INDONESIAN JOURNAL OF INNOVATION AND APPLIED SCIENCES (IJIAS)
Journal Homepage: https://ojs.literacyinstitute.org/index.php/ijias
ISSN: 2775-4162 (Online)
Research Article

Volume 4	Issue 3	October (2024)	DOI: 10.47540/ijias.v4i3.1482	Page: 208 – 216

Investigating Security Awareness and Incident Reporting levels at Mbarara University of Science and Technology

Mbonimpa Thomas[1], Ntwari Richard[2], Muhereza, J. Innocent[3], Muheki Priscilla[1]
[1]Department of Physics, Mbarara University of Science and Technology, Uganda
[2]Department of Computer Science, Mbarara University of Science and Technology, Uganda
[3]Department of Security, Mbarara University of Science and Technology, Uganda
Corresponding Author: Mbonimpa Thomas; Email: tmbonimpa@must.ac.ug

ARTICLE INFO

Keywords: Incident Reporting, Security Awareness, Security Behavior, Security Incident.

Received : 17 June 2024
Revised : 11 September 2024
Accepted : 28 October 2024

ABSTRACT

Higher learning institutions confront heightened cyber threats due to the value of their data, necessitating a robust security culture. In addition to cyber threats, various security incidents cause danger to devices and personal belongings on campuses. Security incidents present a substantial challenge to academic institutions, especially higher education, where their occurrence is notably prevalent. These incidents encompass a broad spectrum, including thefts, data breaches, malware attacks, and other breaches in physical security. Addressing security incidents necessitates critical strategies involving educating and raising awareness among the academic and surrounding communities. In this study, we aimed to investigate the security awareness levels of students at Mbarara University of Science and Technology and establish their incident reporting attitudes and levels. We used a quantitative research method and conducted different statistical tests. The findings indicate that ~50% of the participants had not had any security awareness training, indicating a very big gap in the security culture at this institution. Although some of the students indicated their awareness of security threats, the percentage who showed a lack of awareness or a noncommittal response suggests that there is a very big need for security awareness strategies. Additionally, about 60% of the students showed their will to report security threats which implies that they can be vigilant about their and the institutional security. Based on these findings we recommend continuous training programs for students to increase their levels of awareness and incident reporting and consequently develop an institutional security culture.

INTRODUCTION

Business organizations invest substantially in cutting-edge technologies to streamline their production processes and gather critical data for their operations. These technologies are pivotal in enhancing efficiency and facilitating informed decision-making (Rosin et al., 2022). However, alongside the benefits, the increased reliance on technology also exposes organizations to cyber threats (Li & Liu, 2021). Consequently, organizations including higher learning institutions prioritize protecting their data and digital assets by investing in robust computer security solutions. These solutions encompass a range of measures, including firewalls, encryption, intrusion detection systems, and employee training programs (Jamal et al., 2024). By implementing comprehensive security measures, organizations aim to safeguard their sensitive information, intellectual property, and financial assets from cyberattacks and unauthorized access.

Despite concerted efforts to fortify their cyber defenses, organizations face persistent challenges from cybercriminals who continue to evolve and adapt their tactics (Shah, 2024). Cybercriminals employ sophisticated techniques to breach networks, systems, and databases, exploiting vulnerabilities in software and exploiting human

error (Aslan et al., 2023). Indeed, a significant proportion of cyber incidents can be attributed to human factors, such as clicking on malicious links, falling victim to phishing scams, or using weak passwords (Sawyer & Hancock, 2018). Moreover, the proliferation of mobile devices, cloud computing, and internet-connected devices further expands the attack surface, making organizations more susceptible to cyber threats (Djenna et al., 2021). Consequently, organizations must adopt a proactive approach to cybersecurity, continually assessing and enhancing their defenses to mitigate the risk of cyberattacks and data breaches.

In addition to cyber threats, various security incidents such as thefts, physical attacks on individuals, etc threaten organizational infrastructure, individuals, and their tangible and intangible assets. These security incidents present a substantial challenge, especially to higher learning institutions, where their occurrence has become notably prevalent (Mofokeng et al., 2023; Moghayedi et al., 2024; Ulven & Wangen, 2021).

