JOURNAL OF MANAGEMENT & INFORMATION TECHNOLOGY RESEARCH
AL-SULTAN ABDULLAH AHMAD SHAH QURANIC UNIVERSITY OF PAHANG

Vol. 01 No. 01 (2025)
e-ISSN: 3141-1371
https://ejournal.unipsaas.edu.my/

EXPLORING FACTORS INFLUENCING CYBERSECURITY AWARENESS AMONG MALAYSIAN UNIVERSITY STUDENTS

Zuraini Mohamad @ Abdul Rahman[1], Mohd Fazzly Rassis Md. Kasim[1], Zarina Kamarozaman[1], Wan Hashridz Rizal Wan Abu Bakar[2]

[1]Faculty of Management and Informatics, [2]Faculty of Islamic Studies,
Al-Sultan Abdullah Ahmad Shah Quranic University of Pahang (UNIQSAAS)

Abstract

Cybersecurity awareness has become a critical concern among university students, given their extensive use of digital technologies for both academic and social purposes. This study aims to explore the level of cybersecurity awareness among Malaysian university students and to examine the relationships between Password Security, Web Browser Security, Social Media Activities, and cybersecurity awareness. A quantitative research design was employed using an online questionnaire distributed to university students across Malaysia. The online survey approach enabled efficient data collection within a limited timeframe, resulting in 142 valid responses for analysis. Descriptive analysis revealed a high overall level of cybersecurity awareness, with a mean score of 4.656. Hypothesis testing revealed a positive and significant relationship between Web Browser Security and cybersecurity awareness (t = 2.302), whereas Password Security did not demonstrate a significant relationship (t = 1.574). Interestingly, Social Media Activities exhibited a significant negative relationship with cybersecurity awareness (t = -6.387). These findings suggest that while students demonstrate high awareness overall, certain cybersecurity practices, particularly related to passwords and social media behavior, require further attention. The study provides valuable insights for universities and policymakers in designing targeted cybersecurity awareness programs.

Keywords: Cybersecurity Awareness, Web Browser Security, Password Security, Social Media Activities

Perkembangan Artikel

Diterima: 16/12/2025
Disemak: 24/12/2025
Diterbit: 31/12/2025

*Corresponding Author:
Zuraini Mohamad @ Abdul Rahman, Faculty of Management and Informatics, Al-Sultan Abdullah Ahmad Shah Quranic University of Pahang (UNIQSAAS).
Email:zuraini@uniqsaas.edu.my

INTRODUCTION

In the digital era, cybersecurity has emerged as a fundamental pillar of modern society. Insufficient cybersecurity awareness not only exposes individuals to escalating digital threats but also undermines organizational resilience and poses serious implications for national security and economic stability.

Educational institutions in Malaysia are increasingly confronted with a wide range of cybersecurity challenges. Students frequently rely on information and communication technologies (ICT) for learning, communication, and daily activities, which heightens their exposure to cyber threats. Consequently, numerous studies have been conducted to examine the level of understanding and awareness of cybersecurity issues among students in Malaysia, encompassing primary schools, secondary schools, and higher education institutions.

According to studies by Xiang & Hasbullah (2023), Hamzaha et al. (2021), and Kamalulail et al. (2022), university students demonstrate a low level of cybersecurity awareness. With the advent of Industry 4.0, cybercrime has been escalating and has emerged as a major challenge to digital security (Johari et al., 2022). Studies conducted by Zwilling et al. (2022) and Zulkifli (2020) show that internet users have an adequate understanding of cyber threats, but typically implement only basic and common protective measures. Therefore, the government plays a crucial role in establishing regulations and policies to ensure secure cybersecurity management (Daud & Rasiah, 2023). Meanwhile, initiatives such as the adoption of cyber insurance in organizations are also being implemented for cyber risk management (Abd Rahman et al., 2022).

Public universities in Malaysia are also actively addressing the growing threats by focusing on cybersecurity risk management frameworks (Dioubate et al., 2022). In general, Malaysia is actively strengthening its cybersecurity measures through policy development, awareness campaigns, risk mitigation strategies, and technological advancements to protect against cyber threats and ensure a secure digital environment.

