EDUCAÇÃO E DESENVOLVIMENTO SOCIAL
EDUCATION AND SOCIAL DEVELOPMENT
EDUCACIÓN Y DESAROLLO SOCIAL

millenium

Millenium, 2(29)

en

CONSCIENTIZAÇÃO E MEDIDAS PREVENTIVAS SOBRE PHISHING ENTRE ESTUDANTES UNIVERSITÁRIOS: CONHECIMENTO, COMPORTAMENTOS E PERSPETIVAS DE VITIMIZAÇÃO

PHISHING AWARENESS AND PREVENTIVE MEASURES AMONG UNIVERSITY STUDENTS: KNOWLEDGE, BEHAVIORS, AND VICTIMISATION PERSPECTIVES

CONCIENCIACIÓN SOBRE EL PHISHING Y MEDIDAS PREVENTIVAS ENTRE ESTUDIANTES UNIVERSITARIOS: PERSPECTIVAS DE CONOCIMIENTO, COMPORTAMIENTOS Y VICTIMIZACIÓN

Helmy Ruzaili[1] *https://orcid.org/0009-0005-0080-2913*
Norliza Katuk[2] *https://orcid.org/0000-0001-8805-2574*
Khuzairi Zaini[2] *https://orcid.org/0000-0002-7049-3205*
Wan Abdullah[2] *https://orcid.org/0000-0002-9302-0806*

[1] Faculty of Management and Information Technology, Perak, Malaysia
[2] University Utara Malaysia, Kedah, Malaysia

Helmy Ruzaili – hlmyanip86@gmail.com | Norliza Katuk – k.norliza@uum.edu.my | Khuzairi Zaini - khuzairi@uum.edu.my | Wan Abdullah – w.aida.nadia@uum.edu.my

Corresponding Author:
Norliza Katuk
School of Computing
06010 – Sintok Kedah– Malaysia
k.norliza@uum.edu.my

RECEIVED: 04th October, 2025
REVIEWED: 20th January, 2026
ACCEPTED: 22nd January, 2026
PUBLISHED: 27th February, 2026

DOI: https://doi.org/10.29352/mill0229.43489

RESUMO

Introdução: O phishing representa riscos significativos para indivíduos e organizações, especialmente estudantes universitários que usam plataformas online com frequência e lidam com informações confidenciais. Apesar da disponibilidade de programas de educação e treinamento, há uma compreensão limitada de como o conhecimento, a conscientização e as medidas preventivas interagem para reduzir os riscos de phishing.

Objetivo: Explorar as relações entre conhecimento sobre phishing, medidas preventivas, conscientização sobre segurança cibernética, conscientização sobre phishing e vitimização entre estudantes universitários.

Métodos: Este estudo quantitativo utilizou uma abordagem baseada em inquérito envolvendo 202 estudantes universitários. Os dados foram recolhidos através de questionários autoaplicados, e dez hipóteses foram testadas para analisar as relações entre os principais fatores relacionados com a consciencialização sobre phishing, o comportamento e a vitimização.

Resultados: Foram identificadas correlações positivas entre medidas preventivas e conscientização sobre segurança cibernética e phishing, enfatizando a importância de comportamentos proativos. No entanto, o conhecimento sobre phishing não apresentou relação significativa com a conscientização ou comportamentos preventivos, indicando que o conhecimento por si só não leva a ações eficazes. Apesar dos esforços preventivos, 27,2% dos estudantes relataram ter sofrido ataques de phishing, destacando a necessidade de estratégias mais robustas e práticas.

Conclusão: Os resultados sugerem que programas direcionados de educação, treinamento e conscientização sobre phishing são essenciais para aprimorar comportamentos defensivos contra o phishing. Este estudo oferece insights práticos para educadores, formuladores de políticas e profissionais de segurança cibernética desenvolverem iniciativas de treinamento mais eficazes que reduzam os riscos de phishing, especialmente entre grupos de alto risco, como estudantes universitários.

Palavras-chave: conscientização sobre phishing; segurança cibernética; medidas preventivas; comportamento

ABSTRACT

Introduction: Phishing poses significant risks to individuals and organisations, particularly university students who frequently use online platforms and handle sensitive information. Despite the availability of education and training programs, there is a limited understanding of how knowledge, awareness, and preventive measures interact to reduce phishing risks.

Objective: To explore the relationships between knowledge of phishing, preventive measures, cybersecurity awareness, phishing awareness, and victimisation among university students.

Methods: This quantitative study employed a survey-based approach involving 202 university students. Data were collected using self-administered questionnaires, and 10 hypotheses were tested to analyse relationships among key factors related to phishing awareness, behaviour, and victimisation.

Results: Positive correlations were identified between preventive measures and cybersecurity and phishing awareness, emphasising the importance of proactive behaviours. However, knowledge of phishing showed no significant relationship with awareness or preventive behaviours, indicating that knowledge alone does not lead to effective action. Despite preventive efforts, 27.2% of students reported experiencing phishing attacks, highlighting the need for more robust and practical strategies.

Conclusion: The findings suggest that targeted phishing education, training, and awareness programmes are essential for improving defensive behaviours against phishing. This study offers actionable insights for educators, policymakers, and cybersecurity professionals to develop more effective training initiatives that reduce phishing risks, particularly among high-risk groups such as university students.

Keywords: phishing awareness; cybersecurity; preventive measures; behaviour

RESUMEN

Introducción: El phishing supone riesgos significativos para personas y organizaciones, en particular para estudiantes universitarios que utilizan plataformas en línea con frecuencia y manejan información confidencial. A pesar de la disponibilidad de programas de educación y capacitación, existe una comprensión limitada de cómo interactúan el conocimiento, la concienciación y las medidas preventivas para reducir los riesgos del phishing.

Objetivo: Explorar las relaciones entre el conocimiento del phishing, las medidas preventivas, la conciencia de la ciberseguridad, la conciencia del phishing y la victimización entre los estudiantes universitarios.

