Cybersecurity Awareness Among Polytechnic Mersing Students

Syarifah Hana Binti Syed Zubin[1*], Puziah Haiza Binti Pazui[2], Dr Nurul Shida Binti Noni[3]

[1,2,] Department of Information Technology & Communication, Politeknik Mersing Johor,
[3]Department of Mathematics, Science & Computer, Politeknik Ibrahim Sultan.

*Corresponding author's email: hana@tvet.pmj.edu.my

Abstract: This study investigates the cybersecurity awareness level among Politeknik Mersing students, addressing the growing need for cybersecurity education in academic institutions. With the rise in cyber threats such as phishing, data breaches, and identity theft, students are increasingly vulnerable to online attacks. A survey of 62 students assessed their understanding of key cybersecurity concepts, behaviors related to online security, and experiences with cybersecurity incidents. The findings reveal a moderate to high level of awareness, particularly regarding privacy settings on social media and caution regarding data collection. However, gaps were identified in crucial practices such as password management and email security. A significant number of students reuse passwords across devices and are unaware of the risks associated with using unsecured Wi-Fi networks. This study highlights the critical need for tailored cybersecurity education programs to bridge the gap between students' theoretical knowledge and their practical application of security measures, enhancing their overall cybersecurity posture.

Keywords: Cybersecurity awareness; Phishing attacks; Password management; Cybersecurity education; Online security practices

1.0 INTRODUCTION

In today's digital age, cybersecurity awareness is of paramount importance, particularly in educational institutions like polytechnics, where students are increasingly exposed to the internet for both academic and personal purposes. The rise in cybercrime, including phishing attacks, data breaches, and malware incidents, highlights the need for enhanced security measures and greater awareness among users (Alharbi & Tassaddiq, 2021). According to recent studies, educational institutions have become prime targets for cybercriminals due to the vast amounts of personal and institutional data they manage. Students, often inexperienced in identifying online threats, are vulnerable to these attacks, which can have serious consequences for both their personal information and academic integrity (Saeed, 2023).

The main objective of this study is to identify the level of cybersecurity awareness among students at Politeknik Mersing. Understanding their awareness levels will provide insights into potential knowledge gaps and allow for targeted interventions to improve cybersecurity practices. Specifically, the study aims to assess students' understanding of key cybersecurity concepts, familiarity with common cyber threats, and behaviour in managing personal data and online security.

Technology integration into education has transformed how students access information, collaborate, and complete their academic tasks. However, with these advancements come new risks. Frequent internet usage, particularly for accessing educational platforms, cloud services, and social media, has increased students' exposure to cyber threats. A recent report by Saeed (2023) highlights that while students are becoming more digitally literate, their cybersecurity knowledge remains insufficient, particularly in password management and phishing detection. This gap in awareness could lead to increased vulnerability to cyberattacks, which, in turn, can disrupt academic processes and lead to financial losses or identity theft.

One of the latest issues impacting cybersecurity awareness is the prevalence of phishing attacks aimed at educational institutions. These attacks often target students' email accounts, tricking them into divulging sensitive information or downloading malicious software. A study conducted in 2023 by Alharbi & Tassaddiq (2021) found that a significant number of students in Saudi Arabian universities were unaware of how to identify phishing emails, reflecting a broader trend in global cybersecurity literacy. Additionally, the COVID-19 pandemic has intensified online learning, increasing the time students spend online and thus their exposure to potential threats. As students rely more on online

platforms, their personal information and academic records become attractive targets for cybercriminals.

As educational institutions increasingly adopt digital tools and platforms, students must be equipped with knowledge and skills to protect themselves against online threats. This study on the cybersecurity awareness of Politeknik Mersing students will provide valuable insights into their preparedness and suggest ways to improve their security practices. By raising awareness and providing practical cybersecurity education, institutions can help mitigate the risks associated with frequent internet use and ensure a safer academic environment for students (Chugh et.al, 2021). Promoting cybersecurity awareness in educational settings helps students develop good digital hygiene, which not only protects them individually but also contributes to a safer online community. By fostering a culture of cybersecurity awareness, schools and universities can equip students with the skills they need to navigate the digital world safely and confidently.

Furthermore, research has shown that targeted cybersecurity training can significantly improve awareness and promote safer online behaviour among young users. Zukarnain et al. (2020) demonstrated that after receiving cybersecurity education, students were more likely to engage in secure online practices, such as using stronger passwords and avoiding suspicious links. The impact of such training programs is clear, but continuous reinforcement is necessary to ensure that awareness persists, especially as new cyber threats evolve.

