ECOSIA | International Conference
Institut Teknologi dan Bisnis Asia Malang
Indonesia, 10 December 2025

Cybersecurity Challenges in Internet Usage by Engineering Students

Ahmady bin Solong[1]
Muliadi bin Wahid[1]
[1]Affiliation: Politeknik Kuching Sarawak, Sarawak, Malaysia
Email Correspondence: ahmadysolong@gmail.com

Abstract

Introduction/Main Objectives: The internet has become an indispensable resource for engineering students, supporting their academic and daily activities. However, the increasing reliance on online platforms raises concerns about cybersecurity awareness among students. This study aims to examine the level of cybersecurity knowledge and practices among engineering students, highlighting the importance of safeguarding personal and institutional data.

Background Problems: Despite the widespread use of the internet, it remains unclear to what extent engineering students prioritize cybersecurity in their online activities. Therefore, the research question addressed in this study is: What is the level of cybersecurity knowledge and practices among engineering students?

Research Methods: The study was conducted among diploma-level engineering students at Politeknik Kuching Sarawak. Data were collected using a structured questionnaire distributed online through random sampling. Respondents rated their agreement with the items on a 5-point Likert scale. Descriptive analysis was employed to determine the mean scores, which reflect the students' level of knowledge and practices.

Finding/Results: The findings indicate that students possess a high level of cybersecurity knowledge and demonstrate good practical cybersecurity practices. These results suggest that students are generally aware of the importance of cybersecurity in their academic and personal online activities.

Conclusion: This study concludes that while the current level of awareness and practice is satisfactory, continuous efforts are necessary to maintain and enhance cybersecurity consciousness among students. Institutions should implement targeted programs and training to strengthen students' understanding and application of cybersecurity measures, ensuring a safer digital environment.

Keywords: Cyber knowledge, security practice, engineering student

Introduction

The internet has become the backbone of modern education, supporting students throughout their academic journey. It plays a crucial role in accessing vast online learning resources, engaging in collaborative projects, participating in virtual learning environments, and connecting with peers globally. With the rapid advancement of technology, internet usage has grown exponentially, serving diverse purposes such as e-commerce, online learning, and social interaction. However, alongside these opportunities, the internet also exposes users to significant cybersecurity risks. According to the Cybersecurity Guide (2025), the increasing integration of the internet into daily life creates a complex network of security vulnerabilities that require users, particularly students, to adopt safe online practices.

Engineering students represent one of the most intensive user groups of internet technologies. Their academic tasks often demand access to digital resources, specialized software, and online communication platforms. For instance, design projects require students to search for component specifications, download simulation tools and data sheets from manufacturer websites, and collaborate virtually on complex calculations and modeling. These activities, while essential for academic success, increase exposure to potential cyber threats. Therefore, understanding the level of cybersecurity knowledge and practices among engineering students is critical to mitigating risks and ensuring safe digital engagement.

Existing literature highlights the growing concern over cybersecurity awareness among students. Cybersecurity encompasses strategies and technologies designed to prevent unauthorized access, data breaches, and cyberattacks (Diana et al., 2023). Despite widespread internet use, studies reveal gaps in cybersecurity practices among students. For example, Ismail et al. (2024) found that while students at Politeknik Tuanku Syed Sirajuddin (PTSS) avoid suspicious emails and protect personal information, many still rely on weak passwords and unsafe behaviors. Similarly, Pitchan et al. (2019) emphasized that good cybersecurity practices significantly reduce cybercrime risks. Higher education students are frequent targets of cybercriminals due to their heavy reliance on technology (Shahjahan & Durani, 2024). Furthermore, research in Selangor indicates low cybersecurity literacy among youth, underscoring the need for enhanced awareness programs and protective measures (Oskar & Hed, 2023). These findings reveal a critical gap in understanding cybersecurity awareness among engineering students, warranting further investigation.