Métodos: Este estudio cuantitativo empleó un enfoque basado en encuestas que involucró a 202 estudiantes universitarios. Los datos se recopilaron mediante cuestionarios autoadministrados, y se probaron diez hipótesis para analizar las relaciones entre los factores clave relacionados con la concienciación sobre el phishing, el comportamiento y la victimización.

Resultados: Se identificaron correlaciones positivas entre las medidas preventivas y la concienciación sobre ciberseguridad y phishing, lo que resalta la importancia de las conductas proactivas. Sin embargo, el conocimiento sobre phishing no mostró una relación significativa con la concienciación ni las conductas preventivas, lo que indica que el conocimiento por sí solo no conduce a acciones efectivas. A pesar de los esfuerzos preventivos, el 27,2 % de los estudiantes reportaron haber sufrido ataques de phishing, lo que resalta la necesidad de estrategias más sólidas y prácticas.

Conclusión: Los hallazgos sugieren que los programas de educación, capacitación y concientización sobre phishing son esenciales para mejorar las defensas contra el phishing. Este estudio ofrece información práctica para educadores, legisladores y profesionales de la ciberseguridad, con el fin de desarrollar iniciativas de capacitación más efectivas que reduzcan los riesgos del phishing, especialmente entre grupos de alto riesgo como los estudiantes universitarios.

Palabras clave: concienciación sobre el phishing; ciberseguridad; medidas preventivas; comportamiento

DOI: https://doi.org/10.29352/mill0229.43489

INTRODUCTION

Phishing is a form of cyberattack in which attackers deceive individuals into providing sensitive information, such as usernames, passwords, and financial details, by pretending to be a trustworthy entity (Aziz et al., 2024). It can lead to significant financial losses, identity theft, and data breaches, severely affecting individuals and organisations (Katuk, Ruhani, et al., 2024). The Internet and smart mobile devices have significantly increased the number of Internet users and applications, leading to a sharp rise in phishing attacks. For example, in 2022, 1,097,811 phishing attacks were reported, showing a significant increase, including 47% more threats targeting social media users. This sharp rise highlights the growing sophistication of phishing tactics and the need for increased awareness and proactive measures to mitigate these threats, particularly on platforms like social media, where users are often less vigilant and more susceptible to deception.

Today, university students are among the most active users of the Internet and social media (Ayhan et al., 2025). They are frequent users of online platforms and often less experienced with cybersecurity threats; having a high level of phishing awareness is crucial to protecting their data and ensuring a secure educational environment (Kadaviparambil, 2025). Phishing awareness is especially important for students in higher learning institutions (Katuk, Zaimy, et al., 2024). These students will eventually enter the job market and be recruited by various organisations. It is essential to ensure they have strong phishing awareness as part of good cybersecurity practice to reduce risks for their future employers. They can help minimise potential losses for organisations caused by cybersecurity vulnerabilities, particularly phishing attacks. University students have distinct characteristics compared to other internet users (Kudus et al., 2017). They are typically early adopters of new technologies and platforms, spend significant time online for academic and social purposes, and often lack extensive experience with cybersecurity practices. Therefore, awareness is crucial for university students to help them identify and avoid phishing threats (Rehman et al., 2024). They can effectively filter potential phishing attempts when they know how to recognise suspicious emails and differentiate legitimate communications from fraudulent ones.

Cybersecurity is increasingly essential in today's digital landscape as students enter the workforce. Their level of cybersecurity awareness plays a critical role in protecting organisational assets from threats like phishing and data breaches (Akter et al., 2022). A well-informed workforce contributes to stronger cybersecurity governance by adhering to best practices and supporting the organisation's policies (Edwards, 2024). In organisations, individual awareness is a key factor in effective cybersecurity governance (Alam et al., 2024). Employees with a strong understanding of cybersecurity threats, such as phishing, are better equipped to follow policies and implement preventive measures (Wong et al., 2022). Awareness is essential for minimising vulnerabilities and ensuring the organisation's resilience against cyber threats (Al-Hawamleh, 2024b). It supports the organisation's efforts to establish a robust cybersecurity framework, minimising risks and enhancing security compliance (Al-Hawamleh, 2024a).

There is a lack of understanding among university students about the connections between knowledge of phishing, preventive measures, cybersecurity awareness, phishing awareness, and victimisation (Zwilling et al., 2022). While these factors have been studied individually, their interactions and combined impact on phishing susceptibility remain unclear. Exploring these relationships is crucial for designing more effective strategies to reduce phishing risks among students (Naqvi et al., 2023). Therefore, this study examines the interrelationships among these factors to provide insights into improving cybersecurity awareness and prevention efforts at the university level, particularly among students.

1. THEORETICAL FRAMEWORK

Understanding the factors that drive individuals to adopt protective behaviours against phishing attacks is crucial in developing effective awareness and prevention strategies. Building on the Knowledge-Attitude-Behaviour (KAB) model (An et al., 2023; Hong et al., 2023), which highlights the importance of knowledge acquisition, attitude development, and behavioural outcomes in shaping cybersecurity awareness. This study distinguishes between cybersecurity awareness and phishing awareness. Cybersecurity awareness refers to a broad understanding of online security risks, safe digital practices, and common cyber threats, whereas phishing awareness focuses on phishing tactics, indicators, and response strategies. This section further integrates additional theoretical frameworks to explain how these distinct yet related forms of awareness, together with psychological, social, and motivational factors, shape users' perceptions of cybersecurity threats and their adoption of phishing-prevention behaviours.