This study aims to address the urgent need to enhance cybersecurity knowledge among Politeknik Mersing students by identifying current knowledge gaps and behavioral tendencies. The prevalence of cyber threats, including phishing scams, data breaches, and identity theft, emphasizes the need for proactive security measures and cybersecurity knowledge. Understanding the various demographic groups at Politeknik Mersing's levels of cybersecurity knowledge is crucial for devising effective strategies to tackle these issues. Based on the study’s findings, potential interventions such as cybersecurity workshops, password security training, curriculum integration, and awareness campaigns will be proposed to address identified gaps and promote safer online behaviours.

2.0 LITERATURE REVIEWS

Cybersecurity has emerged as a critical issue across various sectors, including education, where students and staff rely heavily on digital tools for communication, learning, and administration. The increasing integration of information and communication technology (ICT) in educational institutions has heightened the risks posed by cyber threats such as phishing, identity theft, and data breaches. This literature review synthesizes findings from multiple studies on cybersecurity awareness within educational settings to identify existing knowledge and pinpoint critical research gaps

Current research reveals a concerning trend that students often exhibit a mixed and sometimes inadequate level of cybersecurity awareness. A survey at Politeknik Mersing, for instance, found that students engage in risky behaviors such as opening emails from unknown senders and reusing passwords across multiple accounts (Badela, 2024). This is consistent with broader findings that college students often lack knowledge of cybersecurity risks, possess overconfidence in their online safety, and demonstrate a lack of accountability for their actions. These behaviors highlight the urgent need for comprehensive and practical awareness programs to mitigate risks and promote safe online practices.

However, the existing body of research suffers from two significant limitations. First, there is a scarcity of studies that specifically address the unique challenges faced by polytechnic students. Most research provides valuable but generalized insights, failing to adequately consider the distinctive behaviors and knowledge gaps of students in technical and vocational institutions. Consequently, recommendations are often too broad, such as simply "implementing more comprehensive educational programs" without offering the specificity required for this demographic. A more effective approach would involve targeted interventions, such as specialized workshops on phishing detection or hands-on training in multi-factor authentication (MFA).

A more effective approach would involve targeted interventions tailored to polytechnic learners. These include specialized workshops on phishing detection, hands-on training in multi-factor

authentication (MFA), and the integration of cybersecurity modules into ICT curricula. For example, Zukarnain et al. (2020) emphasized the effectiveness of cybersecurity training programs in improving student practices, especially when reinforced over time. Similarly, Kont (2024) suggests that interactive simulations and real-life threat scenario analysis could improve retention and application of cybersecurity knowledge.

Second, many studies do not sufficiently address emerging cyber threats. While there is growing recognition of the dynamic nature of cybersecurity, risks associated with ransomware and the vulnerabilities of Internet of Things (IoT) devices are often overlooked. These threats are particularly relevant to students, who frequently use a wide array of mobile and connected technologies. A forward-looking approach to cybersecurity education is necessary to prepare students for these evolving challenges.

Bottyan (2023) also highlights several challenges faced by college students regarding cybersecurity awareness, such as a lack of knowledge about cybersecurity risks, overconfidence in their online safety, and a lack of accountability for their online actions. He suggests the necessity of ongoing cybersecurity education, starting from primary school, to instill a culture of awareness and responsibility among students.

While the existing body of research on cybersecurity awareness in educational institutions is extensive, there is a paucity of studies that specifically address the unique challenges faced by students in polytechnics. For example, Ramakrishnan et al. (2022) and Badela et al. (2024) provide valuable insights into cybersecurity awareness among general student populations, but they do not adequately consider the demographic traits, technical backgrounds, and behavioral patterns of polytechnic students. Hence, it is imperative to conduct a more targeted study that considers these factors.

The reviewed studies often propose generalized solutions to improve cybersecurity awareness, such as enhancing password practices or delivering one-off awareness campaigns. However, these recommendations tend to lack specificity. More impactful strategies would include gamified cybersecurity modules, demographic-specific awareness campaigns, and collaborations with industry to develop certification-based cybersecurity programs. Studies by Garba et al. (2020) and Jia et al. (2023) reinforce the need to move beyond passive learning and into active, experiential learning models to bridge the theory-practice gap.

Although there is growing recognition of the dynamic nature of cybersecurity threats, many studies fail to adequately address emerging risks such as ransomware, or the vulnerabilities associated with IoT devices. These threats are particularly relevant to students, who frequently use mobile devices and other connected technologies (Zukarnain et al., 2020). A forward-looking approach to cybersecurity awareness is necessary to address both current and future challenges, ensuring that students are adequately prepared for evolving threats. This study aims to close this gap by focusing on polytechnic students' specific needs and behaviors and proposing targeted educational interventions.

