptualisation of social-engineering victimisation. The objective of this study is to identify the most prevalent victim profiles by using cluster analysis and to test the moderating role of situational factors on the relationship between social engineering factors and cybersecurity awareness, highlighting the need to have better education and preparedness against cyber threats.

To achieve this, a survey was conducted to measure attack experiences and victim vulnerabilities among a relevant population. Our preliminary analysis indicates that while social engineering tactics are the most prevalent factor influencing awareness, situational factors did not function as a significant moderator but rather as a layer of context, a finding that challenges common assumptions and refines the focus for effective countermeasures.

Section 2 discusses a list of previous works and the theoretical framework used for this study. Methods used in this study, such as sampling and population, are discussed in Section 3. Findings and data analysis of the most prevalent victim profiles by using cluster profiling analysis and social engineering factors affecting cybersecurity awareness, and to test the moderating role of situational factors on the relationship between social engineering factors and cybersecurity awareness, are presented in Section 4. Finally, we conclude and provide recommendations of this study in Section 5.

2. LITERATURE REVIEW

Social engineering has become a global trend, and scammers are increasingly attacking trusting individuals in local communities. As Bora (2023) notes, cybercrime, including hacking, financial fraud, and data theft, is committed with the help of technology as the main tool. Sophisticated social-engineering techniques (including phishing and advance-fee fraud) are used by attackers to exploit psychological vulnerabilities in demographic categories (Gomes et al., 2020). The increasing threat highlights the pressing need to create better community awareness and victim profiling, and to provide specific cybersecurity training to reduce risks. By analysing attack methods, victim characteristics, and situational factors, stronger preventive measures can be developed to combat these evolving scams effectively.

2.1 Social Engineering

Social engineering is a form of psychological attack where the attackers use persuasion to make a victim act in a way they want(Montañez et al., 2020). Phishing, advance-fee fraud, and vishing are some of the attacks that exploit vulnerabilities in human relations and behavioural structures (Linvill et al., 2019). In the 2016 U.S. election, attackers took advantage of social-media sock-puppets or Russian trolls to manipulate public opinion (Linvill et al., 2019). With the evolution of cybersecurity technologies, social engineering has become the most dominant approach or the entrance to the exploitation of cyber systems. Numerous advanced and extremely destructive cyberattacks begin with social-engineering tactics, including phishing, which enables attackers to access enterprise networks (Montañez et al., 2020). In addition, Montañez et al. (2020) state that social engineering is used to infiltrate security systems in different ways. Research on social engineering has primarily focused on identifying and preventing attacks in the form of phishing emails; however, a gap remains in the systematic understanding of the psychological factors underlying these attacks. This lack of knowledge justifies the rampant success of such attacks.

2.2 Psychological Factors

Social-engineering attacks can take on a variety of psychological forms, including phishing attacks and extended romance schemes (Oguntoye, 2023). Scenarios designed by attackers to circumvent the use of rational thought by exploiting users' emotions, creating artificial urgency about account safety, promising rewards too good to be true, or simulating trusted relationships, are carefully created (Moustafa et al., 2021). Romance scams are another classic example of deceptive manipulation, whereby attackers can create a false perception of intimacy and trust over time and then impose financial demands (Carter, 2021). These scams sustain victim compliance by carefully playing with emotions, alternating between vulnerability and affection to establish a distorted reality (Bilz et al., 2023). Similarly, phishing attacks use the concepts of social proof, suggesting that many users have performed the requested action, and authority by posing as reputable institutions, making the harmful request appear legitimate(Wang et al., 2021). These strategies prove to be effective because they can bypass the instinctive scepticism of normal security to exploit the underlying attributes of human psychology, rather than technical weaknesses (Montañez et al., 2020).

2.3 Victim Profile

Nolte et al. (2021) and Faklaris et al. (2023) note that younger adults (18-40) have higher vulnerability to online scams than older adults because of overconfidence and digital naivety, while older adults are more vulnerable to trust-based attacks, and often provide sensitive information when influenced by a credible message, because of lower technical competence (Huda et al., 2021;Mittal & Ilavarasan, 2019). Studies from Muniandy et al., (2017); Jagadeesan et al., (2023); Arora, (2024) indicate that there are critical vulnerabilities in cybersecurity awareness levels, especially among students and young adults, as the majority of them lack fundamental password security and scam-recognition skills. For example, some share their passwords (32.81%), accept requests from strangers (14.84%), and meet people they have only known online, with threat awareness being low, and only 25% of them know best practices, and 41.41% unsure of scam tactics. These findings emphasise the critical need to implement specific educational trials, such as the inclusion of cybersecurity units in learning programmes and the creation of age-focused training courses, to counter the lack of knowledge, threats of behaviour, and the increasing financial effects of cyber threats in all age groups (Sudha et al., 2023; Huda et al., 2021).

2.4 Behavioural Factors

The level of cybersecurity knowledge and awareness can largely influence individual internet-use behaviour; many users cannot remain vigilant because of security fatigue. The phenomenon occurs when protective mechanisms are viewed as too complex or annoying, leading to disengagement (Bada et al., 2019). For example, when downloading games or streaming music, users can be exposed to malicious websites; without proper knowledge, they may disregard security warnings, which increases their vulnerability to threats. Despite the rapid growth of the internet and digital services, not all users are informed about basic risks of cybersecurity, and many have only limited knowledge of securing a device or recognising threats (Zwilling et al., 2022). This lack of awareness makes them easy targets for hackers who exploit both technical weaknesses and human factors, including poor password habits and susceptibility to phishing, as cybercriminals specifically target people with limited knowledge of risks related to applications and social networks. Zwilling et al. (2022) indicate that the least informed users are the primary victims of online attacks and therefore emphasise the importance of increased cybersecurity awareness in promoting safer Internet usage and preventing avoidable breaches. Until active interventions are implemented to sensitise the masses, many users will continue to unknowingly open security gaps, leaving themselves to exploitation.

2.5 Situational Factors

Strong supervision, defensive behaviours, and cybersecurity education are critical in addressing the risks posed by scams. Parental monitoring fosters more protective online behaviour, and protective measures, such as security software and phishing recognition, align with Routine Activity Theory because they interrupt the process of committing a crime (Paek et al., 2022; Drew & Farrell, 2018). Education is vital; engagement training, scenario-driven training, and blended-learning models are effective in producing practical defence competencies and cyber literacy (Gerontakis et al., 2023). However, motivated offenders constantly develop advanced strategies, using psychological influence and technical skills, which allow them to adapt their scams to new platforms and target audiences (Peersman et al., 2022; Lwin Tun & Birks, 2023). Therefore, a multi-layered approach, which combines supervision, behavioural protection, and immersive education, is needed to combat these emerging challenges and create a strong security-focused culture.