According to a study by (Ekpoh et al., 2020), theft, kidnaps, sexual abuse, room and office break-ins, cell phone stealing, violent demonstrations by students, vandalism, etc are major security challenges on campuses. Universities are complex organizations comprising people from diverse backgrounds and with diverse goals and therefore are at risk of security threats.

In response to the evolving threat landscape, organizations are increasingly prioritizing security awareness and education as integral components of their defense strategy (Cheng & Wang, 2022). Recognizing that security is not solely the responsibility of specific departments but requires collective vigilance, organizations invest in training programs to educate employees about risks and best practices (Ahmad et al., 2020). Moreover, fostering a culture of security awareness promotes a sense of shared responsibility and commitment among stakeholders, breaking down departmental barriers and promoting collaboration against security threats.

Therefore insufficient understanding and awareness of security culture among students and staff lead to unauthorized access, data breaches, and malware vulnerabilities (González-Granadillo et al., 2021). In addition to this, the most utilized means of reporting security incidents at most universities in Uganda including Mbarara University of Science and Technology (MUST) include the use of email, phone calls, and other platforms that don't give immediate responses to the incidents and are not reliable. Therefore implementing a comprehensive communication platform and awareness of security incidents is crucial to mitigate risks, improve preparedness, and foster a security culture, thus fortifying the academic community and preserving institutional integrity. The main aim of security is to: ensure the safety of both staff and students, protect the university's property, and detect and investigate crime to apprehend and prosecute offenders.

This study therefore explores the pivotal role of security awareness information amidst multifaceted challenges faced by universities. It seeks to identify the current status of security awareness initiatives being utilized in the university and further progress to develop a communication framework to improve security incident management.

METHODS

The study employed a descriptive cross-sectional design, incorporating a quantitative survey approach to investigate information security awareness among students at MUST. Mbarara University of Science and Technology is the largest and oldest public university in the western part of Uganda (www.must.ac.ug). It offers programs in different faculties i.e. Science, Medicine, Applied Science and Technology, Information Technology and Computing, Business and Management Science, and Interdisciplinary Studies.

The sample size for the study was determined using Israel's tables for sample size calculation, considering a confidence level of 95%. The University has a total estimated population of 7700 individuals. A total of 374 students were randomly sampled from different faculties within the University. This was done to ensure the representativeness of the study. A survey questionnaire was developed based on the Protection Motivation Theory (PMT), a widely recognized framework for understanding individuals' responses to threats and risks. The questionnaire comprised items assessing various dimensions of information security awareness, including perceived vulnerability, severity, response

efficacy, and self-efficacy. Participants were briefed about the purpose of the study and provided informed consent before completing the questionnaire. Data collection was conducted through a paper-based survey. Ethical guidelines were adhered to throughout the research process to ensure the protection of participants' rights and the confidentiality of their responses. Institutional review board (IRB) approval was obtained from the University review board (The MUST REC) before commencing data collection.

The collected data were subjected to statistical analysis using SPSS. Descriptive statistics, including frequencies, percentages, means, and standard deviations, were computed to summarize the demographic characteristics of the sample and the key variables related to information security awareness. Potential limitations of the study, such as sample representativeness, self-report biases, and generalizability of findings, were acknowledged. Steps were taken to minimize these limitations, including random sampling and ensuring anonymity of responses.

RESULTS AND DISCUSSION

Response Rate

The sample that was used included participants (students) from different faculties. 46.3% of the respondents belonged to the Faculty of Science indicating the availability and willingness of participants. The rest of the respondents were from the Faculty of Business and Management Science (13.0%), Faculty of Applied Science and Technology (10.6%), Faculty of Medicine (13.0%), Faculty of Computing and Informatics (7.9%), and Faculty of Interdisciplinary Studies (10.4%).

Training and Security Awareness

The outcomes of the survey conducted among university students uncover various notable trends concerning security awareness, incident reporting, and password management. Initially, a significant proportion of students expressed dissatisfaction with the adequacy of training or guidance provided regarding security incidents (see Figure1), with more than half of the respondents indicating a lack of any such training.

