JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT (JISTM)
www.jistm.com

BRIDGING THE GAPS: EVALUATING CYBERSECURITY AWARENESS AND PRACTICES FOR ENHANCED DIGITAL SECURITY

Andria[1], Ridam Dwi Laksono[2], Kelik Sussolaikah[3], Siti Rafidah M-Dawam[4*], Mazura Mat Din[5], Shaifizat Mansor[6]

[1] University of PGRI Madiun JI Auri 14-15 Kanigoro, Madiun 63117 Indonesia
Email: andria@unipma.ac.id
[2] University of PGRI Madiun JI Auri 14-15 Kanigoro, Madiun 63117 Indonesia
Email: ridam.dl@unipma.ac.id
[3] University of PGRI Madiun JI Auri 14-15 Kanigoro, Madiun 63117 Indonesia
Email: kelik@unipma.ac.id
[4] Faculty of Computer And Mathematical Sciences, UiTM Kedah Branch, Malaysia
Email: srafidah192@uitm.edu.my
[5] Faculty of Computer And Mathematical Sciences, UiTM Kedah Branch, Malaysia
Email: mazuramd@uitm.edu.my
[6] Faculty of Computer And Mathematical Sciences, UiTM Kedah Branch, Malaysia
Email: shaifizat@uitm.edu.my
[*] Corresponding Author

Article Info:

Article history:
Received date: 14.01.2025
Revised date: 23.01.2025
Accepted date: 27.02.2025
Published date: 20.03.2025

To cite this document:

Andria, Laksono, R. D., Sussolaikah, K., M-Dawam, S. R., Mat Din, M., & Mansor, S. (2025). Bridging The Gaps: Evaluating Cybersecurity Awareness and Practices for Enhanced Digital Security. *Journal of Information System and Technology Management, 10* (38), 202-210.

DOI: 10.35631/JISTM.1038013

Abstract:

Cybersecurity threats become a normal phenomenal in our daily life due to the advancement of Internet technology and the widespread use of it. To mitigate the risk aside from the advantages of these technology, one of the ways is to educate the users. In this preliminary study we evaluate cybersecurity awareness, practices, and preparedness among respondents, focusing on their knowledge of fundamental concepts, adherence to institutional policies, and incident response capabilities. There are 35 respondents who are among the schoolteachers who taught basic computer subject in various secondary schools in Kuala Muda and Yan districts of Kedah. While 77.7% of respondents are familiar with cybersecurity concepts and 100% demonstrate awareness of critical issues such as phishing and strong passwords, gaps persist in applying cybersecurity measures. Inconsistent password hygiene, low training participation (84.9%), and limited confidence in incident response are notable challenges. Furthermore, only 27.3% of respondents are well-versed in institutional cybersecurity policies. These findings emphasize the need for improved training programs, clearer policy communication, and enhanced institutional support to bolster readiness. Recommendations include expanding educational initiatives, mandating regular password updates, and refining incident response protocols. Addressing these gaps can strengthen organizational cybersecurity defences and create a more secure digital environment, highlighting the urgency of proactive measures to bridge the gap between knowledge and practical implementation.

Keywords:

Cybersecurity, Awareness, Incident Preparedness, Cyber Threats

Introduction

Cybersecurity has become a critical concern in educational institutions, as the increasing reliance on digital tools and online platforms (Ariffin et al., 2021) exposes schools to a countless of cyber threats. From phishing attempts to malware attacks, the potential risks underscore the need for robust cybersecurity practices among educators and staff (Ramakrishnan et al., 2022). This study aims to assess the current level of cybersecurity awareness, practical application, and incident preparedness within the surveyed population, focusing on five key areas: basic knowledge, practical practices, institutional policies, incident response, and improvement feedback.

Despite the global emphasis on cybersecurity, gaps in knowledge and inconsistent practices remain prevalent in many institutions (Syed Ibrahim et al., 2021). Educators, often on the frontlines of implementing digital tools, must balance the demands of their roles with the imperative to maintain secure practices (Daud & Rasiah, 2023) . This study investigates these challenges by analysing survey responses to identify strengths, weaknesses, and opportunities for improvement.

The findings serve as a baseline to understand the current cybersecurity landscape in educational settings and inform targeted interventions (Saachi, 2022). By highlighting areas such as password management, two-factor authentication usage, policy awareness, and training needs, this research provides actionable insights to enhance cybersecurity resilience. The subsequent sections detail the results, propose recommendations, and outline strategies for fostering a culture of cybersecurity within educational institutions.