Based on this context, the present study aims to identify the level of cybersecurity knowledge and practices among engineering students at Politeknik Kuching Sarawak. This research is important for determining the extent to which students are aware of cybersecurity aspects and for providing insights that can guide institutional actions to develop programs that enhance their level of awareness. Cybersecurity refers to the methods and technologies used to prevent unauthorized access, use, disclosure, disruption, modification, or destruction of computer systems, networks, and sensitive information from cyberattacks. Cyberattacks are among the most severe issues faced by today's rapidly changing technology. Individuals skilled in cybersecurity can identify, respond to, and limit the impact of cyber threats on themselves. However, reports indicate that even those with expertise in cybersecurity can fall victim to attacks, suggesting that individual characteristics and behaviors play a significant role (Diana et al., 2023). Ismail et al. (2024) examined internet usage patterns and cybersecurity knowledge among students at PTSS and found that students frequently use the internet, primarily through mobile data. While many students exercise caution by avoiding suspicious emails and protecting personal information, some continue to use weak passwords and engage in unsafe practices. Pitchan et al. (2019) stressed that adopting good cybersecurity practices can significantly reduce the risk of cybercrime. Shahjahan and Durani (2024) further noted that students in higher education institutions are prime targets for cybercriminals due to their intensive use of technology and the internet. Additionally, Oskar and Hed (2023) reported low levels of cybersecurity literacy among youth in Selangor, highlighting the need for improved cyber surveillance and filtering mechanisms to protect users. Collectively, these studies underscore the importance of enhancing cybersecurity awareness and practices among students, particularly those in engineering disciplines who rely heavily on digital tools and resources.

Research Methods

This study employed a quantitative research design to assess the level of cybersecurity knowledge and practices among engineering students. The population consisted of diploma-level engineering students at Politeknik Kuching Sarawak. Data collection was conducted using a structured questionnaire as the primary research instrument. The questionnaire items were self-developed based on the study objectives and subsequently reviewed by subject-matter experts, including lecturers actively engaged in academic writing. Furthermore, the instrument was validated by the Research, Innovation, and Commercialization Unit (UPIK) at Politeknik Kuching Sarawak to ensure content validity.

Reliability testing was performed using Cronbach’s alpha, yielding values of 0.891 for the knowledge construct (5 items) and 0.794 for the practice construct (13 items). These values indicate a high level of internal consistency, confirming that the instrument is reliable for research purposes. The questionnaire utilized a 5-point Likert scale ranging from “Strongly Disagree” (1) to “Strongly Agree” (5), enabling respondents to express their level of agreement with each item.

The sampling technique applied was simple random sampling, and the questionnaire was distributed online to facilitate accessibility. Respondents completed the survey voluntarily within a specified timeframe. Data analysis was conducted using descriptive statistics to calculate mean scores for each item. The interpretation of mean values followed the scale proposed by Ngadiman et al. (2019): 1.00–1.99 (Weak), 2.00–2.99 (Low), 3.00–3.99 (Moderate), and 4.00–5.00 (High). This systematic approach ensures that the methodology can be replicated by other researchers under similar conditions.

Result

The respondents’ demographic profile provides important context for interpreting the study findings. A total of 114 engineering students participated, with a significant majority being male (78.1%) and the remaining 21.9% female. The largest proportion of respondents were enrolled in the Diploma in Electrical & Electronic Engineering program (52.6%), followed by the Diploma in Mechanical Engineering (23.7%). Other programs, such as Civil Engineering and specialized mechanical engineering tracks, accounted for smaller percentages. Most respondents were in semesters three and four, representing the second year of study, which suggests they have substantial exposure to academic requirements involving technology. In terms of academic performance, the majority achieved a high Cumulative Grade Point Average (CGPA) between 3.01 and 4.00 (64.9%), indicating strong academic achievement among participants.