The Protection Motivation Theory (PMT) suggests that individuals are driven to safeguard themselves against potential harm by considering the seriousness of the threat, their susceptibility to it, the effectiveness of the recommended protective actions, and their confidence in carrying them out (Marikyan & Papagiannidis, 2023). For instance, when individuals view phishing as a significant threat and consider themselves vulnerable, they are more likely to adopt preventive measures, such as exercising caution with emails and avoiding clicking on suspicious links (Sulaiman et al., 2022). In the Theory of Planned Behaviour (TPB), Ajzen (2011) argued that an individual's intention to engage in a particular behaviour is shaped by their attitude towards the behaviour, subjective norms, and perceived control over it. The TPB is a valuable framework for understanding how social factors

DOI: https://doi.org/10.29352/mill0229.43489

influence an individual's tendency to follow phishing prevention measures, such as peer behaviour and organisational culture. An organisation must have a robust cybersecurity culture that regularly promotes awareness of phishing attacks.

The Social Learning Theory (SLT), Maisto et al. (1999), emphasised observational learning, reinforcements, and self-efficacy. Individuals can learn to avoid phishing by observing others exhibiting positive security behaviours, understanding the benefits of safe practices, and gaining confidence in identifying phishing efforts. The Protection Control Theory (PCT) examines how individuals regulate and adapt their protective actions against phishing, encompassing the utilisation of security tools and tactics (Ezati Rad et al., 2021). In Self-Determination Theory (SDT), Deci and Ryan (2012) emphasised the importance of autonomy, competence, and relatedness in driving behaviour. It posits that individuals are more likely to engage in proactive security behaviours when they perceive these activities as self-determined and under their control (Gagné et al., 2022). Frequently, students come to understand the significance of cybersecurity only after encountering or learning about phishing among their peers (Švábenský et al., 2022). Many students have limited cybersecurity awareness, especially in recognising online security risks and understanding the consequences of cyberattacks.

This study investigates five key factors influencing phishing resilience and cybersecurity behaviour among university students—preventive measures, cybersecurity awareness, phishing awareness, knowledge of phishing, and phishing victims—and examines their connections with the theoretical frameworks discussed earlier. Preventive measures (such as using strong passwords and avoiding suspicious links) align with the PMT, which emphasises adopting protective actions when individuals perceive the severity and vulnerability of a threat. Cybersecurity awareness reflects the broader understanding of online risks and is shaped by the TPB, highlighting how attitudes, norms, and perceived control influence preventive intentions. Phishing awareness, a more targeted aspect, aligns with the SLT, as individuals can develop awareness by observing others' positive security practices and experiencing reinforcement.

Knowledge of phishing, which includes understanding the tactics and strategies employed by attackers, aligns with the SDT, as individuals with greater competence are more likely to adopt proactive security behaviours. Lastly, phishing victims, or individuals who have fallen prey to phishing attacks, represent outcomes that are influenced by insufficient awareness, lack of confidence (as outlined by the PCT), and inadequate preventive measures. This study examines the interplay between these factors and theoretical foundations, aiming to provide a more comprehensive understanding of the drivers and barriers to effective phishing prevention.

Figure 1 illustrates the relationships between several elements related to phishing awareness and victimisation. The components include preventive measures, cybersecurity awareness, phishing awareness, knowledge of phishing, and support for phishing victims. The various components are connected by a set of hypotheses, Hypothesis 1 (H1) to Hypothesis 10 (H10), as below:

a. H1: Preventive Measures Positively Influence Cybersecurity Awareness.
b. H2: Cybersecurity Awareness positively influences Phishing Awareness.
c. H3: Cybersecurity Awareness positively influences Knowledge of Phishing.
d. H4: Knowledge of Phishing positively influences Preventive Measures.
e. H5: Knowledge of Phishing positively influences Phishing Awareness.
f. H6: Phishing Awareness positively influences Preventive Measures.
g. H7: Knowledge of Phishing negatively influences the likelihood of becoming a Phishing Victim.
h. H8: Preventive Measures negatively influence the likelihood of becoming a Phishing Victim.
i. H9: Phishing Awareness negatively influences the likelihood of becoming a Phishing Victim.
j. H10: Becoming a Phishing Victim negatively impacts Preventive Measures.
k. The hypotheses demonstrate the impact of one element on another in the context of phishing attacks. The model proposes that preventive measures and cybersecurity awareness directly affect phishing awareness, which, in turn, influences the likelihood of falling victim to phishing attacks. In addition, the model incorporates feedback loops, including the impact of becoming a phishing victim on preventive actions and the cyclical effects of awareness and knowledge on phishing attack prevention. The model's hypotheses explore the interconnected relationships among factors related to phishing awareness and victimisation.

DOI: https://doi.org/10.29352/mill0229.43489

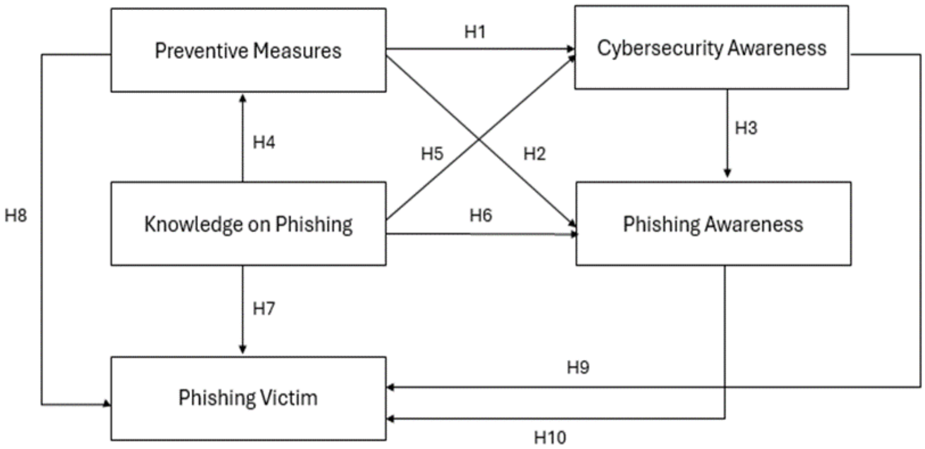

Figure 1 – The Research Model and Hypotheses

H1 suggests that preventive measures positively influence cybersecurity awareness, while H2 and H3 propose that cybersecurity awareness, in turn, positively influences phishing awareness. H4 posits that preventive measures also positively affect knowledge of phishing, and H5 further indicates that cybersecurity awareness contributes to this knowledge. According to H6, phishing awareness enhances knowledge of phishing. The model then explores the negative relationships: H7 suggests that increased knowledge of phishing reduces the likelihood of becoming a phishing victim. However, H8, H9, and H10 hypothesise that being a phishing victim negatively affects preventive measures, phishing awareness, and knowledge of phishing, respectively. These relationships collectively highlight the dynamic interplay between awareness, preventive actions, and the impact of phishing incidents on an individual's ability to defend against such threats.