Literature Review

Cybersecurity awareness and practices have become a focal point for institutions aiming to mitigate risks associated with increasing cyber threats (Mat et al., 2022). Studies have consistently highlighted the importance of foundational knowledge (Wahid et al., 2021), practical measures, and organizational policies in building a robust cybersecurity framework (Sulaiman et al., 2022). Ahmad, Maynard, and Shanks (2015) emphasized the need for systematic incident response strategies to address cybersecurity threats effectively. Their research aligns with the current study's findings, which reveal varied confidence levels in incident response preparedness among respondents.

The implementation of basic cybersecurity knowledge is crucial, as studies show widespread lack of awareness about cybercrime among students and teachers, despite the rising use of the internet (Mat et al., 2022). This highlights the need for comprehensive cybersecurity programs to protect users from digital threats, particularly in educational environments (Al, 2021). The growing threat of cyberattacks on educational institutions is highlighted in this paper's thorough review of cybersecurity awareness initiatives in schools (Srivastava et. al, 2024). It looks at existing programs, their difficulties, and the part administrators and instructors play in raising awareness. The significance of taking proactive steps to improve cybersecurity education in schools is emphasized in the report. This recommendation echoes the present findings, where 84.9% of respondents reported not attending training in the past year.

Password management remains a critical component of cybersecurity. Hadlington (2017) explored the psychological factors influencing password hygiene and found that consistent education on strong password practices significantly improves security behaviors. Similarly, this study observed inconsistencies in respondents' password update frequencies.

Institutional policies play a crucial role in shaping cybersecurity practices. Ifinedo (2014) highlighted the impact of social and cognitive factors on policy compliance, reinforcing the finding that only 27.3% of respondents are thoroughly aware of their institution's policies.

Practical measures such as the adoption of two-factor authentication and antivirus software are essential. Kayworth and Whitten (2010) argued that balancing technical solutions with human awareness is key to effective cybersecurity. The current study's finding that 88% of respondents use antivirus software reflects progress in this area but also underscores the need for broader adoption of best practices.

Finally, Saini, Rao, and Panda (2012) emphasized the importance of awareness campaigns to combat threats like phishing, a topic where this study found high levels of respondent knowledge but varying levels of practical implementation. Shillair et. al (2022) evaluates the impact of cybersecurity education, awareness, and training (CEAT) on internet use across 80 countries. It shows CEAT positively influences internet vitality, particularly in low-income nations, and suggests improvements in policy, practice, and future research for effective cybersecurity capacity building.

These studies collectively underscore the importance of integrating education, policy, and practice to create a resilient cybersecurity culture, aligning closely with the findings and recommendations of this research.

Methodology

The design of a Cybersecurity Awareness Questionnaire is crucial for assessing the knowledge and practices of educators in relation to digital security. Jouini et al. (2021) describe a well-structured questionnaire that covers three key areas: basic knowledge, practical practices, and security protocols. The basic knowledge section aims to gauge participants' understanding of fundamental cybersecurity concepts, such as password management, phishing threats, and data protection. The practical practices section focuses on how educators implement cybersecurity measures in their daily activities, such as using secure networks or safeguarding educational content. The final section assesses participants' familiarity with and adherence to established security protocols, such as encryption and authentication procedures. To ensure the comprehensive evaluation of these areas, the questionnaire incorporates various types of questions. Multiple-choice questions are used to assess basic knowledge and understanding of specific cybersecurity concepts. Likert scale questions are included to measure the extent to which educators engage in secure practices and their level of confidence in implementing cybersecurity protocols. This combination of question types provides a holistic view of educators' cybersecurity awareness, helping to identify both strengths and areas that require further attention (Jouini et al., 2021).

The sampling is a critical role in ensuring the validity and relevance of a study on cybersecurity awareness among educators. In this context, the study focuses on the selection of 35 computer science educators from various schools in Kuala Muda district of Kedah to provide a diverse representation of teaching experiences and institutional settings. By targeting educators with expertise in technology-related fields, the study aims to gather insights into the specific challenges and practices related to cybersecurity in educational environments.

Results and Findings

The results of the study are presented across five key sections of cybersecurity awareness and practices namely, Cybersecurity Knowledge, Cybersecurity Practices, Security Policies & Procedures, Incident Response and Feedback & Improvements.