2.6 Cybersecurity Awareness

Cybersecurity awareness can be defined as the knowledge and readiness of individuals and organisations to protect against cyber threats, not only in terms of technical efforts, but also in terms of human and operational weaknesses as well (Arora, 2024). Human error has been one of the most prominent causes of security breaches, such as phishing attacks, weak passwords, and unintentional data leakage (Sharma & Thapa, 2023). Arora (2024) emphasises that these risks can be reduced most effectively through education and training. For example, studies in Serbia have shown that 99.3% of students use social media, whereas 73.5% reported never experiencing minor security breaches, with more than half (54.4%) claiming to have used weak passwords because of the memorability problem. Studies revealed that even with the average level of cybersecurity awareness, there is a wide knowledge-practice gap. While 93% of users agree that cybersecurity is relevant, only 40% follow safe behaviours, and younger and heavy internet users are at a high risk of falling prey to phishing and ineffective passwords (Muniandy et al., 2017). According to Bora (2023), Cybercrime, such as theft, fraud, and hacking, is an activity that depends on the widespread use of internet-connected devices; therefore, awareness programmes are necessary (Asadullah et al., 2021; Muniandy et al., 2017). The introduction of cybersecurity in educational programmes is essential, particularly among higher-education students, who are most vulnerable because of their heavy usage of online capabilities and their inexperience.

2.7 Conceptual Framework

Routine Activity Theory (RAT) and Protection Motivation Theory (PMT) offer complementary perspectives for understanding cybersecurity vulnerabilities. RAT, developed by Cohen and Felson (1979), explains cybercrime through three converging elements: motivated offenders (hackers), suitable targets (users with valuable data), and the absence of capable guardians (lack of security measures). In digital contexts, this theory emphasises the vulnerabilities that regular online actions present people to, especially when they commit unsafe actions, such as accessing dangerous websites or ignoring fundamental safety measures (Parti, 2023; Hawdon et al., 2020). The theory highlights how cybersecurity awareness programmes can mitigate these habitual vulnerabilities, particularly among the high-risk groups, such as heavy internet users, by enhancing protective behaviours, like the use of antivirus software and management of passwords, and decreasing target suitability, by means of education (Smith, 2024).

In contrast, PMT explains the cognitive mechanisms that lead to the presence of protective actions through threat and coping appraisals. Users have to experience a threat as a serious threat and themselves as vulnerable, but they also have to feel that protective actions are effective and capable of doing it (Bulbulia & Maharaj, 2013; Mou et al., 2022). An integrated approach is essential; RAT reduces criminal opportunities by promoting guardianship, while PMT motivates individuals to act by addressing psychological barriers. This study moves beyond the individual constructs to explore their theoretical unification. Although PMT explains the motivation and RAT explains the opportunity, this paper argues that the vulnerability of a victim can only be well understood by considering the interaction between psychological predispositions (which are explained by PMT) and demographic profiles with the situational context (which are explained by RAT). Situational factors are identified as more than background variables; they form a contextual layer that defines the boundary conditions of susceptibility.

The study proposes integrating both theoretical constructs into one conceptual framework (Figure 1), in which cybersecurity awareness depends on social engineering tactics, psychological threat appraisal, behavioural factors, and victim profiles. In this framework, these constructs are conceptually distinct. Knowledge of Social Engineering Tactics means the understanding of specific attack methods such as phishing, vishing, and advance fee fraud. Besides, Threat Appraisal refers to the cognitive evaluation of threat severity and personal vulnerability. Meanwhile, Cybersecurity Awareness acts as the dependent variable in our framework, representing the integration of threat knowledge, perceived risk, and behavioural intention to apply security measures. These situational factors, which are based on RAT, also provide a contextual layer rather than acting as a moderating variable. Therefore, the framework goes beyond the independent variables of PMT and RAT, arguing that the vulnerability of victims is best explained by the interplay of psychological predispositions (PMT) and situational factors (RAT). Figure 1 shows the refined cybersecurity awareness framework connecting cybersecurity awareness, victim profiles, and social engineering factors to provide a complete defensive framework.

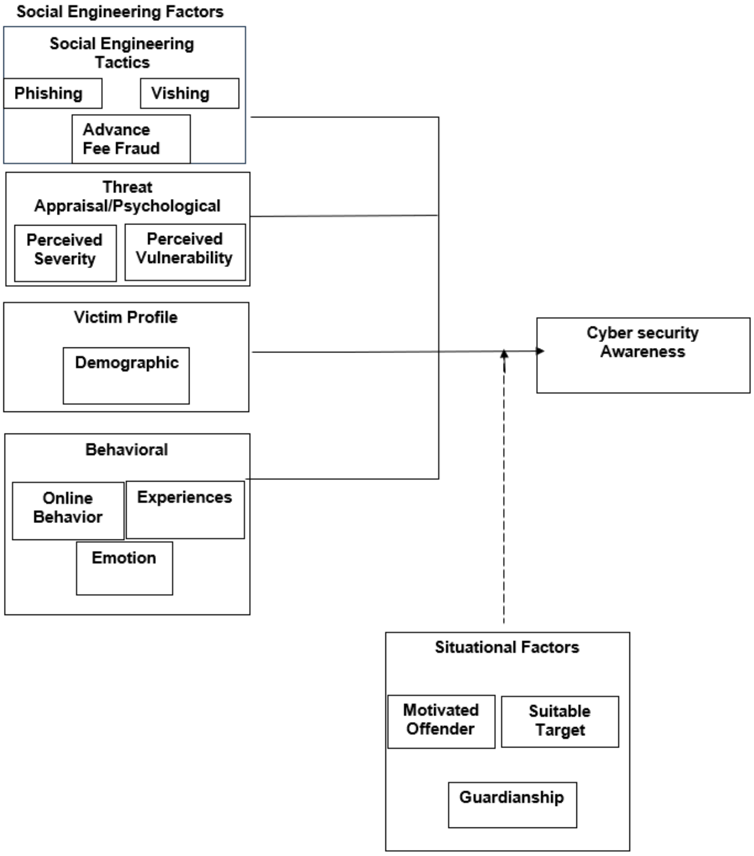

Fig.1: The Conceptual Framework of Social Engineering Factors and Situational Factors in Social Engineering and Cybersecurity Awareness

2.8 Hypothesis Development

Social Engineering in shaping Threat Appraisal/Psychological and Cybersecurity Awareness

Social engineering tactics, such as impersonation, emotional manipulation, and urgency, exploit psychological vulnerabilities and directly influence threat appraisal by increasing perceived severity and vulnerability (Bilz et al., 2023; Sulaiman et al., 2023). These tactics are employed by attackers across different platforms, utilising fake job opportunities on social media platforms or conducting phishing attacks via email, which enhances the psychological impact and risk perception (Whitty, 2019; Houtti et al., 2024). The exposure can be reduced by situational factors and educational interventions, but the psychological process of social engineering tactics increases threat appraisal, which in turn can increase cybersecurity awareness. Thus,

H1a: Social Engineering Tactics Influence Cybersecurity Awareness.
H1b: Threat Appraisal/ Psychological Factors Influence Cybersecurity Awareness.
H1c: Social engineering Factors have a significant influence on Cybersecurity Awareness.