Implementing preventive measures, particularly H1, H4, and H8, is crucial for enhancing cybersecurity awareness and knowledge about phishing. The strong association between implementing preventive measures and enhancing cybersecurity awareness suggests that organisations and individuals who adopt proactive measures are better able to understand cybersecurity issues. Furthermore, implementing preventive measures may reduce the likelihood of becoming vulnerable to phishing attacks. Cybersecurity knowledge is essential, as a deeper understanding of cybersecurity enhances phishing awareness. Proficiency in essential cybersecurity principles enhances individuals' ability to recognise and understand phishing attempts. Gaining a comprehensive understanding of phishing and its many strategies is crucial in this framework, as greater knowledge of phishing enhances cybersecurity awareness (Frauenstein et al., 2023).

2. METHODS

This study employs a survey-based approach, utilising self-rated questionnaires to gather data from respondents. Unlike experimental methods or simulated phishing environments, this approach allows participants to self-assess their awareness, knowledge, and behaviour related to phishing. The study captures respondents' perceptions and experiences in a natural context rather than in controlled or artificial scenarios, focusing on self-reported data. This method provides valuable insights into their understanding and practices while avoiding the potential biases that may arise from simulated experiments or phishing simulations.

2.1 Sample

The respondents in this survey were students from a public university in Malaysia. An advertisement inviting participation was distributed through the university's official social media channels. Participation was voluntary, with no incentives given. Data collection was conducted through a Google Form survey accessible to respondents during May 2024. A total of 202 students participated in the study.

2.2 Data collection instruments

The primary instrument used in this study was a structured online self-administered questionnaire designed to assess various factors related to phishing awareness and behaviours. The instrument was reviewed and validated by two experts in social science and cybersecurity research to ensure its validity and reliability. A pilot test was conducted with ten respondents to evaluate the

DOI: https://doi.org/10.29352/mill0229.43489

clarity and comprehensibility of the questions. Feedback from the pilot test was used to refine the questionnaire and enhance its effectiveness. The final questionnaire consisted of four sections summarised below:

a. Section A - Demographic information (10 multiple-choice questions)
b. Section B - Phishing knowledge (10 multiple-choice knowledge-based questions)
c. Section C – Preventive measures (6 dichotomous Yes/No questions)
d. Section D - Cybersecurity and phishing awareness (2 self-rating scale questions; scales from 1-10)

2.3 Statistical analysis

After downloading survey responses in CSV format, data cleaning was done. Missing values, repeats, and discrepancies were addressed. Clean data was imported into SPSS for analysis. Means, medians, and standard deviations were calculated to evaluate students' phishing awareness and cybersecurity behaviour. A non-parametric correlation analysis utilising Spearman's rank-order correlation examined the relationships between phishing knowledge, cybersecurity behaviours, and phishing threat attitudes. To facilitate statistical analysis, composite scores were computed for the main study constructs, namely phishing knowledge, preventive measures, cybersecurity awareness, and phishing awareness. For each construct, responses to the relevant questionnaire items were aggregated by calculating the mean score of the items within the corresponding section. Multiple-choice knowledge items were coded as binary values (correct = 1, incorrect = 0), while dichotomous behavioural items were coded as Yes = 1 and No = 0. Self-rating awareness items were retained on their original 1–10 scale. The resulting composite scores provided standardised representations of each construct and were subsequently used in the correlation analysis.

3. RESULTS

3.1 Demographic background

The majority are female (74.8%) and aged 21-25 years (79.2%), with most being Malaysian (97.0%). Smartphone ownership is highest (38.34%), followed by laptops (32.56%) and tablets (24.66%). Instagram is the most popular social media platform (28.49%), followed by TikTok (25.64%) and Facebook (19.34%). Financial services are nearly evenly split between phone banking (33.74%), internet banking (33.04%), and e-wallets (31.28%), while cryptocurrency investment is rare (1.93%). Regarding cybersecurity, 13.9% have experienced identity theft, 27.2% have encountered phishing attacks, and the frequency of password updates varies: 38.1% update annually, and 35.6% never update them. Table 1 summarises the participants' demographics, technological habits, and security behaviours.

Table 1 - The participants' demographics, technological habits, and security behaviours

Items	Frequency (%)
Gender	Male: 51(25.2%), Female:151 (74.8%)
Age	18-20 Years Old: 131 (15.3%), 21-25 Years Old: 160 (79.2%), 26-30 Years Old: 3(1.5%), 31 Years Old and Above: 8 (4%)
Nationality	Malaysian: 196 (97%), Non-Malaysian: 6 (3%)
Devices	Smartphone: 199 (38.34%), Laptop: 169 (32.56%), Tablet: 128 (24.66%), Desktop: 16 (3.085), Gaming Console: 7 (1.35%)
Social Media	Instagram: 190 (28.49%), Tiktok: 171 (25.64%), Facebook: 129 (19.34%), Twitter: 109 (15.29%), Snapchat: 60 (9%), Other: 1 (0.5%)
Financial Services	Phone Banking: 192 (33.745%), Internet Banking: 188 (33.04%), E-Wallet: 178 (31.28%), Cryptocurrency Investment: 11 (1.93%), Other: 0 (0%)
Identity Theft	Yes: 28 (13.9%), No: 174 (86.1%)
Participants Experiencing Phishing Attacks	Yes: 55 (27.2%), No: 147 (72.8%)
Frequency of Password Updates	Monthly: 4 (2%), Every three months: 26 (12.9%), Every six months: 23 (11.4%), Annually: 77 (38.1%), Never: 72 (35.6%)

The students' responses to the phishing-related knowledge questions were analysed. It highlights the frequency and percentages of correct and incorrect answers for each question, demonstrating participants' overall understanding of phishing. The analysis reveals varying levels of knowledge, with the highest correct response rate being 94.55% for identifying recommended practices to protect against phishing, while the lowest was 44.55% for knowing what to do when receiving a suspicious email. The overall mean percentage of correct answers is 71.26%, with a standard deviation of 16.04%, indicating variability in participants' phishing knowledge and awareness. Table 2 presents a detailed analysis of participants' responses to various phishing awareness and prevention questions.