Basic Cybersecurity Knowledge

The findings reveal that a significant majority of respondents possess a solid foundation in cybersecurity concepts. Notably, 77.7% are familiar with the general principles of cybersecurity, demonstrating a clear understanding of its primary objective: safeguarding data and systems from unauthorized access and attacks. Furthermore, all respondents correctly identified "P@ssw0rd!2024" as an example of a strong password and recognized phishing as a deceptive attempt to obtain sensitive information by impersonating a trustworthy entity. These results highlight a widespread awareness of essential cybersecurity principles among the participants as shown in Figure 1.

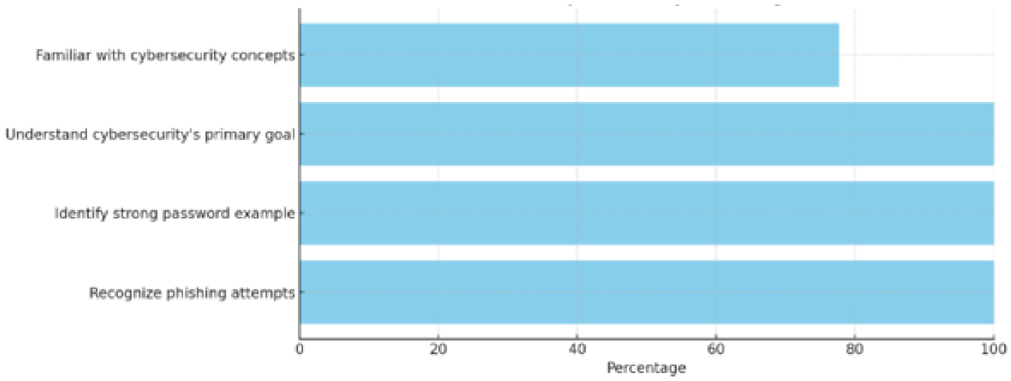

Figure 1: Basic Cybersecurity Knowledge

Practical Cybersecurity Practices

The survey highlighted varying levels of adherence to practical cybersecurity measures. Based on Figure 2, nearly 90% of respondents reported using two-factor authentication (2FA) for important accounts, indicating widespread adoption of this critical security practice. However, password update habits vary significantly: around 20% update their passwords regularly (every 3–6 months), one-third update them occasionally (once a year), over 40% rarely do so, and a small minority (3%) never update their passwords.

When faced with unexpected emails from unknown senders requesting sensitive information, most respondents (85%) choose to ignore and delete such emails, while 15.2% take the additional step of forwarding them to IT support or relevant authorities.

Regarding cybersecurity education, just over half of the respondents (51.5%) regularly educate their students on cybersecurity practices, 42.4% do so occasionally, and 6% never address this topic. These findings underscore both strengths and gaps in practical cybersecurity engagement and awareness.

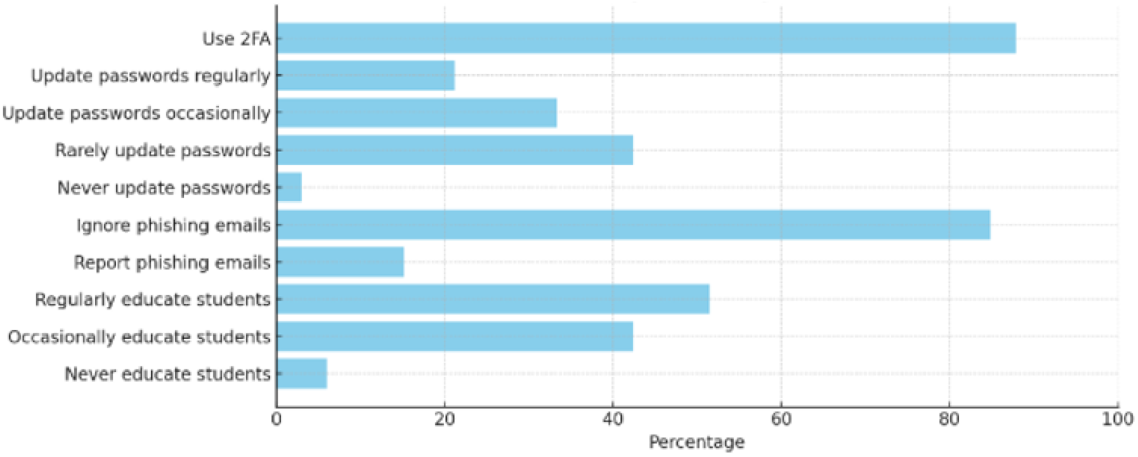

Figure 2: Practical Cybersecurity Practices

Security Policies and Procedures

Awareness and implementation of institutional cybersecurity policies and procedures were evaluated, revealing notable disparities. Only 27.3% of respondents are thoroughly familiar with their school's cybersecurity policies, while two-thirds have a partial understanding, and 6.1% are entirely unaware as shown in Figure 3.