Victim Profiles and Their Influence on Cybersecurity Awareness of Social Engineering Attacks

The victim profiles, defined by demographic and experiential factors, including age, gender, online activity, and previous experience with scams, have a significant effect on how people perceive and react to social engineering attacks (Bilz et al., 2023; Faklaris et al., 2023). Younger, more digitally engaged people are more vulnerable to phishing and impersonation strategies, whereas older adults may fall prey to misguided plots as a valid charity request. This phenomenon highlights the importance of demographic and behavioural patterns in the development of threat recognition (Bilz et al., 2023). Financial literacy and risk perception also influence vulnerability. Lack of financial literacy also significantly increases the likelihood of treating scams as plausible opportunities, while people with higher awareness are better able to notice a threat and act on it (Faklaris et al., 2023; Sur et al., 2021). Cybersecurity awareness targeted educational programmes that promote an improved understanding of social engineering tactics can strengthen a scam-resistant stance and reduce the susceptibility of this population to victimisation (Sulaiman et al., 2022). Therefore,

H2a: Victim Profile, including demographic factors, significantly influences Cybersecurity Awareness.

Behavioural and Situational Factors in Mitigating Vulnerabilities to Social Engineering Attacks

According to RAT, reducing the vulnerability to social engineering is possible through capable guardianship, such as parental monitoring, protective behaviour, and formal cybersecurity education, which limits criminal opportunities (Paek et al., 2022; Drew and Farrell, 2018). In contrast, motivated offenders use technical expertise, psychological manipulation, and tactical flexibility to exploit human and system vulnerabilities (Peersman et al., 2022 ; Wen et al., 2022). These dynamics highlight the role of behavioural aspects in adopting safe online behaviours and avoiding riskier behaviours and situational protective measures (institutional control) in influencing cybersecurity awareness and resilience (Lwin Tun & Birks, 2023). Hence,

H3b: Situational Factors have a significant moderating effect on Social Engineering Factors.
H3a: Behaviour influences Cybersecurity Awareness.

3. METHODOLOGY

The methods used in the study, such as sampling, population, and data analysis, are discussed in this section. The current study employs a quantitative methodology to review the effect of social engineering attacks on the victim profile and uses a correlational research design to test the relationship between Social Engineering Factors and Cybersecurity Awareness. The study framework integrates Protection Motivation Theory (PMT) and Routine Activity Theory (RAT), which are used to determine the level of awareness among higher education students. Data were collected through a structured survey featuring closed-ended and Likert-scale questions, ensuring precise and measurable responses. All information about the participants is kept confidential, and only contact details are stored for follow-up processes.

3.1 Sampling

The study used purposive sampling to focus on people who are more likely to be exposed to social engineering, including those who use the internet frequently, with a focus on higher education institutions in Kuching and Samarahan, Sarawak. The recruitment was carried out through online surveys, shared through social media, LinkedIn, and email among students at target universities. The sample size was estimated at 129 individuals using the G*Power software, and oversampled by 20% (a total of 150). The approach provides both diversity and contextual representativeness, increasing the validity of this study in assessing the effect of social engineering on cybersecurity awareness. Whilst purposive sampling of higher education students may impair the generalisation of findings to the overall population, it was an intentional choice in the context of the current study. Students were chosen as the target population because they are digitally native, regular internet users, and frequent victims of social engineering attacks; they also tend to be overconfident and have a knowledge-practice gap when it comes to cybersecurity (Muniandy et al., 2017; Jagadeesan et al., 2023; Arora, 2024). The method enables a narrower study of vulnerability processes among a highly susceptible group, therefore serving as a basis for studies that can be replicated in greater populations in the future.

3.2 Population

This study targets higher education students in Kuching and Samarahan, Sarawak, Malaysia, aged between 18 and 30, to determine their level of cybersecurity awareness as well as exposure to social engineering attacks. Respondents were asked to fill out questionnaires assessing their level of knowledge and experience of online scams, thus offering insights into demographic and behavioural vulnerabilities. The study aims to uncover awareness gaps and enhance cybersecurity awareness and preparedness in students by focusing on this demographic, which provides meaningful information to address social engineering threats in educational institutions in Sarawak.

3.3 Data Analysis

The statistical analysis of the data was performed with SPSS version 30, and included descriptive and inferential analysis (including indices of central tendency, such as the mean, and indices of dispersion, such as the standard deviation) to characterise the important features of the data. The first stage of data processing and cleaning involved the use of Microsoft Excel. In addition, a post-hoc power test was conducted using G*Power to confirm the suitability of the sample size. Moreover, to achieve the study's objectives, both multiple regression and moderated multiple regression analyses were conducted.

4. FINDINGS

4.1 Demographic Information

The demographic profile of the study participants (N = 131) is presented in Table 1. The sample was mainly female (61.8%) and was focused on the 22-25 age group (76.3%). Most respondents were undergraduate students (58.8 %), in their third year of study (35.1 %), and were studying on a full-time basis (91.6%). Most respondents (77.1% and above) were based in Kuching, and the majority (55.0%) were enrolled in Science and Technology programmes. Data were gathered from eight higher-education institutions in the area, with the largest cohorts from UiTM Samarahan (36.6%), UNIMAS (22.1%), and Swinburne University, Kuching.

Table 2 presents the descriptive statistics for the demographic profile and the key variables of the study sample (N = 131). Measures of central tendency and variability were obtained using descriptive analyses. Threat Appraisal (M = 3.75, SD = 0.68) and Situational Factors (M = 3.65, SD = 0.68) had relatively high mean scores, indicating that the participants were well-informed about external cybersecurity threats. The Behavioural Factors had the lowest mean score (M = 3.17, SD = 0.92), implying that consistent secure online security behaviours were less prevalent among the respondents. The standard deviation for this construct was quite high, indicating substantial behavioural variability within the sample. Furthermore, overall Cybersecurity Awareness among the participants was moderate (M = 3.39, SD = 0.70), as was the awareness of Social Engineering Tactics (M = 3.35, SD = 0.77). These descriptive findings provide a foundational profile of the sample for the inferential analyses.