DOI: https://doi.org/10.29352/mill0229.43489

Table 2 - The student responses to phishing knowledge questions

Questions	Correct Answer		Wrong answer	
	Frequency	%	Frequency	%
What is phishing?	153	75.74	49	24.26
Which of the following is a common method used in phishing attacks?	123	60.89	79	39.11
How can you identify a phishing email?	171	84.65	31	15.35
What should you do if you receive a suspicious email?	90	44.55	112	55.45
Which of the following is a recommended practice to protect yourself from phishing attacks?	191	94.55	11	5.45
Phishing emails often contain spelling and grammatical errors.	180	89.11	22	10.89
Which of the following is an example of spear phishing?	111	54.95	91	45.05
What is the primary goal of a phishing attack?	135	66.83	67	33.17
How can social media platforms be used in phishing attacks?	126	62.07	77	37.93
Which of the following steps would you take to handle a phishing email?	160	79.21	42	20.79
Mean	144	71.26	58.10	28.74
Standard Deviation	32.36	16.04	32.42	16.04

Table 3 provides an overview of participants' behaviours and practices related to online security, focusing on actions such as checking URLs, using two-factor authentication, sharing passwords, and managing privacy settings. The data indicates a high level of awareness in some areas: 92.57% of participants use two-factor authentication, and 90.59% check their social media privacy settings. However, there are also areas of concern, such as 78.71% of participants having clicked on a phishing link in an email. The mean percentage of correct practices is 60.97%, with a standard deviation of 35.58%, reflecting a wide range of security behaviours among the participants.

Table 3 - Student awareness of preventive measures against phishing

Questions	Correct Answer		Wrong answer	
	Frequency	%	Frequency	%
Do you check the URL before clicking on links in emails or messages?	168	83.17	34	16.83
Do you use two-factor authentication for your online accounts?	187	92.57	15	7.43
Have you ever shared your password with someone else?	25	12.38	177	87.62
Have you checked the privacy settings on your social media accounts?	183	90.59	19	9.41
Have you ever clicked on a link in an email and found it to be a phishing attempt?	43	21.29	159	78.71
Is your device equipped with the latest antivirus software?	133	65.84	69	34.16
Mean	123.17	60.97	78.83	39.03
Standard Deviation	71.87	35.58	71.87	35.58

Table 4 illustrates the distribution of responses on a 10-point scale, reflecting the frequency and percentage of participants' ratings. The most common rating is 8, selected by 28.7% of participants, followed by 9, chosen by 16.3%. Lower ratings, such as 1 and 3, are rare, accounting for only 0.5% of responses each. The table shows that higher ratings are more common, with 8, 9, and 10 accounting for over 57% of the total responses, suggesting that participants tend to rate their experiences or opinions on the higher end of the scale.

Table 4 - Self-rated cybersecurity awareness levels on a scale of 1 to 10

Scale	Frequency	%
1	1	0.5
2	0	0.0
3	1	0.5
4	2	1.0
5	15	7.4
6	35	17.3
7	32	15.8
8	58	28.7
9	33	16.3
10	25	12.4
Total	202	100.0

Table 5 provides a breakdown of participant responses on a 10-point scale, showing the frequency and percentage for each rating. The most frequent rating is 8, selected by 28.2% of participants, followed by 7, chosen by 15.3%. Ratings of 9 and 10 are equally standard, each representing 14.4% of the responses. Lower ratings, such as 1 and 2, are less frequent, with only 1.0% and 0.0% of participants selecting them, respectively. The data suggests that most participants rated their experiences or opinions in the higher range of the scale, with 72.3% of the ratings falling between 7 and 10.

DOI: https://doi.org/10.29352/mill0229.43489

Table 5 - Self-rating of participants' phishing awareness level

Scale	Frequency	%
1	2	1.0
2	0	0.0
3	5	2.5
4	6	3.0
5	20	9.9
6	23	11.4
7	31	15.3
8	57	28.2
9	29	14.4
10	29	14.4
Total	202	100.0

3.2 Hypotheses test

This study analyses the relationships between phishing knowledge, preventive measures, cybersecurity awareness, phishing awareness, and victimisation among university students. The study found strong positive correlations between preventive measures and awareness levels, indicating that existing educational programs have improved students' phishing awareness and responses. Knowledge of phishing does not significantly connect with preventive measures or cybersecurity and phishing awareness levels. It underlines a fundamental deficiency in education programs: knowledge alone cannot motivate effective preventive behaviours. The findings emphasise the need to teach and encourage proactive security in educational programs. Correlation analysis was used to determine phishing awareness and behaviour characteristics for the third objective.

Table 6 presents Spearman's rho correlation coefficients, showing the relationships between factors related to phishing knowledge, preventive measures, cybersecurity awareness, phishing awareness, and victimisation. Each correlation is accompanied by the significance level (p-value) and the number of participants (N) for each relationship. Knowledge of phishing shows weak and non-significant correlations with other factors. The strongest positive correlation is with a victim (correlation coefficient = 0.112, p < 0.113), but this is not statistically significant. Preventive measures are positively and significantly correlated with both cybersecurity awareness levels (correlation coefficient = 0.388, p < 0.001) and phishing awareness levels (correlation coefficient = 0.366, p < 0.001), indicating that higher preventive measures are associated with greater awareness in these areas. However, it shows a weak, non-significant negative correlation with a victim (correlation coefficient = -0.100, p = 0.159).