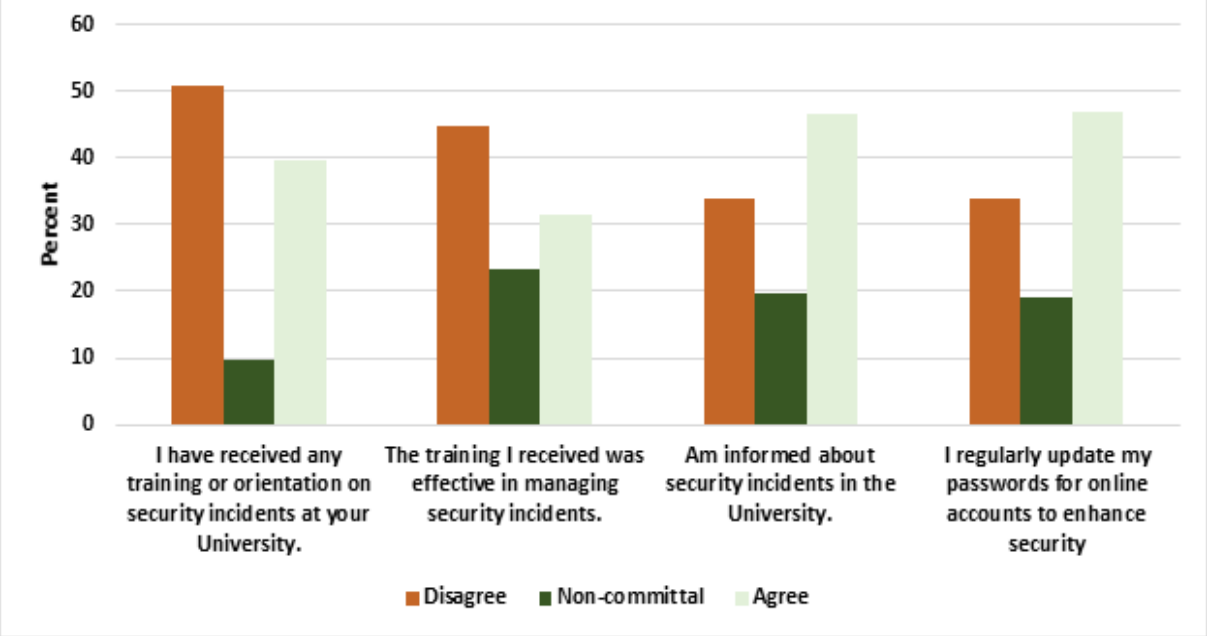

Figure 1. Shows the responses to training on security awareness and preparedness

This emphasizes a critical deficiency in awareness and readiness, potentially leaving students susceptible to security risks. Importantly, similar concerns echoed through interviews with staff members, suggesting a systemic issue within the institution regarding security training. As indicated by (Da Veiga et al., 2020) it is necessary to have regular communication and training on security awareness. This promotes the idea of having a security culture that all the community members embrace.

According to (Alshaikh, 2020) building a cybersecurity culture in Higher Education Institutions can be achieved through continuous

training and awareness campaigns. This can be done during orientation seminars for the new students as they join the University. During these seminars, important information on security policies and procedures should be shared. Additionally, possible disciplinary actions for breaches need to be highlighted. Both students and staff need to understand that security is a shared responsibility and should aim at doing the right thing (Chapman, 2019). Fundamentally, academic institutions should include active security awareness and training programs in their strategic plans.

Awareness of Security Incidents and Reporting

Regarding awareness of security incidents within the university, while a notable fraction of students reported feeling adequately informed, the considerable proportion of non-committal responses and the relatively similar percentages between agreement and disagreement (see Figure 2) imply scope for improvement in the dissemination of information. This supports the necessity for consistent and dependable communication channels to ensure all students receive timely and accurate updates about security incidents. Without effective communication strategies, misinformation, or lack of awareness among students could impede security endeavors.