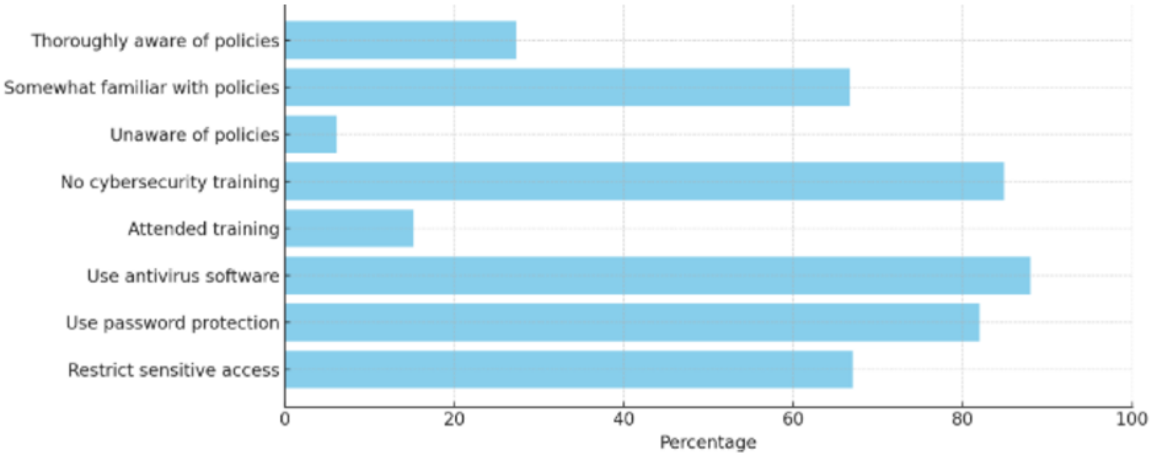

Figure 3: Security Policies and Procedures

Training participation is particularly low, with 84.9% of respondents not attending any cybersecurity workshops or training sessions in the past year, and only 15.2% reporting recent training.

Despite these gaps, key cybersecurity measures are widely practiced. Nearly 88% of respondents use antivirus software and perform regular updates to protect against threats. Additionally, over 80% ensure that all devices are password-protected, and two-thirds implement access restrictions to safeguard sensitive information. These findings highlight both strengths in specific practices and areas for improvement in policy awareness and training participation.

Incident Response

Respondents' preparedness for and experience with cybersecurity incidents show notable variation. Based on Figure 4, when suspecting malware, nearly 80% would immediately disconnect from the internet and run a malware scan. A smaller group (15.2%) would seek advice from a colleague without taking immediate action, while a minimal 6.1% would continue using the computer while attempting to address the issue.

In terms of experiences with cybersecurity incidents at schools, over half (57.6%) have never encountered an incident. Meanwhile, nearly one-quarter (24.2%) have experienced and successfully resolved such incidents, while 18.2% have faced incidents that remain unresolved.

Confidence in responding to cybersecurity incidents is divided, with a slight majority (57.6%) expressing confidence in their ability to handle such situations, while 42.4% report a lack of confidence. These findings highlight both proactive behaviours and areas requiring improved training and support.