Table 6 - Spearman's Rho correlation coefficients for phishing knowledge, preventive measures, and awareness levels

Variables	Knowledge on Phishing	Preventive Measures	Cybersecurity Awareness	Phishing Awareness	Victim
Knowledge on Phishing	1.000	-0.011	-0.055	-0.094	0.112
p-value	-	0.875	0.435	0.183	0.113
Preventive Measures	-0.011	1.000	0.388	0.366	-0.100
p-value	0.875	-	<0.001	<0.001	0.159
Cybersecurity Awareness	-0.055	0.388	1.000	0.834	-0.067
p-value	0.435	<0.001	-	<0.001	0.342
Phishing Awareness	-0.094	0.366	0.834	1.000	-0.099
p-value	0.183	<0.001	<0.001	-	0.163
Victim	0.112	-0.100	-0.067	-0.099	1.000
p-value	0.113	0.159	0.342	0.163	-

Cybersecurity awareness shows a strong positive correlation with phishing awareness (r = 0.834, p < 0.001), indicating that individuals with higher cybersecurity awareness are more aware of phishing threats. The correlations with the victim (correlation coefficient = -0.067, p = 0.342) and knowledge of phishing (correlation coefficient = -0.055, p < 0.435) are weak and non-significant. Phishing awareness level has a weak, negative, and non-significant correlation with victims (correlation coefficient = -0.099, p < 0.163). The victim is negatively correlated with most other variables, except knowledge of phishing. Although there are significant positive correlations between preventive measures, cybersecurity, and phishing awareness levels, many are weak and insignificant, suggesting that these variables may not have substantial direct relationships in this study.

The hypothesis testing confirmed significant correlations between preventive measures and both cybersecurity awareness (r = 0.388, p < 0.001) and phishing awareness (r = 0.366, p < 0.001). Additionally, a strong and significant relationship was observed between cybersecurity and phishing awareness (r =0.834, p < 0.001). These results validate the hypothesis that preventive measures positively influence cybersecurity and phishing awareness. Conversely, the analysis found no significant relationships between knowledge of phishing and preventive measures (r = -0.011, p = 0.875), cybersecurity awareness (r = -0.055, p = 0.435), or phishing awareness (r = -0.094, p = 0.183). Similarly, there was no significant correlation between phishing knowledge and the likelihood of becoming a phishing victim (r = 0.112, p = 0.113).

These findings suggest that while students may be aware of phishing, this awareness does not necessarily translate into heightened vigilance or the adoption of protective measures. Moreover, no substantial correlations were found between becoming a phishing victim and other variables, including preventive measures (r = -0.100, p = 0.159), cybersecurity awareness (r = -0.067, p = 0.342), and phishing awareness (r = -0.099, p = 0.163). It indicates that, despite awareness of phishing risks and preventive measures, students remain vulnerable to phishing attacks, underscoring the need for more comprehensive strategies that go beyond awareness and preventive measures alone. The results of the hypothesis testing are summarised below:

a. H1: Preventive Measures positively influence Cybersecurity Awareness - Accepted
b. H2: Cybersecurity Awareness positively influences Phishing Awareness - Accepted
c. H3: Cybersecurity Awareness positively influences Knowledge of Phishing - Accepted
d. H4: Knowledge of Phishing positively influences Preventive Measures - Rejected
e. H5: Knowledge of Phishing positively influences Phishing Awareness - Rejected
f. H6: Phishing Awareness positively influences Preventive Measures- Rejected
g. H7: Knowledge of Phishing negatively influences the likelihood of becoming a Phishing Victim - Rejected
h. H8: Preventive Measures negatively influence the likelihood of becoming a Phishing Victim - Rejected
i. H9: Phishing Awareness negatively influences the likelihood of becoming a Phishing Victim - Rejected
j. H10: Becoming a Phishing Victim negatively impacts Preventive Measures - Rejected

4. DISCUSSION

The findings provide important insights into university students' cybersecurity preparedness and vulnerabilities in contemporary digital environments. The demographic profile indicates that most respondents were young adults aged 21–25 years (79.2%), predominantly female (74.8%), and heavily reliant on smartphones (38.34%) and social media platforms, particularly Instagram (28.49%) and TikTok (25.64%). This strong dependence on mobile and social media technologies increases exposure to phishing threats, especially those exploiting informal communication channels and social engineering tactics. These patterns highlight the need for awareness programmes that specifically address phishing risks in mobile and social media contexts. Although a high proportion of students reported adopting basic preventive measures—such as using two-factor authentication (92.57%) and checking social media privacy settings (90.59%)—a substantial majority (78.71%) admitted to having clicked on a phishing link. In addition, 35.6% of respondents reported never updating their passwords. These findings indicate a clear gap between the adoption of basic security practices and the ability to effectively recognise and respond to phishing attempts. From the perspective of Protection Motivation Theory (PMT), this suggests that while coping mechanisms may be present, threat appraisal and response efficacy may not be sufficiently internalised to prevent risky behaviour in real situations.

The study also revealed uneven levels of phishing knowledge. While most participants correctly identified recommended protective practices (94.55%), fewer than half (44.55%) knew the appropriate actions to take upon receiving a suspicious email. The overall mean score for phishing knowledge was 71.26% (SD = 16.04%), indicating moderate understanding with considerable variability among students. Despite this, correlation analysis showed that phishing knowledge was not significantly associated with preventive measures (r = −0.011, p = 0.875), cybersecurity awareness (r = −0.055, p = 0.435), or phishing awareness (r = −0.094, p = 0.183). These results empirically reinforce the knowledge–action gap, challenging assumptions embedded in traditional awareness programmes and supporting extensions of the Knowledge–Attitude–Behaviour (KAB) model, which emphasise that knowledge alone does not guarantee behavioural change. Preventive measures, however, were significantly correlated with cybersecurity awareness (r = 0.388, p < 0.001) and phishing awareness (r = 0.366, p < 0.001), suggesting that students who actively practise protective behaviours tend to demonstrate higher awareness levels. Furthermore, cybersecurity awareness showed a very strong positive correlation with phishing awareness (r = 0.834, p < 0.001), indicating that general cybersecurity understanding provides a foundation for recognising phishing-specific threats. This finding aligns with the Theory of Planned Behaviour (TPB), where attitudes and perceived behavioural control play key roles in shaping awareness and intentions.