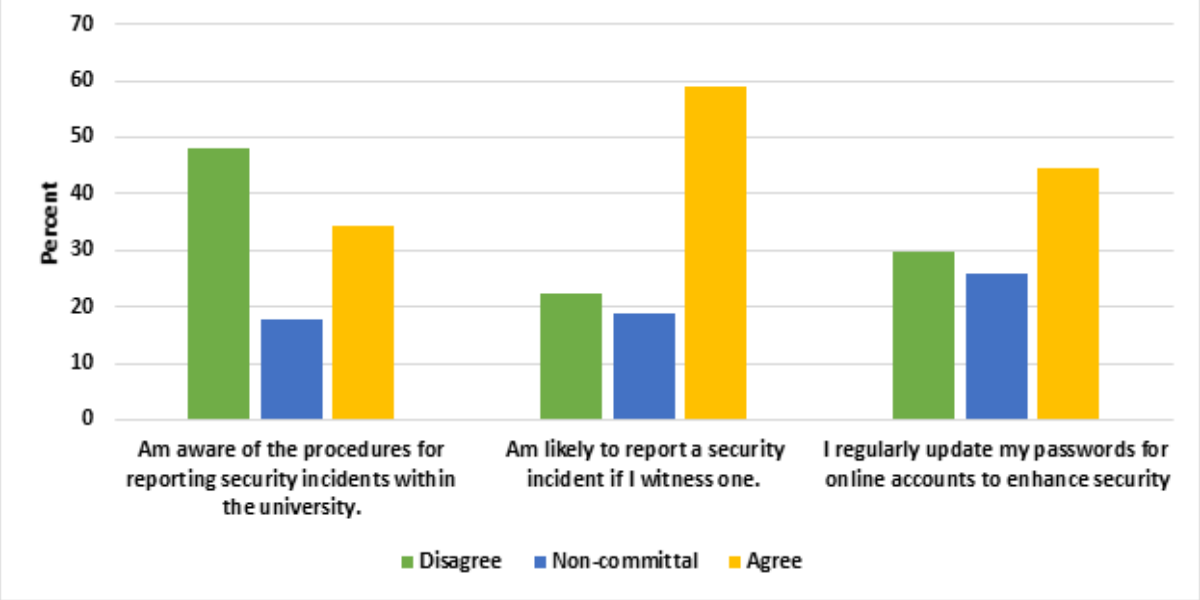

Figure 2. Shows the distribution of students' responses to incident reporting

Related studies worldwide, e.g., (Alharbi & Tassaddiq, 2021; Alqahtani, 2022; Hong et al., 2023) show that security awareness levels among students are generally insufficient, especially in cybersecurity. Even for students with the required information regarding cybersecurity, the approach they use while dealing with this information is inappropriate (Taha & Dahabiyeh, 2021; Thompson et al., 2018) in practical circumstances. Therefore, there is a need for continuous security awareness and training programs (Dash & Ansari, 2022; Khando et al., 2021; Taha & Dahabiyeh, 2021; Zwilling et al., 2022) to ensure that students can improve their alertness.

Concerning password practices, although a significant portion of students claimed regular password updates, a considerable number indicated otherwise(Alqahtani, 2022; Garba et al., 2020). The findings of this study correlate with those of (Alharbi & Tassaddiq, 2021) who found in their investigation of the level of cybersecurity awareness and user compliance among undergraduate students at Majmaah University in Saudi Arabia that the majority of the students found having strong passwords unpleasant and therefore opted to use the same password for all accounts. Inadequate password management could expose students to security breaches or unauthorized access to their accounts.

This highlights the importance of reinforcing the significance of password hygiene and implementing measures to promote secure password management practices among students (Barakovic

& Barakovic Husic, 2023; Hall et al., 2023; Kasowaki & Ali, 2024; Neigel et al., 2020)

Furthermore, the findings indicate a necessity for enhancing awareness of reporting procedures for security incidents. A substantial proportion of students admitted unawareness of these procedures, suggesting a lack of clarity or communication regarding reporting mechanisms. Efforts should be directed toward educating students on prompt and efficient reporting of security incidents, as timely reporting is pivotal for effectively addressing security threats within the university community(Ahmad et al., 2020; Hina & Dominic, 2020; Kumar et al., 2021; Ulven & Wangen, 2021). One such effort is to develop a communication platform for the students that enables real-time reporting of any form of security threat(Hatzivasilis et al., 2021; Hu et al., 2022; Maddireddy & Maddireddy, 2022).