Table 1: Demographic Profile

		Number	Frequency
Gender	Male	50	38.2%
	Female	81	61.8%
Age Group	18-21	10	7.6%
	22-25	100	76.3%
	26-30	21	16.0%
	31-40	0	0%
	41-50	0	0%
Education Level	SPM	25	19.1%
	Diploma/STPM	25	19.1%
	Bachelor's Degree	77	58.8%
	Master's Degree	4	3.1%
Place of study	UiTM SAMARAHAN	48	36.6%
	UNIMAS	29	22.1%
	SWINBURNE KUCHING	29	22.1%
	ICATS	4	3.1%
	POLITEKNIK KUCHING	13	9.9%
	UCSI KUCHING	4	3.1%
	INSTITUT TEKNOLOGI SARAWAK (ITS)	2	1.5%
	SEGI COLLEGE KUCHING	2	1.5%
Year of study (Number Only)	1	5	3.8%
	2	19	14.5%
	3	46	35.1%
	4	24	18.3%
	5	36	27.5%
	6	1	0.8%
Study Mode	Full Time	120	91.6%
	Part Time	11	8.4%
Place of Origin (Birthplace/ Hometown)	1-Kuching	101	77.1%
	2-Bintulu	3	2.3%
	3-Miri	6	4.6%
	4-Sibu	8	6.1%
	5-Samarahan	2	1.5%
	6-Mukah	2	1.5%
	7-Sarikei	2	1.5%
	8-Lawas	1	0.8%
	9-Serian	1	0.8%
	10-Betong	1	0.8%
	11-Sri Aman	1	0.8%
	12-Other from Sarawak (Johor, Sabah, etc)	3	2.3%
Field of study	Sciences and Technology	72	55.0%
	Social Sciences	59	45.0%

Table 2: Descriptive Statistics of Variables (Means, Standard Deviations)

	Mean	Std. Deviation
Gender	.62	.488
Age	2.08	.481
Education Level	2.46	.834
Place of study	2.50	1.67
Year of study (Number Only)	3.53	1.17
Study Mode	1.08	.278
Place of Origin (Birthplace/ Hometown)	2.04	2.43
Field of study	1.45	.499
Social Engineering Tactics	3.35	.768
Threat Appraisal/Psychological	3.75	.676
Behavioural Factors	3.17	.917
Situational Factors	3.65	.68
Cybersecurity Awareness	3.39	.696

4.2 Multiple Regression Analysis

RO1: To identify the most prevalent victim profiles by using cluster profiling analysis and social engineering factors affecting cybersecurity awareness.

Table 3 shows that a multiple regression was performed to define the predictors of cybersecurity awareness. The model indicated that Social Engineering Tactics (β=.370, p =.001) and Threat Appraisal (β=.244, p =.007) were strong positive predictors, meaning that knowledge of scamming and a higher perception of the threat severity resulted in greater awareness. This indicates that deeper knowledge of social engineering tactics, such as phishing and vishing, is more critical to the development of awareness than general security knowledge. Gender (β= -.167, p =.029) and Place of Study (β= -.171, p =.025) were other factors that significantly negatively predicted the items. Other variables like Age, Education Level, Year of Study, and Behavioural Factors were not statistically significant. This implies that although self-reported secure behaviours are important, they may have an indirect impact on the overall awareness, maybe through a mediating variable, which could be a prior exposure or threat appraisal. Furthermore, the findings indicate that psychological and knowledge-based variables have a stronger impact on cybersecurity awareness than most demographic attributes, and the ability to comprehend particular social engineering techniques can be regarded as the most influential factor.

Table 3: Multiple Regression of Social Engineering Factors and Cybersecurity Awareness

Model	Standardised Coefficients Beta	t	Sig.
(Constant)		2.02	.045
Gender	-.167	-2.21	.029
Age	.007	.088	.930
Education Level	.061	.769	.443
Place of study	-.171	-2.27	.025
Year of study (Number Only)	.004	.045	.964
Study Mode	.074	.987	.326
Place of Origin (Birthplace/ Hometown)	-.023	-.310	.757
Field of study	.081	1.09	.278
Social Engineering Tactics	.370	3.76	<.001
Threat Appraisal/Psychological	.244	2.74	.007
Behavioural Factors	.041	.451	.653
a. Dependent Variable: Cybersecurity Awareness			

4.3 Cluster Analysis: Identifying Distinct Victim Profiles

To complement the variable-centred regressions, a K-means cluster analysis was conducted to develop comprehensive victim profiles. This relational approach classifies individuals based on their similarity across several variables at a time. The four most important constructs, the Social Engineering Tactics, Threat Appraisal, Behavioural Factors, and Cybersecurity Awareness, were included in the analysis. Before clustering, these variables were standardised (z-score transformation) to ensure equal weighting in the cluster formation process. The algorithm yielded a strong three-cluster solution. Analysis of variance (ANOVA) was used to establish that all four variables significantly differed among the clusters ($p < .001$). The resulting cluster centroids, representing the mean profile of each group, are presented in Table 4.

Table 4: Final Cluster Centres from K-Means Cluster Analysis

	Final Cluster		
	Cluster 1: The Vigilant Expert (n=34)	Cluster 2: The Aware but Inconsistent (n=63)	Cluster 3: The Vulnerable Novice (n=34)
Social Engineering	4.2	3.3	2.5
Threat Appraisal	4.3	3.7	3.2
Behavioural Factors	3.8	3.3	2.1
Cybersecurity Awareness	4.0	3.3	3.0

4.4 Moderated Regression Analysis

RO2: To test the moderating role of situational factors on the relationship between social engineering factors and cybersecurity awareness

Table 5 presents the multiple regression analyses that were conducted to examine the effects of social-engineering variables on cybersecurity awareness, and specifically whether situational variables moderated the relationships between demographic variables (victim profiles) and the other social-engineering variables. The findings indicate that situational variables generated a strong statistically significant positive main effect on cybersecurity awareness in most of the models. In addition, situational factors significantly moderated the relationship between two particular variables and awareness. First, gender and situational factors interacted significantly ($\beta = -0.346$, $p = .019$). Second, a significant interaction between year of study and situational factors was found ($\beta = .237$, $p = .002$). Situational factors were not significant moderators of the other variables tested, such as age, educational level, social engineering tactics, threat appraisal, and behavioural factors. These results imply that the social-engineering variables did not act as direct predictors of awareness, but that the relationship between social-engineering factor variables and awareness remained consistent across situational contexts. Contrary to H3b and the common applications of Routine Activity Theory, there were no moderating situational variables; instead, they served as direct predictors. This subtlety suggests that a safe environment elevates baseline vigilance universally, rather than altering the way people perceive certain dangers.