Internet usage patterns among respondents reveal their heavy reliance on digital resources for academic purposes. A considerable proportion of students reported frequent internet use, with 34.2% spending more than six hours per day online for academic activities. Another 35.1% used the internet for two to four hours daily, while a smaller group reported less than two hours of usage. These findings highlight the central role of internet connectivity in engineering education, where students depend on online platforms for accessing learning materials, downloading software, and collaborating on projects. Such extensive usage underscores the importance of cybersecurity awareness, as prolonged exposure to online environments increases vulnerability to cyber threats.

The analysis of cybersecurity knowledge among engineering students at Politeknik Kuching Sarawak demonstrates a high overall level of awareness. Students exhibited strong understanding of key concepts, including the importance of updating software and operating systems immediately, which recorded the highest mean score (4.28). Knowledge of risks associated with public Wi-Fi usage ranked second (Mean = 4.27), followed by awareness of steps to protect Internet of Things (IoT) devices and familiarity with phishing detection techniques (Mean = 4.12). Respondents also showed competence in distinguishing between viruses, malware, and ransomware, as well as understanding Two-Factor Authentication (2FA). These results indicate that students possess substantial theoretical knowledge of cybersecurity threats and preventive measures.

In terms of practical application, students generally demonstrated good cybersecurity practices, although some gaps remain. The most consistently practiced behavior was the use of unique and complex passwords for important accounts such as email, banking, and university portals (Mean = 4.18). Students also reported regularly checking URLs and email sender validity before clicking links or downloading files (Mean = 4.14) and deactivating Bluetooth or Wi-Fi when not in use (Mean = 4.11). These habits reflect a proactive approach to safeguarding personal and academic data. However, certain practices were less prevalent, such as using licensed antivirus software (Mean = 3.96) and employing VPNs when accessing public Wi-Fi networks (Mean = 3.48), suggesting areas where improvement is needed.

Negative behaviors identified in the study highlight potential vulnerabilities among students. Some respondents admitted to ignoring security practices, such as using simple passwords, for the sake of academic convenience (Mean = 2.98). Others reported sharing sensitive information online despite being aware of the risks (Mean = 2.74). Additional challenges include uncertainty about university cybersecurity policies (Mean = 3.13) and lack of knowledge on reporting cybersecurity incidents (Mean = 3.13). Financial constraints also emerged as a barrier, with students citing the cost of security software as a limitation to optimal cybersecurity practices (Mean = 3.54). These findings indicate that while students are knowledgeable and generally cautious, practical limitations and behavioral tendencies can compromise their overall security posture.

Overall, the results suggest that engineering students at Politeknik Kuching Sarawak possess high cybersecurity knowledge and exhibit good practices, but there are notable gaps that require attention. The combination of strong theoretical understanding and moderate practical implementation underscores the need for targeted interventions. Institutions should consider implementing structured awareness programs, providing affordable access to security tools, and establishing clear reporting mechanisms for cybersecurity incidents. By addressing these areas, educational institutions can enhance students' ability to protect themselves against evolving cyber threats, ensuring a safer and more secure digital learning environment.

Discussion

The findings of this study reveal that engineering students at Politeknik Kuching Sarawak possess a high level of cybersecurity knowledge and demonstrate generally good cybersecurity practices. This outcome aligns with previous research by Ismail et al. (2024), which reported that students in higher education institutions exhibit awareness of basic cybersecurity principles. The high mean scores for knowledge items, such as understanding the importance of software updates and recognizing risks associated with public Wi-Fi, indicate that students are well-informed about common threats and preventive measures. This suggests that exposure to technology and academic requirements may contribute to their familiarity with cybersecurity concepts.

Despite strong theoretical knowledge, the practical implementation of cybersecurity measures shows variability. While students consistently apply certain best practices, such as using complex passwords and verifying URLs, other behaviors—such as using VPNs and licensed antivirus software—are less prevalent. This gap between knowledge and practice reflects findings by Pitchan et al. (2019), who emphasized that awareness alone does not guarantee compliance with security protocols. Factors such as convenience, cost, and time constraints appear to influence students' decisions, as indicated by responses highlighting financial barriers and the tendency to ignore security measures for academic efficiency.