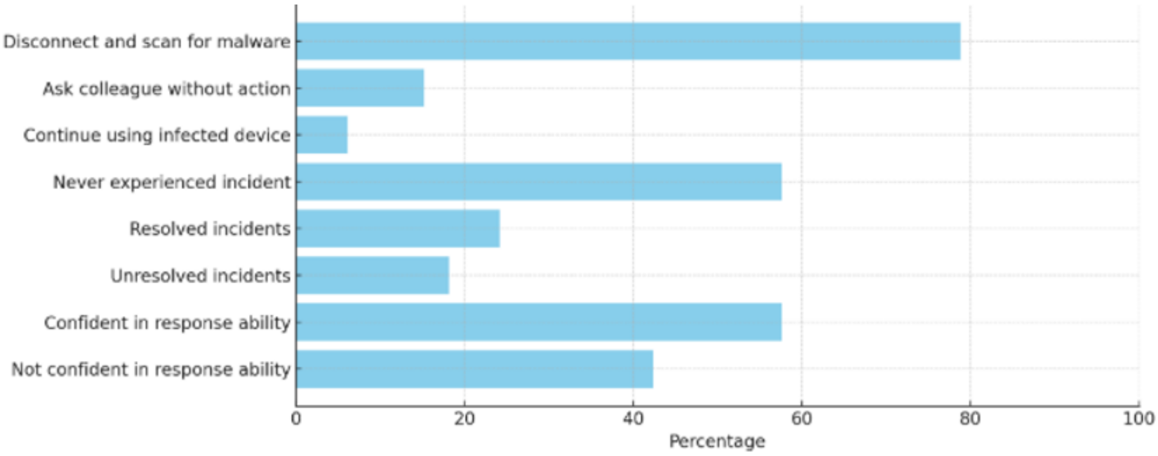

Figure 4: Incident Responses

Feedback and Improvement

Respondents identified key areas for improving cybersecurity practices. A majority (60%) expressed the need for additional training or workshops to enhance their knowledge and skills. Half of the respondents (50%) emphasized the importance of access to clear cybersecurity guidelines and best practices, while 40% indicated that regular updates and alerts about emerging cyber threats would be beneficial. Additionally, another 40% highlighted the need for greater support from their IT department to strengthen cybersecurity efforts as shown in Figure 5.

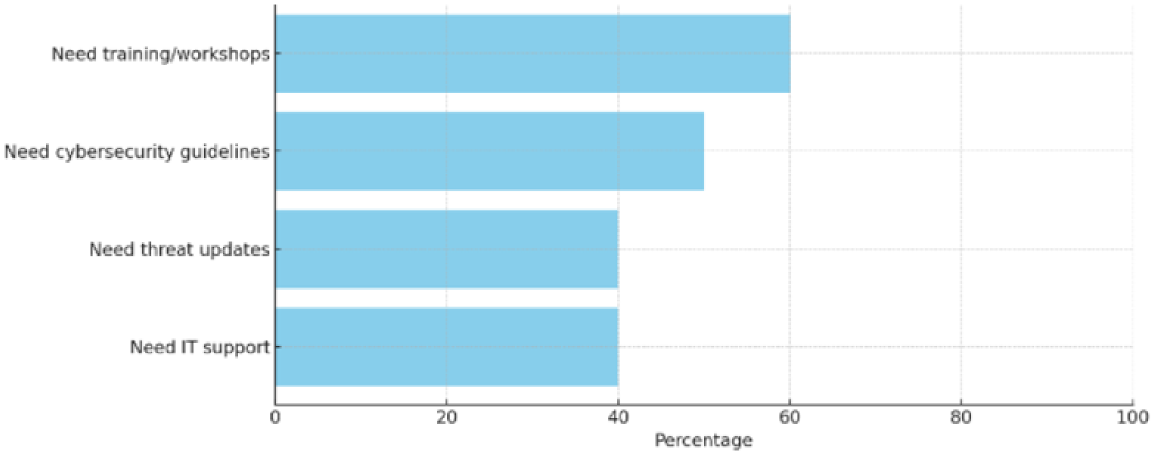

Figure 5: Feedback and Improvement Responses

Recommendations

Based on the findings, the following recommendations are proposed to enhance cybersecurity awareness and practices. To raise awareness, targeted campaigns or workshops should be launched to familiarize staff and students with basic cybersecurity concepts, particularly for the 22.3% who lack awareness. Additionally, clear and accessible cybersecurity guidelines and best practices should be shared with all stakeholders.

To improve password practices, organizational policies should mandate regular password updates, supported by automated reminders, and provide training on the importance of password hygiene, including how to identify strong passwords.

To expand training opportunities, mandatory, regular cybersecurity training sessions should be conducted for the 84.9% who have not attended any programs. These sessions should also incorporate scenario-based training to build confidence in handling cybersecurity incidents.

To strengthen incident response, regular drills and workshops should be organized to improve preparedness and confidence. Clear protocols should be established, and accessible IT support should be provided to help staff and students manage potential threats effectively.

To encourage practical measures, the adoption of two-factor authentication (Wahid et al., 2021) should be promoted, and the importance of securing sensitive data should be emphasized. Ongoing education about phishing attacks and other cyber threats is crucial for ensuring proactive cybersecurity practices.