3.0 METHODOLOGY

This study aimed to identify the level of cybersecurity awareness among students at Politeknik Mersing, Johor. A quantitative research design was adopted, using a descriptive survey approach to gather data related to students' knowledge, behaviours, and experiences in cybersecurity.

A convenience sampling technique was employed due to its practicality and efficiency in accessing the student population. According to administrative records, the total number of diploma-level students enrolled at Politeknik Mersing at the time of the study was approximately 720 students. A total of 62 students participated voluntarily in the survey. While this represents about 8.6% of the total population, it falls within the acceptable range for small-scale exploratory studies in educational research and provides preliminary insights into student cybersecurity awareness.

The data collection instrument was a web-based questionnaire distributed via widely used social media platforms, including WhatsApp and Telegram groups. The questionnaire was structured into three sections, as detailed in Table 1.

Table 1
Parts of the Questionnaire

No	Parts of Questions
1	Part I: Demographics
2	Part II: Cybersecurity Awareness Behaviour
3	Part III: Cybersecurity Incidents and Practices

The items in Part II and Part III were developed based on validated instruments from previous studies (e.g., Zukarnain et al., 2020; Saeed, 2023). Responses in Part II were measured using a five-point Likert scale, where 1 indicated "strongly disagree" and 5 indicated "strongly agree." Part III consisted of dichotomous "yes/no" items to capture actual incidents and risky behaviours.

To ensure the internal consistency and reliability of the instrument, a pilot test was conducted involving 15 students from a different cohort. The Cronbach's alpha coefficient for Part II of the questionnaire was calculated as 0.812, indicating a high level of reliability.

The data collected was analysed using the Statistical Package for Social Sciences (SPSS) version 26. Descriptive statistics, including frequency distributions, percentages, mean values, and standard deviations, were computed to summarize respondents' demographic characteristics, awareness behaviours, and cybersecurity experiences.

4.0 DATA ANALYSIS AND FINDINGS

4.1 Respondents' General Profiles

The demographic profile of the 62 respondents is summarized in Table 2. The sample comprised 52% female and 48% male students. The majority (90%) of participants were between 18 and 24 years old, while 8% were between 25 and 29, and 2% were aged 30 years or older. In terms of departmental distribution, most respondents (74%) belonged to the Jabatan Teknologi Maklumat & Komunikasi (JTMK), followed by the Jabatan Perdagangan (JP, 14%), and the Jabatan Kejuruteraan Elektrik (JKE, 12%). This demographic distribution allows for a relevant analysis of cybersecurity awareness, particularly among ICT students who are frequently exposed to digital environments.

Table 2
Respondents' Profiles

Respondents' background		Frequency	Percentage (%)
Gender			
	Male	48	48
	Female	52	52
Age			
	18-24years	90	90
	25-29 year	8	8
	30 years and above	2	2
Department			
	JTMK	74	74
	JKE	12	12
	JP	14	14

4.2 Cybersecurity Awareness Behaviour

Table 3 presents the descriptive statistics of students' cybersecurity awareness behaviours. The results indicate an overall high level of awareness (mean = 3.79, SD = 1.09). However, specific behaviours revealed varying levels of understanding and application.

Table 3
The Descriptive Analysis of Cybersecurity Awareness Behaviour

No	Item	Mean	SD	Interpretation
Q1	How often do you adjust your privacy settings on social media platforms to minimize the amount of publicly accessible personal information?	3.64	1.198	Moderate
Q2	How often do you update your email account settings for enhanced security?	3.58	1.153	Moderate
Q3	How often do you change your passwords for email and online accounts?	3.34	1.167	Moderate
Q4	It's wise to be cautious about what you share on social media.	4.44	.917	High
Q5	Are you aware that some of your data will be collected by websites and apps irrespective of your consent?	3.97	.991	High
	Total Average	**3.79**	**1.0852**	**High**

4.2.1 Privacy Settings on Social Media

The mean score of 3.64 with a standard deviation of 1.198 indicates that students moderately adjust their privacy settings on social media to minimize publicly accessible personal information. This moderate score suggests that while students are somewhat conscious of their privacy on social platforms, there is still room for improvement in ensuring that their personal information is better protected.