The presence of negative behaviors, including sharing sensitive information online and uncertainty about reporting procedures, raises concerns about institutional support and policy communication. These issues suggest that while students are individually proactive, systemic factors such as lack of clear guidelines and accessible resources may hinder optimal cybersecurity practices. Similar observations were made by Oskar and Hed (2023), who noted that low literacy and unclear institutional frameworks contribute to vulnerabilities among youth.

Overall, the discussion underscores the need for a holistic approach to cybersecurity education. Institutions should not only provide theoretical knowledge but also facilitate practical implementation through affordable tools, structured training, and clear reporting mechanisms. By bridging the gap between awareness and action, educational institutions can strengthen students' resilience against cyber threats and foster a culture of digital safety.

Conclusion

This study was conducted to assess the extent to which engineering students are aware of cybersecurity issues, especially given their high dependence on the internet for academic purposes. The quantitative study conducted at Politeknik Kuching Sarawak found that students overall have high knowledge of cybersecurity, particularly about the importance of updating software (mean 4.28) and the dangers of public Wi-Fi (mean 4.27). Furthermore, cybersecurity techniques are rated well, with a high tendency to use unique and complex passwords (mean 4.18) and caution in checking URLs before clicking. However, the key finding shows a gap in practice as students were found to have a Low tendency to ignore security practices (Mean=2.98) or share sensitive information (Mean=2.74) for the sake of fulfilling project demands and academic efficiency. In addition, the practice of using a VPN (Mean=3.48) is still at a Moderate level. This study indicates that institutions need to implement more specific actions to raise public awareness about security. They also need to provide practical training to address the conflict between security protocols and academic needs, as well as strengthen the use of VPNs and clear guidelines for handling sensitive data.

References

Cybersecurity Guide. (2025, April 21). Student Internet Safety Resource Kit. https://cybersecurityguide.org/resources/internet-safety/

Ngadiman, D. W. T., Yacoob, S. E., & Wahid, H. (2019). Tahap Harga Diri Kumpulan Berpendapatan Rendah yang Berhutang dan Peranan Organisasi dalam Sektor Perladangan. Melayu: Jurnal Antarabangsa Dunia Melayu, 12(2), 238-254

Ismail, N. N. S., Norizan, T. T., & Hashim, N. L. (2024). Internet Usage and Cybersecurity Awareness Among Students at Politeknik Tuanku Syed Sirajuddin. Politeknik & Kolej Komuniti Journal of Social Sciences and Humanities, 9(1), 45-57.

Diana, I., Ismail, I. A., & Zairul, M. (2023). Cybersecurity Issues among High School Students: A Thematic Review. International Journal of Academic Research in Business and Social.

Oskar, A., & Hed, N. M. (2023). Literasi dan Kesedaran Belia Selangor terhadap Pengawasan dan Penapisan Siber Kerajaan. Perspektif Jurnal Sains Sosial dan Kemanusiaan, 15, 1-15.

Pitchan, M. and Omar, S. (2019). Dasar keselamatan siber malaysia: tinjauan terhadap kesedaran netizen dan undang-undang (cyber security policy: review on netizen awareness and laws). Jurnal Komunikasi Malaysian Journal of Communication, 35(1), 103-119. https://doi.org/10.17576/jkmjc-2019-3501-08

Pitchan, M., Omar, S., & Ghazali, A. (2019). Amalan keselamatan siber pengguna internet terhadap buli siber, pornografi, e-mel phishing dan pembelian dalam talian (cyber security practice among internet users towards cyberbullying, pornography, phishing email and online shopping). Jurnal Komunikasi Malaysian Journal of Communication, 35(3), 212-227. https://doi.org/10.17576/jkmjc-2019-3503-13

Shahjahan, M. and Durani, N. (2024). Sikap terhadap keselamatan siber: kajian terhadap pelajar institusi pengajian tinggi. DiJITAC, 1-10. https://doi.org/10.21093/dijitac.v4i2.8284