This study is conducted to identify the level of cybersecurity awareness among Malaysian students and to understand the factors influencing it. Based on the study by Alqahtani (2022), this research also focuses on examining the relationship between password security practices, web browser security, and social media activities with cybersecurity awareness among students in Malaysian higher education institutions.

Understanding this issue is essential for designing more effective educational strategies and interventions to enhance protection against cyber threats and to foster a secure digital culture.

OBJECTIVES

The objectives of the study are as follows:

i. To identify the level of cybersecurity awareness among university students.
ii. To determine the relationship between Password Security and Cybersecurity Awareness
iii. To determine the relationship between Web Browser Security and Cybersecurity Awareness
iv. To determine the relationship between Social Media Activities and Cybersecurity Awareness

LITERATURE REVIEW

Cybersecurity Awareness

Cybersecurity awareness encompasses the awareness, understanding, and knowledge of cyber risks and the appropriate protective strategies (Nurse, 2021). Cybersecurity relates to the deployment of safeguards for devices, networks, and online information to block unauthorized access while maintaining data confidentiality, integrity, and availability (Seemma et al., 2018). A comprehensive understanding of cybersecurity is essential for safeguarding against threats such as phishing, malware, and data breaches or manipulation.

Password Security

Password security refers to the practices, policies, and technologies applied to the creation, management, and protection of passwords. Ensuring password security is one of the methods that can be employed to maintain cybersecurity (Gallus et al., 2025). The implementation of technologies such as blockchain-based two-factor authentication (2FA) can enhance security by adding a layer of verification (McCabe et al., 2024). Graphical Password Authentication methods also serve as an additional layer of verification that strengthens authentication systems and helps reduce security risks (Chuen et al., 2020). Based on this, it can be inferred that students who practice strong password security are more likely to demonstrate higher levels of cybersecurity awareness.

Web Browsers Security

Web browsers serve as the main gateway to the internet, positioning them as a crucial interface between users and potential online threats (Kaushik et al., 2021). Browsers commonly include built-in security features, such as pop-up blockers (G. Shipkovenski, T. Kalushkov, E. Petkov, n.d.), warnings for unsafe websites (Kraus et al., 2020), as well as tools that allow users to manage cookies (O. Kulyk, P. Mayer, 2018). Users need to understand the security aspects of using web browsers because an insufficient understanding makes them more prone to cyber attacks. This indicates a positive relationship between web browser security and cybersecurity awareness

Social Media Activities

Social media has become an integral part of daily life, providing avenues for communication, information sharing, and entertainment. However, engaging in these platforms also exposes users to various cybersecurity threats, highlighting the importance of cyber awareness for safe and responsible online behavior. This highlights the occurrence of critical cybersecurity risks within social media activities (Khidzir et al., 2016). This suggests that engagement in social media activities positively correlates with cybersecurity awareness.

The following hypotheses are proposed:

H_1 Password Security will be positively related to cybersecurity awareness.
H_2 Web Browser Security will be positively correlated with cybersecurity awareness.
H_3 Social Media Activities will be positively related to cybersecurity awareness.

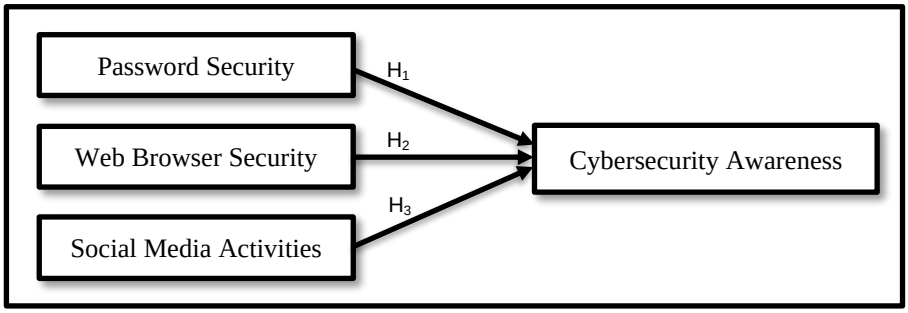

Figure 1: Research Conceptual Framework adapted from Alqahtani (2022)