4.2.2 Email Account Security

For email security, the mean score of 3.58, with a standard deviation of 1.153, also falls under the "Moderate" category. This implies that students sometimes update their email account settings to enhance security, but not consistently enough. Although students are somewhat cautious, they do not consistently update email security settings, leaving accounts potentially vulnerable.

4.2.3 Password Change Frequency

The question about password changes for email and online accounts reveals a mean of 3.34 and a standard deviation of 1.167, also interpreted as "Moderate." This moderate score demonstrated the lowest mean score, emphasizing significant vulnerability and highlighting a critical area requiring improvement through targeted interventions.

4.2.4 Caution with Social Media Sharing

With a mean score of 4.44 and a lower standard deviation of 0.917, the interpretation for this behaviour is "High." Students exhibit a greater degree of caution when it comes to sharing personal information on social media platforms. It's shown that they were generally aware and cautious about oversharing personal information online, reflecting effective awareness campaigns around privacy and online identity protection.

4.2.5 Awareness of Data Collection

The mean score of 3.97 (SD = 0.991) indicates that students demonstrate a strong awareness of the risks associated with online data collection. This suggests that most students are conscious of how websites and applications may gather personal information, often without explicit consent. To strengthen this awareness, it is recommended that educational institutions integrate modules on data privacy laws, such as the Personal Data Protection Act (PDPA) and digital ethics into relevant courses.

Although the overall awareness score of 3.79 is encouraging, inconsistencies in students' cybersecurity practices, particularly in areas such as email and password management, underscore the need for continuous reinforcement through structured training and regular engagement.

4.3 Cybersecurity Incidents and Practices

Table 4 summarizes students' experiences with cybersecurity threats and their online behaviours.

Table 4
The Descriptive Analysis of Cybersecurity Incidents and Practices

Item	Cybersecurity incidents and practices	Frequency		Percentage %	
		Yes	No	Yes	No
Q6	Have you ever experienced a cybersecurity incident or breach related to email security?	27	35	43.5	56.5
Q7	Have you ever received suspicious emails requesting personal or sensitive information?	34	28	54.8	45.2
Q8	Do you understand the meaning of common cybersecurity terms such as phishing, malware, and encryption?	55	7	88.7	11.3
Q9	Have you ever used free Wi-Fi without considering potential security risks?	33	29	53.2	46.8
Q10	Do you have a password that you use for more than one device?	51	11	82.3	17.7

The data shows that 27 students, approximately 43% of the sample, have experienced a cybersecurity incident or breach related to email security. However, the majority (35 students or 57%) have not faced such issues. This suggests that while a significant portion of students are at risk of email-related security breaches, the overall number is still relatively moderate. The finding aligns with the broader literature, which shows that email remains a common vector for cybersecurity attacks, particularly phishing attempts (Alharbi & Tassaddiq, 2021). Therefore, these results indicate a need for continued vigilance and education on secure email practices to prevent incidents from escalating.

When asked if they had received suspicious emails requesting personal or sensitive information, 55% (34 students) reported encountering such phishing attempts. This highlights a critical issue, as phishing is one of the most widespread cybersecurity threats, especially in educational settings where students may be less vigilant. This result supports prior studies that have documented high levels of phishing attacks targeting young internet users (Saeed, 2023). The fact that more than half of the respondents have encountered these emails underscores the necessity for improved awareness and preventive measures, including training on how to recognize and avoid phishing scams.

On a more positive note, most students (88%) reported understanding common cybersecurity terms such as phishing, malware, and encryption. This is an encouraging result, as it suggests that students possess a foundational knowledge of cybersecurity concepts. Prior research has emphasized the importance of theoretical knowledge in promoting safer online behaviours (Bottyan, 2023). However, while this awareness is a positive sign, knowledge alone may not translate into secure practices, as evidenced by risky behaviours noted in other aspects of the study.

The responses to this question reveal a significant division among students regarding their use of free Wi-Fi. About 53% admitted to using unsecured Wi-Fi networks without considering potential risks, while 47% indicated that they exercise caution in such situations. The use of unsecured Wi-Fi networks presents substantial cybersecurity risks, as attackers can easily intercept data over these networks (Kumar et al., 2024). These findings suggest a need for greater education on the dangers associated with free Wi-Fi use, particularly in public spaces, and highlight an area where theoretical knowledge may not always lead to secure practices.

One of the most concerning findings is that 82% of respondents reuse passwords across multiple devices. This is a risky practice that significantly increases vulnerability to cyberattacks, as a compromised password on one platform could lead to breaches across other accounts. This behaviour points to a gap between students' cybersecurity knowledge and their actual practices, reinforcing the importance of practical cybersecurity education (Yuliana, 2022). Students must be encouraged to adopt stronger password habits, such as using unique passwords for different accounts and enabling two-factor authentication, to reduce their susceptibility to attacks.