Despite these positive associations, neither preventive measures nor awareness levels were significantly related to reduced victimisation. Notably, 27.2% of students reported experiencing phishing attacks, and 13.9% reported identity theft. Preventive measures showed a weak and non-significant negative correlation with victimisation (r = −0.100, p = 0.159), while cybersecurity awareness (r = −0.067, p = 0.342) and phishing awareness (r = −0.099, p = 0.163) also failed to demonstrate protective effects. These findings suggest that awareness and basic preventive actions alone may be insufficient to counter increasingly sophisticated phishing techniques. The lack of association between victimisation and improved preventive behaviour (H10) is particularly noteworthy. Contrary to expectations that prior negative experiences would enhance caution, the findings suggest the presence of risk normalisation, overconfidence bias, or security fatigue, where repeated exposure to threats reduces vigilance rather than strengthening it. From a Self-Determination Theory (SDT) perspective, this may indicate that preventive behaviours are externally motivated rather than internally regulated, limiting sustained behavioural change. Similarly, Social Learning Theory (SLT) suggests that without consistent reinforcement and observable successful avoidance behaviours, students may fail to translate awareness into action.

Overall, the results indicate that while preventive measures and awareness are interrelated, their impact on reducing phishing victimisation remains limited. These findings underscore the need for behaviourally grounded and experiential training approaches, such as phishing simulations, scenario-based exercises, and reflective learning activities. Integrating Phishing Education, Training, and Awareness (PETA) strategies that address cognitive, motivational, and psychological factors may help bridge the gap between knowledge and action, ultimately strengthening students' resilience against phishing attacks (Sarker et al., 2024).

CONCLUSION

This study analysed the relationships among preventive measures, cybersecurity awareness, and phishing awareness among university students and how these factors affect phishing victims. The study revealed significant correlations between preventive measures and cybersecurity, as well as between preventive measures and phishing awareness. Proactive behaviours, such as prevention, increase students' awareness in both areas. The study also revealed a connection between cybersecurity and phishing awareness. Surprisingly, phishing knowledge alone does not increase cybersecurity or enhance phishing awareness, nor does it influence preventive measures. It challenges the idea that knowledge automatically leads to action or awareness. The study also found no significant effect of preventive measures or knowledge levels on phishing vulnerability, suggesting that other factors are more important. These findings suggest the need for further research into the knowledge-action gap, particularly regarding phishing awareness. This study advances cybersecurity by examining university students' phishing awareness. One important finding is that preventive measures improve cybersecurity and increase phishing awareness. It emphasises the need for students to receive proactive cybersecurity education.

The study also reveals that cybersecurity and phishing knowledge are closely linked, suggesting that educational programs in either area can benefit from the other. The discovery that knowing about phishing does not immediately raise awareness or protective behaviour is another key finding. It challenges assumptions and emphasises the need for more effective teaching practices that go beyond mere information. The research also highlights factors that increase the vulnerability to phishing attacks, suggesting that awareness and knowledge may not be enough to prevent victims. These insights help educators, politicians, and IT security experts create more effective awareness programs and interventions that educate and promote protective behaviours.

Despite its contributions, this study has some limitations. The sample was drawn from a single public university, which may limit the generalisability of the findings to other institutional or cultural contexts. The reliance on self-reported questionnaire data may introduce response and social desirability biases, as reported awareness and behaviours may not fully reflect actual practices. In addition, the cross-sectional and correlational design prevents causal interpretation of the relationships examined and does not allow for the exploration of more complex multivariate effects. Furthermore, this study adopted an exploratory approach and did not incorporate advanced causal or multivariate analytical techniques, such as regression analysis or structural equation modelling. Although expert review and pilot testing were used to enhance clarity and content validity, reliability coefficients and advanced construct validity testing were not conducted. The absence of behavioural validation, such as simulated phishing exercises, also limits the assessment of real-world responses. Future research could address these limitations by employing longitudinal or experimental designs, larger and more diverse samples, multivariate modelling, and behavioural measures to strengthen methodological rigour.

ACKNOWLEDGEMENTS

This work was supported by the Graduate Development Research Grant Scheme (Code: 21650), Universiti Utara Malaysia.

AUTHORS' CONTRIBUTION

Conceptualization, H.R., N.K., K.Z. and W.A.; data curation, H.R. and N.K.; funding acquisition, N.K., K.Z. and W.A.; investigation, H.R.; methodology, N.K.; project administration, N.K. and K.Z.; resources, N.K. and K.Z.; software, H.R. and N.K.; supervision, N.K. and K.Z.; validation, N.K.; visualization, H.R.; writing – original draft, H.R., N.K., K.Z. and W.A.; writing – review & editing, H.R., N.K. and K.Z.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health, 26*(9), 1113-1127. https://doi.org/10.1080/08870446.2011.613995

Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2022). Reconceptualising cybersecurity awareness capability in the data-driven digital economy. *Annals of Operations Research*. https://doi.org/10.1007/s10479-022-04844-8

Al-Hawamleh, A. M. (2024a). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. *International Journal of Computing and Digital Systems, 15*(1), 1315-1331. https://doi.org/10.12785/ijcds/150193

Al-Hawamleh, A. M. (2024b). Securing the future: Framework fundamentals for cyber resilience in advancing organisations. *Journal of System and Management Sciences, 14*(10), 130-150. https://doi.org/10.33168/JSMS.2024.1008