METHODOLOGY

The questionnaire was adapted from the instrument developed by Alqahtani (2022) to assess cybersecurity awareness among university students. A pre-testing process involving five respondents with comparable demographic characteristics was conducted to ensure consistent interpretation of the questionnaire items. Based on the feedback received, minor revisions were made to enhance item clarity and formatting. A quantitative approach is suitable for this study, as it allows for the statistical analysis of cybersecurity awareness levels through descriptive statistics and the determination of relationships between variables. Data were collected through an online questionnaire distributed to university students across Malaysia. The online survey method was chosen due to its efficiency in reaching a wider population and its suitability for collecting standardized responses. The survey was administered using Google Forms as the data collection tool, allowing respondents to complete the questionnaire electronically. This approach minimized the risk of data entry errors and enhanced the accuracy and reliability of the collected data. A total of 142 valid responses were obtained and used for data analysis. The questionnaire consisted of structured items measuring password security practices, web browser security behavior, social media activity, and cybersecurity awareness. All items were assessed using a 5-point Likert scale, ranging from 1, representing Strongly Disagree with the stated items, while a score of 2, indicating disagreement. A score of 3 reflects a neutral position. Conversely, a score of 4 denotes agreement, and the highest score of 5 signifies strong agreement or endorsement of the statements presented. Non-probability sampling was used because an appropriate sampling frame was unavailable. Respondent demographic variables, specifically gender, race, age, educational level, enrollment status,

IPT category, and institutional regional location, were recorded.

FINDINGS AND DISCUSSIONS

The demographic data of the 142 university students involved in the study are shown in Table 1.

Table 1: Respondent demographic background.

Variables		n	%
Gender	Female	93	65.5%
	Male	49	34.5%
Race	Malay	137	96.5%
	Others	5	3.5%
Age	18-24	122	85.9%
	25-34	12	8.5%
	35-44	5	3.5%
	45-54	3	2.1%
Educational Level	Doctor of Philosophy (PhD)	1	0.7%
	Master's degree	7	4.9%
	Bachelor's degree	57	40.1%
	Diploma	64	45.1%
	Foundation	13	9.2%
Enrollment Status	Full-time	132	93%
	Part-time	10	7%
IPT Category	IPTA	99	69.7%
	IPTS	43	30.3%
Institutional Regional Location	East Coast (Pahang, Terengganu, Kelantan)	90	63.4%
	Northern (Perlis, Kedah, Pulau Pinang, Perak	16	11.3%
	Central (Kuala Lumpur, Putrajaya, Selangor)	23	16.2%
	Southern (Negeri Sembilan, Melaka, Johor)	11	7.7%
	East Malaysia (Sabah, Sarawak, Labuan)	2	1.4%

The collected data were analyzed using IBM SPSS Statistics version 26 (IBM Corp., 2017). The reliability of the measurement items was assessed using Cronbach's alpha value above 0.70, reflecting reliable internal consistency among the items in the scale. Descriptive statistics were

employed to determine the level of cybersecurity awareness among the respondents. Multiple regression analysis was then conducted to examine the influence of Password Security, Web Browser Security, and Social Media Activities on cybersecurity awareness. The results of the hypothesis testing based on the t-values from the multiple regression analysis are presented in Table 2.

Table 2: Results of Hypothesis Testing Using Multiple Regression Analysis

Variable	T value	Remarks	R Square
Password Security	1.574	Not Supported	26.4%
Web Browser Security	2.302	Supported	
Social Media Activities	-6.387	Not Supported	

The overall mean score for this study was 4.656, which indicates a high level of cybersecurity awareness among university students in Malaysia. This result addresses the first research objective of the study, which posits that Malaysian university students demonstrate a high level of cybersecurity awareness. The finding implies that, in general, respondents have a satisfactory understanding of cybersecurity in the context of digital technology usage. This finding is consistent with the results of Zulkifli (2020), even though many users do not actively implement online security measures.

The results of hypothesis testing indicate that H_1 was not supported, as Password Security recorded a t-value of 1.574, contributing to 26.4% of the variance in cybersecurity awareness. The analysis reveals that while password management is a common practice among students, it lacks the robustness necessary to impact or differentiate their overall cybersecurity awareness significantly. These results diverge from the findings of Alqahtani (2022), the password security variable significantly affects cybersecurity awareness.