5.0 DISCUSSION AND CONCLUSIONS

This study reveals that students at Politeknik Mersing exhibit a moderate to high level of cybersecurity awareness, particularly in terms of understanding social media privacy, data collection, and basic cybersecurity terminology. However, several critical gaps in behaviour were identified, especially in password practices, email security management, and the use of unsecured Wi-Fi.

A significant portion of students (82.3%) reported reusing passwords across devices, and 53.2% used public Wi-Fi without considering security risks. Moreover, over 54% had received phishing emails, yet fewer demonstrated effective action to avoid such threats. These findings reinforce what has been highlighted in the literature: students may understand cybersecurity in theory but fail to consistently apply secure practices (Zukarnain et al., 2020; Saeed, 2023).

Given that most participants were from the ICT department, tailored strategies should leverage their technical background. For example, ICT students can be engaged in peer-led training, hands-on simulations like phishing recognition challenges, and integration of advanced security tools such as password managers or MFA apps. While for non-ICT students, particularly from the Commerce or Engineering department, they should receive simplified scenario-based training to boost practical awareness without assuming prior technical knowledge.

Furthermore, younger students (18–24 years) who formed much of the sample may be more responsive to interactive and gamified learning formats, such as mobile app-based quizzes or cybersecurity escape rooms. Considering these insights, the following recommendations are proposed to improve cybersecurity practices among students:

i. Cybersecurity Awareness Campaigns – Periodic workshops covering password hygiene, phishing identification, and safe browsing habits.
ii. Curriculum Integration – Embed cybersecurity education into ICT and general studies syllabi through assignments and collaborative activities.
iii. Email & Wi-Fi Security Training – Use real case studies to train students in secure email usage and VPN adoption when accessing free Wi-Fi.
iv. Simulations and Drills – Run simulated phishing attacks and role-based scenarios to test student reactions and provide immediate feedback.
v. Use of Peer Mentors – Appoint trained student ambassadors to promote cybersecurity practices among their peers, especially within their departments.

In conclusion, while Politeknik Mersing students generally possess a theoretical understanding of cybersecurity, a disconnect remains between awareness and consistent application. Addressing this gap requires targeted, practical, and engaging interventions that reflect students' digital behaviours and demographic profiles. By prioritizing and recurring cybersecurity education, institutions can better prepare students to navigate the digital environment securely and responsibly.

REFERENCES

Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. Big Data and Cognitive Computing, 5(2), 23. https://doi.org/10.3390/bdcc5020023

Badela, N. A., Ariff, M. A. M., & Pazui, P. (2024). Cybersecurity Knowledge and Practices: A Survey of Students and Staff at Politeknik Mersing.

Bottyan, L. (2023). Cybersecurity Awareness among University Students. Journal of Applied Technical and Educational Sciences, 13(3), ArtNo: 363.

Chugh, R., Grose, R., & Macht, S. A. (2021). Social media usage by higher education academics: A scoping review of the literature. Education and information technologies, 26(1), 983-999.

Jia, Y., Qi, H., Shang, R., Jiang, A., & Li, Y. (2023). Cybersecurity Awareness in University Students: A Systematic Review of the Literature. SpringerLink.

Kont, K. R. (2024). Libraries and cyber security: the importance of the human factor in preventing cyber attacks. Library Hi Tech News, 41(1), 11-15.

Kumar, R., Yuliana, N., Berry, T., & Zukarnain, S. (2024). Cybersecurity awareness and youth: Facing the growing threat. Publisher (if available).

Saeed, S. (2023). Education, Online presence and Cybersecurity Implications: A study of information security practices of computing students in Saudi Arabia. Sustainability, 15(12), 9426. https://doi.org/10.3390/su15129426

Triplett, W. J. (2023). Addressing cybersecurity challenges in education. International Journal of STEM Education for Sustainability, 3(1), 47-67.

Yuliana, N. (2022). Cyber risks and online schooling: The vulnerability of children

Zukarnain, Z., Zazira, M., Muhammad, N., Mansor, F., Hazimah, W., Azib, W., Teknologi, U., Kelantan, M., Ilmu, B., & Malaysia, K. (2020). IMPACT OF TRAINING ON CYBERSECURITY AWARENESS. GADING Journal of Science and Technology, 3(1). https://ir.uitm.edu.my/id/eprint/31118/1/31118.pdf