Table 5: Moderated Regression of Situational Factors on Social Engineering Factors and Cybersecurity Awareness

Variable	Coefficient (β)	t- value	p-Value
Gender	1.05	1.91	.05
Situational Factor	.70	7.00	.00
Gender X Situational Factors	-.34	-2.36	.01

Age	-.51	-.84	.39
Situational Factor	.24	.67	.50
Age X Situational Factors	.15	.94	.34
Education Level	.33	1.01	.31
Situational Factor	.81	3.38	.00
Education Level X Situational Factors	-.09	-1.07	.28
Place of Study	.38	1.55	.12
Situational Factor	.79	5.09	.00
Place of Study X Situational Factors	-.11	-1.72	.08
Year of Study	-.83	-2.9249	.00
Situational Factor	-.34	-1.15	.25
Year of Study X Situational Factors	.23	3.15	.00
Study Mode	-.42	-.38	.69
Situational Factor	.38	.1.15	.24
Study Mode X Situational Factors	.17	.57	.56
Place of Origin	-.1031	1.45	.14
Situational Factor	.47	5.10	.00
Place of Origin X Situational Factors	.02	1.53	.12
Field of Study	.54	.96	.33
Situational Factor	.77	3.23	.00
Field of Study X Situational Factors	-.13	.91	.36
Situational Factor	.04	.14	.88
Social Engineering Tactics	-.00	-.00	.99
Situational Factor	.16	.71	.47
Social Engineering Tactics X Situational Factors	.06	.99	.32
Threat Appraisal/Psychological	.30	1.14	.254
Situational Factor	.85	2.84	.00
Threat Appraisal/Psychological X Situational Factors	-.084	-1.14	.255
Behavioural Factors	.13	.52	.59
Situational Factor	.54	2.64	.00
Behavioural Factors X Situational Factors	-.01	-.18	.85

4.5 Discussion

Research Objective 1

To identify the most prevalent victim personas by using cluster profiling analysis and social engineering factors affecting cybersecurity awareness.

This objective aimed to identify prevalent victim profiles and social engineering factors affecting cybersecurity awareness. The multiple regression analysis indicated that social engineering factors explained 31.9% of the variance in awareness. Social Engineering Tactics (β = .370, p < .001) and Threat Appraisal (β = .244, p = .007) emerged as the strongest positive predictors, supporting hypotheses H1a and H1b. Direct exposure to certain threats, including Advance-Fee Fraud (β = .315, p < .001) and Vishing (β = .272, p = .018), was significantly related to the increased awareness (Femi-Oyewole et al., 2024). However, phishing did not show any significant impact, which is perhaps due to the effective prior Anti-

Phishing training. The effect of threat appraisal aligns with Protection Motivation Theory, which posits that perceived severity is the driving force of protection intentions (Wirtz & Rohrbeck, 2018; Ayal et al., 2025; Hromatko et al., 2021). Demographic variables revealed that gender and place of study were the only variables with small negative effects, partially supporting hypothesis H2a; age, education level, and year of study were not found to be significant. Behavioural factors were found to be significant in simple regression (β = .36, p < .001) but not found significant (β = .04, p = .653) when social engineering variables and threat appraisal were added. According to studies, the influence of behavioural variables is mediated by exposure increment and perceived vulnerability (Grassegger & Nedbal, 2021; Alghenaim et al., 2022; Benavides-Astudillo et al., 2022).

Research Objective 2

To test the moderating role of situational factors on the relationship between social engineering factors and cybersecurity awareness.

The moderated regression analysis tested whether situational factors moderated the relationship between social engineering factors and cybersecurity awareness. The findings revealed that situational factors did not significantly moderate Social Engineering Tactics (β = .06, p = .325), Threat Appraisal (β = –.08, p = .255), or Behavioural Factors (β = –.01, p = .855); therefore, hypothesis H3b was not supported. This observation is consistent with previous studies suggesting that awareness pathways are context-independent and not situationally dependent (Smith et al., 2022; Grandhi & Still, 2025; Ifinedo, 2023). However, situational factors had a strong independent positive effect on awareness (β = .85, p = .005), which implied that they acted as direct predictors rather than moderators. Only demographic variables, specifically gender (β = –0.347, p = .019) and year of study (β = 0.237, p = .002), showed significant interactions; however, these did not alter the main results. These findings refine the application of Routine Activity Theory in cybersecurity by allowing situational factors as sources of baseline vigilance rather than conditional moderators of psychological or knowledge-based processes.

Practical Implications and Deployment

The empirical results of the study, especially the discovery of three different victim profiles, allow for a shift from generic cybersecurity training to specific interventions. We propose a deployment model that integrates our evidence-based profiles with established principles from the literature to form a more efficient and effective awareness approach.

i. Persona-Based Adaptive Training.

The findings can serve as a typology for adaptive learning in cybersecurity. Although earlier studies have promoted individualisation based on overall proficiency scores (Schöni et al., 2024), our model advances this approach by establishing specific, actionable user profiles. This allows better refining of training:

For the Vulnerable Novice, training should be based on strengthening general digital literacy and go beyond generic programmes. Such training should aim to build the necessary competencies in threat recognition and address the specific knowledge gaps identified in this study. The Aware but Inconsistent persona is particularly significant since it empirically proves a key mechanism underlying failure among a substantial portion of the population, which refers to the intention-behaviour gap. This shift moves the study agenda beyond merely raising awareness towards addressing cognitive and habitual barriers that hinder the transformation of knowledge into action. Training that is targeted at this population should, therefore, be specifically created to fill this gap. This can be accomplished through lightweight, continuous simulations and reminders, a strategy that is consistent with the nudge theory, in line with a study by Lain et al., 2024) to actively transform their prior knowledge into regular security habits.

ii. Context-Embedded Awareness Campaigns

The observation that situational factors function as direct rather than moderating predictors of awareness shows the underlying weakness of standalone training campaigns, ignoring the continuous, real-world digital context in which users operate. These findings suggest that positive situational contexts serve as critical sources of awareness. Therefore, there is a need to move towards context-specific interventions that embed concise, actionable security messages directly within the platforms where risks are encountered and decisions are made. Such an approach may include installing phishing warning notices within the university email client, placing password hygiene reminders on the student portal login page, and issuing time-limited scam alerts on official social media during high-risk periods. This strategy builds on context-informed design principles by empirically identifying high-activity, high-risk digital situations among our target population. This enables the delivery of just-in-time, just-in-place education that reinforces the baseline vigilance provided by situational factors.

iii. Digital Nudging through risk- Profile.

The concept of digital nudging is powerful, and the identified victim personas serve as a guideline to make it actionable. Instead of applying standardised nudges to all users, the proposed framework enables a dynamic system in which the prevalence and rate of alerts are adjusted according to an individual's risk profile. For example, a user whose actions are consistent with the Vulnerable Novice persona would automatically receive more frequent and assertive warnings. This strategy is supported by a study on adaptive security systems (Farhad, Lashkari). This approach ensures that the intensity of the intervention is related to the level of susceptibility of the user, hence maximising the effectiveness and minimising the alert fatigue among more competent users.