Web Browser Security (t-value = 2.302) was found to significantly support the hypothesis H_2. Research by Razaque et al. (2021) demonstrates a positive relationship between Web Browser Security and Cybersecurity Awareness, showing that the proposed Web-Based Blockchain-Enabled Cybersecurity Awareness (WBCA) system successfully improves users' knowledge and competencies in addressing cybersecurity threats. Additionally, the study by van Oorschot & van Oorschot (2021) emphasizes that understanding the risks involved in browser–server interactions underscores the positive relationship between Web Browser Security and Cybersecurity Awareness. Similarly, Alqahtani (2022) found that Web Browser Security is positively associated with Cybersecurity Awareness.

In contrast, the results of Social Media Activities demonstrate a significant negative relationship with cybersecurity awareness (t = -6.387), which contradicts the proposed hypothesis H_3. This suggests that frequent engagement in social media activities may expose students to risky online behaviors, such as oversharing personal information, clicking on suspicious links, or neglecting to set privacy settings, which in turn lowers their cybersecurity awareness.

This may be due to students' enthusiasm for using social media without adequately considering cybersecurity aspects. This issue has also been discussed by Potgieter (2019), who highlighted a lack of student engagement in cybersecurity awareness programs.

CONCLUSION

This study examined the level of cybersecurity awareness among Malaysian university students and analyzed the relationships between Password Security, Web Browser Security, Social Media Activities, and cybersecurity awareness. The findings indicate that the overall level of cybersecurity awareness among students is high, reflecting their general understanding of cyber risks in the digital environment. The results further reveal that Web Browser Security has a significant positive relationship with cybersecurity awareness, highlighting the importance of safe browsing practices in enhancing students' cyber vigilance. However, Password Security was found to have no significant relationship with cybersecurity awareness, suggesting a possible gap between students' knowledge and their actual password management practices. Notably, Social Media Activities demonstrated a significant negative relationship with cybersecurity awareness, indicating that increased engagement on social media platforms may expose students to higher cybersecurity risks or lead to complacent security behaviors.

Based on the findings, this study recommends that higher education institutions strengthen cybersecurity education by focusing on practical and behavior-oriented training rather than solely theoretical knowledge. Universities are encouraged to establish strategic collaborations with Malaysian agencies responsible for cybersecurity, such as CyberSecurity Malaysia (CSM), the National Cyber Security Agency (NACSA), and the Malaysian Communications and Multimedia Commission (MCMC), to organize regular cybersecurity awareness programs emphasizing secure password practices, such as the use of strong, unique passwords and multi-factor authentication for students at institutions of higher learning. In addition, universities may also establish dedicated cybersecurity units to promote cybersecurity awareness and provide consultation sessions, offering students professional advice and guidance on cybercrime–related issues. In addition, specific attention should be given to educating students about cybersecurity risks associated with social media usage, including phishing attacks, privacy leakage, and oversharing of personal information. Policymakers such as the Malaysian Qualifications Agency (MQA) and university administrators may also consider integrating cybersecurity modules into the academic curriculum to promote consistent and long-term awareness. Future research is encouraged to explore additional factors influencing cybersecurity awareness, such as attitudes, risk perception, and technological self-efficacy, using larger samples.

In conclusion, this study contributes to the existing body of knowledge by providing empirical evidence on cybersecurity awareness among Malaysian university students. The findings underscore the importance of web browser security while revealing critical weaknesses in password practices and social media behavior. Addressing these gaps is essential to fostering a safer digital environment within higher education institutions. By enhancing targeted awareness initiatives and promoting responsible online behavior, universities can play a vital role in strengthening students' cybersecurity resilience and

preparedness against evolving cyber threats.

REFERENCES

Abd Rahman, N. H., Raju, R., Ariffin, S., Hamid, N. H. A. A., & Ahmad, A. (2022). Adoption of cyber insurance in Malaysian organisations. *International Journal of Innovative Computing, 12(2)*, 45–51.

Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences, 12(5)*, 2589.

Chuen, Y. S., Al-Rashdan, M., & Al-Maatouk, Q. (2020). Graphical password strategy. *Journal of Critical Reviews, 7(3)*, 102–104.