Finally, to provide institutional support, resources such as updated cybersecurity guidelines, emerging threat alerts, and increased collaboration between the IT department and staff should be prioritized to offer continuous support and guidance.

Conclusion

The study highlights that while respondents demonstrate a basic understanding of cybersecurity concepts and engage in some practical measures, significant gaps persist in awareness, training, and consistent application of best practices. These gaps include insufficient training opportunities, limited policy awareness, and inconsistent password update practices.

Additionally, a substantial proportion of respondents lack confidence in responding to cybersecurity incidents.

To address these issues, institutions should focus on fostering a culture of cybersecurity awareness through targeted training programs, sharing clear guidelines, and improving password practices through regular updates and training. Strengthen incident response via drills, clear protocols, and accessible IT support. Promote two-factor authentication, secure sensitive data, and educate on phishing threats. In addition to it, institutional support should prioritize updated guidelines, threat alerts, and IT-staff collaboration for continuous guidance. These steps aim to enhance awareness, preparedness, and proactive cybersecurity practices

Acknowledegment

We would like to express our sincere gratitude to the Universitas PGRI Madiun (UNIPMA) and Universiti Teknologi MARA (UiTM) Kedah for their collaboration via Dana Dalaman Negeri Padanan Bersama 2023 600-UiTMKDH(PJI.5/4/1)(6/2023) in securing the matching grant that has made this project possible. This partnership has provided invaluable support and resources, enabling us to advance our research and contribute to the academic community. We are particularly thankful to the funding bodies and the individuals involved from both institutions, whose dedication and commitment have been essential in fostering this successful collaboration.

References

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. International Journal of Information Management, 35(6), 717–723. https://doi.org/10.1016/j.ijinfomgt.2015.08.001

Ariffin, A., Mohd, N., Rokanatnam, T., Malaysia, C., My, A., & My, N. (2021). Cyberbullying via Social Media: Case Studies in Malaysia. *Journal of Cyber Security*, *3*(1).

Daud, M., & Rasiah, R. (2023). Addressing Cybersecurity Issues. In *Digitalization and Development: Ecosystem for Promoting Industrial Revolution 4.0 Technologies in Malaysia*. https://doi.org/10.4324/9781003367093-14

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky online behaviors. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialization, influence, and cognition. Information & Management, 51(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. MIS Quarterly Executive, 9(3), 163–175.

Mat, B., Pero, S. D. M., Zengeni, K. T., & Fakhrorazi, A. (2022). Towards an Understanding of Emerging Cybersecurity Challenges of a Small State: A Case Study of Malaysia. *Tamkang Journal of International Affairs*, *25*(3). https://doi.org/10.6185/TJIA.V.202204_25(3).0002

Ramakrishnan, K., Yasin, N. M., & Periasamy, J. (2022). Digital divide on cybersecurity awareness among the Malaysian higher learning institution students. *AIP Conference Proceedings*, *2472*. https://doi.org/10.1063/5.0092796

Saachi, G. G. (2022). *Malaysia: An analysis of cybersecurity in Malaysia*. ETCIOSEA.

Saini, A., Rao, H., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications, 2(2), 202–209.

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & Von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security, 119, 102756. https://doi.org/10.1016/j.cose.2022.102756

Srivastava, A. K., Singh, A. V., & Som, S. (2024). Critical analysis of cybersecurity awareness programs in school education. LIB PRO, 44(3), JUL-DEC 2024. Published July 31, 2024.

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 (Switzerland)*, *13*(9). https://doi.org/10.3390/info13090413

Syed Ibrahim, S. N., Shamsudin, A., Abdullah, S., Ibrahim, M. T., Jaaffar, M. Y., & Bani, H. (2021). Content Analysis of Voluntary Disclosures on Cybersecurity in Malaysia. *International Journal of Academic Research in Accounting, Finance and Management Sciences*, *11*(4). https://doi.org/10.6007/ijarafms/v11-i4/11346

Wahid, S. D. M., Buja, A. G., Hasrol Jono, M. N. H., & Aziz, A. A. (2021). Assessing the influential factors of cybersecurity awareness in Malaysia during the pandemic outbreak: A structural equation modeling. *International Journal of Advanced Technology and Engineering Exploration*, *8*(74). https://doi.org/10.19101/IJATEE.2020.S1762116