Policy Implications

The findings of this study provide empirically grounded guidance for policymakers, educational administrators, and organisational leaders seeking to strengthen cybersecurity resilience. The refined framework, integrating victim profiling with situational factors, moves beyond generic awareness campaigns towards evidence-based and targeted policy design.

The cluster analysis reveals three unique victim personas: Vigilant Expert, Aware but Inconsistent, and Vulnerable Novice, thus highlighting the need for differentiated cybersecurity education policies. A general national awareness programme is ineffective. As a result, persona-specific training modules should be mandated by policy and included in higher education and public awareness programmes. In particular, funds should be allocated to establishing foundational digital literacy courses for the Vulnerable Novices, whereas the Aware but Inconsistent users, who represent a critical intention-behaviour gap, should be subjected to habitual reinforcement through simulated exercises and digital nudges. Regression analyses show that social engineering variables, such as knowledge of social engineering tactics and threat appraisal, particularly perceived vulnerability, have a more significant effect on cybersecurity awareness than the demographic variables, which were weakly significant for gender and place of study. These results challenge the practice of clustering populations based on age, gender, and education level to support security training. Moreover, national cybersecurity frameworks should therefore prioritise cognitive and behavioural interventions that enhance threat recognition and personal risk perception, aligning with Protection Motivation Theory. Such a paradigm shift is necessary so that policy-led initiatives can tackle the determinants of awareness rather than the demographic correlates. The finding that situational factors have a direct effect but do not moderate core relationships narrows the scope for policy interventions derived from Routine Activity Theory. In particular, secure environments elevate baseline vigilance but do not affect the transfer of knowledge into awareness. Accordingly, policy must facilitate the integration of context-sensitive security nudges in real time within the digital infrastructure used by vulnerable user populations, such as university learning management systems, official email clients, and student portals. Examples of such measures include embedded phishing warnings, prompts on password hygiene, and dynamically displayed scam warnings during high-risk periods. These guardianship-by-design policies create a continuous protective shell that supplements personal training.

5. CONCLUSION

In conclusion, the study proposed and examined a refined cybersecurity awareness framework involving victim profiling, social engineering tactics, and situational factors. The multiple regression results indicated that Social Engineering Tactics and Threat Appraisal were the strongest positive predictors of cybersecurity awareness, while Gender and Place of Study had a moderate yet significant negative influence. These results highlight that psychological, social-engineering -related knowledge has a greater impact on awareness than most demographic variables, making social engineering knowledge the most influential mechanism of cyber vigilance. Furthermore, moderated regression analysis indicated that situational factors were also direct independent predictors, rather than moderators of the relationship between social engineering variables and awareness. Situational factors had a significant impact on Gender and Year of Study, but did not alter the fundamental psychological mechanisms linking social engineering to awareness, suggesting that cybersecurity awareness is relatively stable across situational conditions.

These findings indicate that psychological social engineering variables, especially Social Engineering Tactics and Threat Appraisal, are better predictors of awareness than demographic variables, implying that interventions aimed at demographic variables need to be replaced by psychology-of-social-engineering-informed strategies. Situational variables were direct predictors of awareness, not moderators, refining the use of Routine Activity Theory to digital environments. Moreover, the three different victim profile personas, Vigilant Expert, Aware but Inconsistent, and Vulnerable Novice, demonstrate the most important role of persona-specific strategies, particularly in bridging the intention-behaviour gap within the largest group of participants (the Aware but Inconsistent).

Following these insights, future studies should adopt longitudinal and experimental designs to determine causal pathways and validate the victim profiling cybersecurity awareness framework in multiple cultural and organisational contexts. Besides, future studies should also use more complex modelling methods, such as Structural Equation Modelling, to test more complicated moderation pathways and combine behavioural metrics with self-report data to more objectively determine the intention-behaviour gap.

Policymakers and institutional leaders are encouraged to adopt victim profiling or persona-specific cybersecurity education interventions targeting the use of basic digital literacy among the Vulnerable Novices, as well as providing habit-forming nudges and contextual simulations to the Aware but Inconsistent. Policy should also encourage the incorporation of real-time, context-based protection, including embedded phishing warnings and dynamic scam warnings, into the online platforms used by vulnerable groups. In addition, national cybersecurity plans must focus on cognitive-behavioural interventions in line with Protection Motivation Theory and provide monitoring and evaluation systems to enhance evidence-based awareness campaigns iteratively.

Overall, this paper presents a validated, integrative, and refined framework that contributes to theoretical knowledge and practical intervention design, which can be used to offer a clear flow of how these results can be applied to scalable, effective measures to prevent the risks of social engineering and improve the cyber resilience of vulnerable groups.

6. CONTRIBUTION OF AUTHORS

Haiqal Shazrin carried out the study, wrote the article, conceptualised the central study idea, and provided the theoretical framework. Mohd Norhisham Razali@Ghazali and Marlita Mat Yusof reviewed, proofread, checked the format, and offered technical support.

7. FUNDING

This work received no specific grant from any funding agency.

8. CONFLICT OF INTEREST STATEMENT

The authors agree that this study was conducted in the absence of any self-benefits, commercial or financial conflicts, and declare the absence of conflicting interests with the funders.

9. ACKNOWLEDGEMENT

The authors would like to express their deepest appreciation to the study supervisors who gave invaluable guidance, continuous support, and helpful feedback throughout this study. Sincere thanks to all participants who have provided their time and experiences so generously to make this study possible.

10. REFERENCES

Alghenaim, M. F., Bakar, N. A. A., & Rahim, F. A. (2022). Exploring the factors influencing employee awareness of social Engineering threats: A review. *Applied Mathematics and Information Sciences*, *16*(4), 491–500. https://doi.org/10.18576/amis/160402

APWG. (2025). *2024 Phishing Activity Trends Reports*. https://doi.org/10.55041/IJSREM32833

Arora, M. S. (2024). Threats, effects, and awareness of cybercrime: A Survey. *International Journal of Scientific Research in Engineering and Management*, *8*(5), 1–5. https://doi.org/10.55041/IJSREM32833

Asadullah, M., Adam, M., & Suhaimi, B. (2021). Cybersecurity strategies and challenges in Malaysia. *International Journal of Computer Science and Information Technology Research*, *9*(3), 16–27. https://www.researchpublish.com/papers/cybersecurity-strategies-and-challenges-in-malaysia

Ayal, S., Konis, D., & Saporta, K. (2025). The "Why Me?" model: explaining moral judgments in the eyes of single versus several victims. *Journal of Behavioural Decision Making*, *38*(2). https://doi.org/10.1002/bdm.70012

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). *Cybersecurity awareness campaigns: Why do they fail to change behaviour?* arXiv. https://doi.org/10.48550/arXiv.1901.02672