Daud, M., & Rasiah, R. (2023). *Addressing Cybersecurity Issues* (pp. 243–263). https://doi.org/10.4324/9781003367093-14

Dioubate, B. M., Daud, W., & Norhayate, W. (2022). Cybersecurity risk management frameworks implementation in Malaysian higher education institutions. *International Journal of Academic Research in Business and Social Sciences, 12(4)*, 1356–1371.

G. Shipkovenski, T. Kalushkov, E. Petkov, R. R., and D. V. (n.d.). Selection Of Ad Blockers According To Their Type Of Installation. *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, 2022, Pp. 1-5, Doi: 10.1109/HORA55278.2022.9800050*.

Gallus, P., Stanék, D., & Klaban, I. (2025). Security Evaluation of Password Managers: A Comparative Analysis and Penetration Testing of Existing Solutions. *International Conference on Cyber Warfare and Security*, 105–113.

Hamzaha, S., Ani, F., Rameli, N., Md Nor, N., Halim, H., Md Ali, A., Rahman, R., Attan, N., & Kamri, K. A. (2021). Level of awareness of social media users on cybersecurity: case study among students of University Tun Hussein Onn Malaysia. *Turkish Journal of Computer and Mathematics Education, 12(2)*, 694–698.

Johari, R. J., Rosnidah, I., & Saaid, N. F. M. (2022). Cybercrime fraud: Malaysian perspective. *In Acceleration of Digital Innovation & Technology towards Society 5.0* (pp. 273–278). Routledge.

Kamalulail, A., Razak, N. E. N. A., Omar, S. A., & Yusof, N. M. (2022). Awareness of Cybersecurity: A Case Study in UiTM Negeri Sembilan Branch, Seremban Campus. *E-Academia Journal*, *11*(1).

Kaushik, K., Aggarwal, S., Pandey, S., Mudgal, S., & Garg, S. (2021). Investigating and Safeguarding the Web Browsers from Malicious Web Extensions. *GRD Journal for Engineering, 6*(10).

Khidzir, N. Z., Ismail, A. R., Daud, K. A. M., Afendi, M. S., Ghani, A., & Ibrahim, M. A. H. (2016). Critical cybersecurity risk factors in digital social media: Analysis of information security requirements. *Lecture Notes on Information Theory Vol. 4*(1), 18–24.

Kraus, L., Ukrop, M., Matyas, V., & Fiebig, T. (2020). *Evolution of SSL/TLS Indicators and Warnings in Web Browsers BT - Security Protocols XXVII* (J. Anderson, F. Stajano, B. Christianson, &

V. Matyáš (eds.); pp. 267–280). Springer International Publishing.

McCabe, C., Mohideen, A. I. C., & Singh, R. (2024). A blockchain-based authentication mechanism for enhanced security. *Sensors, 24*(17), 5830.

Nurse, J. R. C. (2021). Cybersecurity awareness. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 1–4). Springer.

O. Kulyk, P. Mayer, M. V., and O. K. (2018). A Concept and Evaluation of Usable and Fine-Grained Privacy-Friendly Cookie Settings Interface. *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA*, 1058–1063.

Potgieter, P. (2019). The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology. *ICICIS*, 272–280.

Razaque, A., Al Ajlan, A., Melaoune, N., Alotaibi, M., Alotaibi, B., Dias, I., Oad, A., Hariri, S., & Zhao, C. (2021). Avoidance of cybersecurity threats with the deployment of a web-based blockchain-enabled cybersecurity awareness system. *Applied Sciences, 11*(17), 7880.

Seemma, P.S., Nandhini, S., & Sowmiya, M. (2018). Overview of cybersecurity. *International Journal of Advanced Research in Computer and Communication Engineering, 7*(11), 125–128.

van Oorschot, P. C., & van Oorschot, P. C. (2021). Web and Browser Security. *Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin*, 245–279.

Xiang, C. S., & Hasbullah, M. (2023). *Cybersecurity Awareness, Cyber Human Values, and Cyberbullying Among University Students in Selangor, Malaysia*.

Zulkifli, Z. et. al. (2020). Cyber Security Awareness Among Secondary School Students in Malaysia. *Journal of Information Systems and Digital Technologies, 2*(2), 28–41.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge, and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97.