DOI: https://doi.org/10.29352/mill0229.43489

Alam, R. G. G., Ibrahim, H., & Karas, I. R. (2024). Key issues in cybersecurity implementation in government agencies: A case study in Jakartasmart city. *Communications in Computer and Information Science, 2001*, 3-16. https://doi.org/10.1007/978-981-99-9589-9_1

An, Q., Hong, W. C. H., Xu, X., Zhang, Y., & Kolletar-Zhu, K. (2023). How education level influences internet security knowledge, behaviour, and attitude: A comparison among undergraduates, postgraduates and working graduates. *International Journal of Information Security, 22*(2), 305-317. https://doi.org/10.1007/s10207-022-00637-z

Ayhan, B., Kose, S., Saban Guler, M., & Bilici, S. (2025). Can social media be a threat or an opportunity to public health via the impacts on diet quality?. *Frontiers in Public Health*, *13*, 1679178. https://doi.org/10.3389/fpubh.2025.1679178

Aziz, M.A.A., Riskhan, B., Zakaria, N.H., & Jambli, M.N. (2024). An exploratory study of automated anti-phishing system. In N. H. Zakaria, N. S. Mansor, H. Husni, & F. Mohammed (Eds.), *Computing and Informatics. ICOCI 2023*. *Communications in Computer and Information Science* (Vol. 2001, pp. 45-60). Springer. https://doi.org/10.1007/978-981-99-9589-9_5

Deci, E. L., & Ryan, R. M. (2012). Self-determination theory. In P. A. M. Van Lange, A. W. Kruglanski, & E. T. Higgins (Eds.), *Handbook of theories of social psychology, 1*(20), 416-436. https://doi.org/10.4135/9781446249215.n21

Edwards, J. (2024). Security policies and procedures. In *Mastering Cybersecurity: Strategies, Technologies, and Best Practices*, 413-434. https://doi.org/10.1007/979-8-8688-0297-3_12

Ezati Rad, R., Mohseni, S., Kamalzadeh Takhti, H., Hassani Azad, M., Shahabi, N., Aghamolaei, T., & Norozian, F. (2021). Application of the protection motivation theory for predicting COVID-19 preventive behaviors in Hormozgan, Iran: A cross-sectional study. *BMC Public Health, 21*(1), 466. https://doi.org/10.1186/s12889-021-10500-w

Frauenstein, E. D., Flowerday, S., Mishi, S., & Warkentin, M. (2023). Unraveling the behavioral influence of social media on phishing susceptibility: A Personality-Habit-Information Processing model. *Information and Management, 60*(7), 103858. https://doi.org/10.1016/j.im.2023.103858

Gagné, M., Parker, S. K., Griffin, M. A., Dunlop, P. D., Knight, C., Klonek, F. E., & Parent-Rocheleau, X. (2022). Understanding and shaping the future of work with self-determination theory. N*ature Reviews Psychology, 1*(7), 378-392. https://doi.org/10.1038/s44159-022-00056-w

Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N.-L., & Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Education and Information Technologies, 28*(1), 439-470. https://doi.org/10.1007/s10639-022-11121-5

Kadaviparambil, S. T. (2025). *Generational cyber curiosity: A quantitative study of security situational awareness* [Tesis doctoral, Universidad correspondiente]. ProQuest Dissertations & Theses Global.

Katuk, N., Ruhani, A. B., Malik, M., Mahamood, A. K., & Omar, M. S. A. (2024). Protecting higher learning institutions from phishing attacks: A staff awareness program. *Intelligent Systems of Computing and Informatics*, 114-132. https://doi.org/10.1201/9781003400387-8

Katuk, N., Zaimy, N. A., Krishnan, S., Kunhiraman, R. K., Lee, H. H., & Eleyan, D. (2024). Fostering cyber-resilience in higher education: A pilot evaluation of a malware awareness program for college students. *Communications in Computer and Information Science*, 2002, 154-167. https://doi.org/10.1007/978-981-99-9592-9_12

Kudus, N., Sidek, S., Izharrudin, Z., Kamalrudin, M., Abu Hassan, M., & Mohamed, S. (2017). Internet usage pattern and types of Internet users among Malaysian university students. *Journal of Engineering and Applied Sciences, 12*(6), 1433-1439. https://doi.org/10.3923/jeasci.2017.1433.1439

Maisto, S. A., Carey, K. B., & Bradizza, C. M. (1999). Social learning theory. In K.E. Leonard & H.T. Blane (Eds.), *Psychological theories of drinking and alcoholism* (2ª ed., pp. 106-163). Guilford Press.

Marikyan, D., & Papagiannidis, S. (2023). Protection motivation theory: A review. *TheoryHub Book*, 78-93. Newcastle University. https://open.ncl.ac.uk/theory-library/TheoryHubBook.pdf

Rehman, M., Akbar, R., Omar, M., & Gilal, A. R. (2024). A systematic literature review of ransomware detection methods and tools for mitigating potential attacks. *Communications in Computer and Information Science, 2001*, 80-95. https://doi.org/10.1007/978-981-99-9589-9_7

Sarker, O., Jayatilaka, A., Haggag, S., Liu, C., & Babar, M. A. (2024). A multi-vocal literature review on challenges and critical success factors of phishing education, training and awareness. *Journal of Systems and Software, 208*, 111899. https://doi.org/10.1016/j.jss.2023.111899

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information, 13*(9), 413. https://doi.org/10.3390/info13090413

Švábenský, V., Weiss, R., Cook, J., Vykopal, J., Celeda, P., MacHe, J., Chudovský, R., & Chattopadhyay, A. (2022). Evaluating two approaches to assessing student progress in cybersecurity exercises. *SIGCSE 2022 - Proceedings of the 53rd ACM Technical Symposium on Computer Science Education,* 1, 787-793. https://doi.org/10.1145/3478431.3499414

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management, 66*, 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520