Benavides-Astudillo, E., Silva-Ordoñez, L., Rocohano-Rámos, R., Fuertes, W., Fernández-Peña, F., Sánchez-Gordon, S., & Bastidas-Chalan, R. (2022). Analysis of vulnerabilities associated with social engineering attacks based on user behaviour. *Communications in Computer and Information Science*, *1535 CCIS*, 351–364. https://doi.org/10.1007/978-3-031-03884-6_26

Bilz, A., Shepherd, L. A., & Johnson, G. I. (2023). Tainted Love: A Systematic literature review of online romance scam research. *Interacting with Computers*, *35*(6), 773–788. https://doi.org/10.1093/iwc/iwad048

Bora, R. (2023). Challenges and emerging trends in cybersecurity. *Shodh Sari-An International Multidisciplinary Journal*, *2*(3), 26–41. https://doi.org/10.59231/SARI7590

Bulbulia, Z., & Maharaj, M. (2013). *Factors that influence young adults' online security awareness. Journal of Information Warfare, 12*(1), 83–96. https://www.jstor.org/stable/26487001

Carter, E. (2021). Distort, extort, deceive, and exploit: Exploring the inner workings of romance Fraud. *British Journal of Criminology*, *61*(2), 283–302. https://doi.org/10.1093/bjc/azaa072

Datta, P., Panda, S. N., Tanwar, S., & Kaushal, R. K. (2020). A Technical Review Report on Cyber Crimes in India. *2020 International Conference on Emerging Smart Computing and Informatics, ESCI 2020*, 269–275. https://doi.org/10.1109/ESCI48226.2020.9167567

Deora, R. S. (2021). Brief study of cybercrime on the internet. *Journal of Communication Engineering & Systems, 11*(1)*,* 1–6. https://doi.org/10.37591/JoCES

Drew, J. M., & Farrell, L. (2018). Online victimisation risk and self-protective strategies: developing police-led cyber fraud prevention programmes. *Police Practice and Research*, *19*(6), 537–549. https://doi.org/10.1080/15614263.2018.1507890

Faklaris, C., Lipford, H. R., & Tabassum, S. (2023). *Preliminary Results from a U.S. Demographic Analysis of SMiSh Susceptibility. arXiv*. https://doi.org/10.48550/arXiv.2309.06322

Femi-Oyewole, F., Osamor, V., & Okunbor, D. (2024). A systematic review of social engineering attacks & techniques: The Past, present, and future. *In Proceedings of the 2024 International Conference on Science, Engineering, and Business for Driving Sustainable Development Goals (SEB4SDG)* 1- 12. IEEE. https://doi.org/10.1109/SEB4SDG60871.2024.10629836

Gerontakis, G., Yannakopoulos, P., & Voyiatzis, I. (2023). Evaluating cybersecurity certifications: A framework for extracting educational scenarios in cybersecurity training. *ACM International Conference Proceeding Series*, 243–248. https://doi.org/10.1145/3635059.3635097

Gomes, V., Reis, J., & Alturas, B. (2020). Social engineering and the dangers of phishing. *Iberian Conference on Information Systems and Technologies, CISTI*, *2020-June*, 1–7. IEEE. https://doi.org/10.23919/CISTI49556.2020.9140445

Grandhi, S. R., & Still, J. D. (2025). The Big Five in Action: A systematic review of personality, cyber awareness, and behaviours. *In A. Moallem (Ed.), HCI for cybersecurity, privacy and trust*, 22–40. Springer. https://doi.org/10.1007/978-3-031-92833-8_2

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, *181,* 59–66. https://doi.org/10.1016/j.procs.2021.01.103

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. *American Journal of Criminal Justice*, *45*(4), 546–562. https://doi.org/10.1007/s12103-020-09534-4

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimisation. *Deviant Behaviour*, *30*(1), 1–25. https://doi.org/10.1080/01639620701876577

Houtti, M., Roy, A., Gangula, V. N. R., & Walker, A. M. (2024). *A survey of scam exposure, victimisation, types, Vectors, and reporting in 12 Countries* (Version 1). arXiv. http://arxiv.org/abs/2407.12896

Hromatko, I., Tonković, M., & Vranic, A. (2021). Trust in Science, perceived vulnerability to disease, and adherence to pharmacological and non-pharmacological COVID-19 recommendations. *Frontiers in Psychology*, *12*. Article 664554 https://doi.org/10.3389/fpsyg.2021.664554

Huda, N., Zulkipli, N., Aimuni, N., Rashid, M., Farhan Zolkeplay, A., & Geogiana Buja, A. (2021). Synthesising cybersecurity issues and challenges for the elderly. *Turkish Journal of Computer and Mathematics Education, 12*(5)*,* 1698–1706. https://doi.org/10.17762/turcomat.v12i5.2180

Ifinedo, P. (2023). Effects of security knowledge, self-control, and countermeasures on cybersecurity behaviours. *Journal of Computer Information Systems*, *63*(2), 380–396. https://doi.org/10.1080/08874417.2022.2065553

Jagadeesan, S., Sameer, Singh, D., Ojha, R., Ibrahim, R. K., & Alazzam, M. B. (2023). Application of cybersecurity in E-learning education. *In 2023 3rd International Conference on Advancement in Electronics and Communication Engineering (AECE),* 932–937. IEEE. https://doi.org/10.1109/AECE59614.2023.10428587

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimisation. *International Journal of Cyber Criminology*, *10*(1), 79–91. https://doi.org/10.5281/zenodo.58523

Lain, D., Jost, T., Matetic, S., Kostiainen, K., & Capkun, S. (2024). Content, nudges, and incentives: A study on the effectiveness and perception of embedded phishing training. *In Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security*, 4182–4196. ACM. https://doi.org/10.1145/3658644.3690348

Linvill, D. L., Boatwright, B. C., Grant, W. J., & Warren, P. L. (2019). "The Russians are hacking my brain!" Investigating Russia's internet research agency twitter tactics during the 2016 United States presidential campaign. *Computers in Human Behaviour*, *99*, 292–300. https://doi.org/10.1016/j.chb.2019.05.027

Lwin Tun, Z., & Birks, D. (2023). Supporting crime script analyses of scams with natural language processing. *Crime Science*, *12*(1), Article 10. https://doi.org/10.1186/s40163-022-00177-w

Mittal, S., & Ilavarasan, P. V. (2019). Demographic factors in cyber security*:* An empirical study. In I. O. Pappas, P. Mikalef, Y. K. Dwivedi, L. Jaccheri, J. Krogstie, & M. Mäntymäki (Eds.), *Digital transformation for a sustainable society in the 21st century*. 667–676. Springer. https://doi.org/10.1007/978-3-030-29374-1_54

Montañez, R., Golob, E., & Xu, S. (2020). Human cognition through the lens of social engineering cyberattacks. *Frontiers in Psychology*, *11*, Article 1755. https://doi.org/10.3389/fpsyg.2020.01755

Mou, J., Cohen, J., Bhattacherjee, A., & Kim, J. (2022). A test of Protection Motivation Theory in the information security literature: A meta-analytic structural equation modelling approach. *Journal of the Association for Information Systems*, *23*(1), 196–236. https://doi.org/10.17705/1jais.00723

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology*, *12*, Article 561011. https://doi.org/10.3389/fpsyg.2021.561011

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cybersecurity behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cybersecurity*, *2017*(1), 1–13. https://doi.org/10.5171/2017.800299

Nolte, J., Hanoch, Y., Wood, S., & Hengerer, D. (2021). Susceptibility to COVID-19 scams: The roles of age, individual difference measures, and scam-related perceptions. *Frontiers in Psychology*, *12*, 789883. https://doi.org/10.3389/fpsyg.2021.789883

Oguntoye, O. (2023). The impact of psychological factors on users' cybersecurity compliance behaviour within corporate environments. *[Master's thesis, Bournemouth University]. ResearchGate.* https://doi.org/10.13140/RG.2.2.25357.92643

Omar, S. Z., Kovalan, K., & Bolong, J. (2021). Effect of age on information security awareness level among young internet users in Malaysia. *International Journal of Academic Research in Business and Social Sciences*, *11*(19), 230–240. https://doi.org/10.6007/ijarbss/v11-i19/11733

Paek, S. Y., Lee, J., & Choi, Y. J. (2022). The impact of parental monitoring on cyberbullying victimisation in the COVID-19 era. *Social Science Quarterly*, *103*(2), 294–305. https://doi.org/10.1111/ssqu.13134

Parti, K. (2023). What is a capable guardian to older fraud victims? Comparison of younger and older victims' characteristics of online fraud utilising routine activity theory. *Frontiers in Psychology*, *14*, 1–10. https://doi.org/10.3389/fpsyg.2023.1118741

Peersman, C., Williams, E., Edwards, M., & Rashid, A. (2022). *Understanding the motivations and characteristics of financially-motivated cybercriminals*. (Version 1). arXiv. http://arxiv.org/abs/2203.08642

Plachkinova, M., Vo, A., Batra, G., & Zafar, H. (2025). Beyond Routine Activity Theory: towards a novel phishing victimisation theory. *Communications of the Association for Information Systems*, *57,* Article 16. https://doi.org/10.17705/1CAIS.05716

Schöni, L., Carles, V., Strohmeier, M., Mayer, P., & Zimmermann, V. (2024). You know what? - Evaluation of a personalised phishing training based on users' phishing knowledge and detection skills. *In Proceedings of the 2024 European Symposium on Usable Security*, 1–14. ACM. https://doi.org/10.1145/3688459.3688460

Sharma, R., & Thapa, S. (2023). *Cybersecurity awareness, education, and behavioural change: strategies for promoting secure online practices among end users 7(1)*. Eigenpub Review of Science and Technology, *7*(1), 224–238. https://studies.eigenpub.com/index.php/erst

Smith, R. W., DeNunzio, M. M., Haynes, N. J., & Thiele, A. (2022). The importance of appraisal in stressor–well-being relationships and the examination of personality traits as boundary conditions. *Journal of Managerial Psychology*, *37*(5), 425–443. https://doi.org/10.1108/JMP-11-2019-0649

Smith, T. (2024). Integrated Model of Cybercrime Dynamics: A Comprehensive Framework for Understanding Offending and Victimisation in the Digital Realm. *International Journal of Cybersecurity Intelligence & Cybercrime*, *7*(2)*,* 54–70. https://doi.org/10.52306/2578-3289.1163

Sudha, S. S., Priyanka Bandreddi, J., Mounika Podila, L., Govindula, R., Richardson, A., Niyaz, Q., Yang, X., & Javaid, A. Y. (2023). Impact of smartphone-based interactive learning modules on cybersecurity learning at the high-school level. In *2023 IEEE Global Engineering Education Conference (EDUCON)* 1–8. IEEE. https://doi.org/10.1109/EDUCON54358.2023.10125124

Sulaiman, N. S., Aziz, N. S., Nasir, A., & Yacob, A. (2023). Cyber security awareness model (among children) using Protection Motivation Theory: A review. *International Journal of Business and Technology Management*, *5*(S5), 86–97. https://doi.org/10.55057/ijbtm.2023.5.s5.9

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity Behaviour among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. *Information (Switzerland)*, *13*(9), 1–17. https://doi.org/10.3390/info13090413

Sur, A., Deliema, M., & Brown, E. (2021). *Contextual and social predictors of scam susceptibility and fraud victimisation* (SSRN Scholarly Paper No. 4053903). Social Science Research Network. https://doi.org/10.2139/ssrn.4053903

Wang, Z., Zhu, H., Liu, P., & Sun, L. (2021). Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. *Cybersecurity*, *4*(1), 1–21. https://doi.org/10.1186/s42400-021-00094-6

Wen, X., Xu, L., Wang, J., Gao, Y., Shi, J., Zhao, K., Tao, F., & Qian, X. (2022). Mental States: A Key Point in Scam Compliance and Warning Compliance in Real Life. *International Journal of Environmental Research and Public Health*, *19*(14), 1–16. https://doi.org/10.3390/ijerph19148294

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/JFC-10-2017-0095

Wirtz, P. W., & Rohrbeck, C. A. (2018). The dynamic role of perceived threat and self-efficacy in motivating terrorism preparedness behaviours. *International Journal of Disaster Risk Reduction*, *27*, 366–372. https://doi.org/10.1016/j.ijdrr.2017.10.023

Zulkifli, Z., Ismail, A., Mat Surin, E. S., & Okfalisa, O. (2024). Cyber security awareness model based on NIST (National Institute of Standards and Technology) for Secondary School Students in Malaysia. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *61*(2), 58–68. https://doi.org/10.37934/araset.61.2.5868

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behaviour: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

About the Authors

Haiqal Shazrin Anuar is a postgraduate Master by Research student in Business and Management at Universiti Teknologi MARA, Sarawak, Samarahan. ORHCID ID: 0009-0007-8756-056X. Email at haiqalanuar09@gmail.com for further correspondence.

Mohd Norhisham Razali@Ghazali is a senior lecturer at the Faculty of Business and Management, Universiti Teknologi MARA, Sarawak. His main expertise is Information, Computer, and Communications Technology (ICT). ORCHID ID: 0000-0002-7512-4839. E-mail: hishamrazali@uitm.edu.my

Marlita Mat Yusof is a senior lecturer at the Faculty of Business and Management, Universiti Teknologi MARA, Sarawak. Her main expertise is Information, Computer, and Communications Technology (ICT). ORCID:0009-0006-1178-9352 E-mail: marlita@uitm.edu.my