Communication Channels for Security Incident Information

It was observed that the majority of the students (over 60%) receive information through social media.

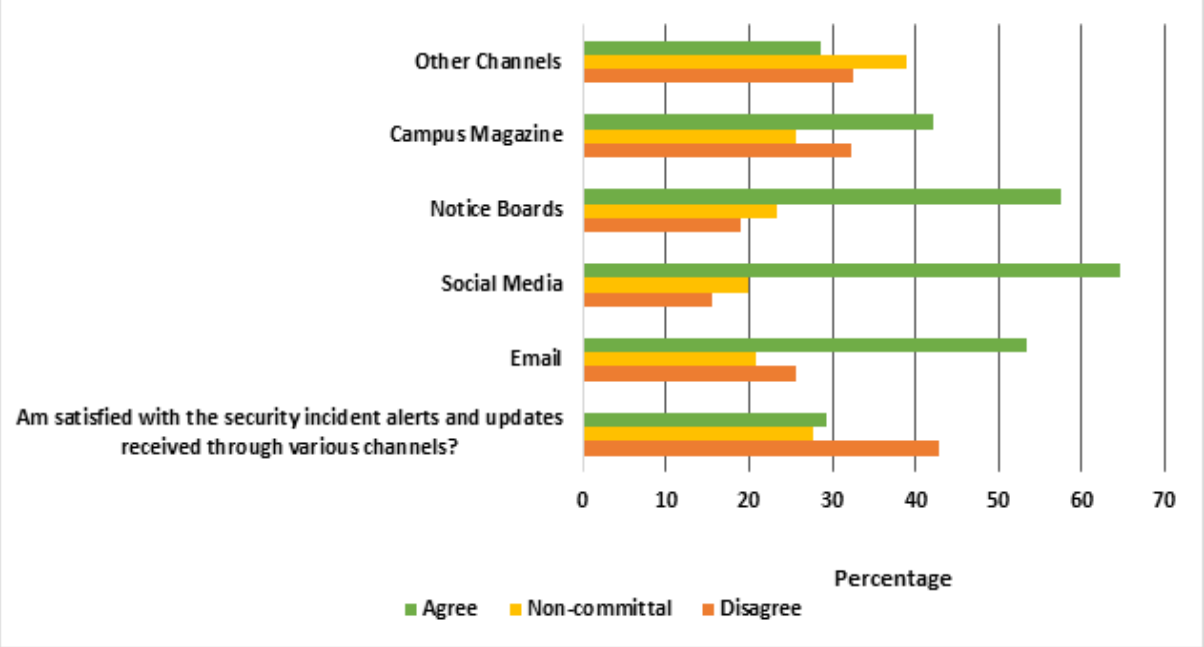

Figure 3. Shows the communication channels used by students

This implies that social media can be one way that can be used to promote security incident awareness. Since social media tends to be embraced by a vast population, it can be utilized to share information regarding cybersecurity and other security matters. Universities including MUST can venture into using social media to share tips, resources, and updates on the security status of the university.

A study by (Rahman et al., 2020) indicates similar findings showing that about 70% of their study population uses social media as their primary source of information. However, even though social media is popular, most people acknowledge that they don't get enough cybersafety information through the platform. This is also evident in the findings of this study. The majority of the respondents showed dissatisfaction with the use of the different communication channels to relay information regarding security. Therefore there is a need for improvement in this arena by relaying security updates through for instance the university's social media accounts.

On the other hand, (Alharbi & Tassaddiq, 2021), suggest that passive awareness methods, such as email, oral presentation, newsletters, and SMS messages, are insufficient for educating users. There is a need to have a combination of passive and proactive methods such as training to have effective security awareness (Arend et al., 2020; Franchina et al., 2021; Kuraku et al., 2023).

Willingness to Report Security Incidents

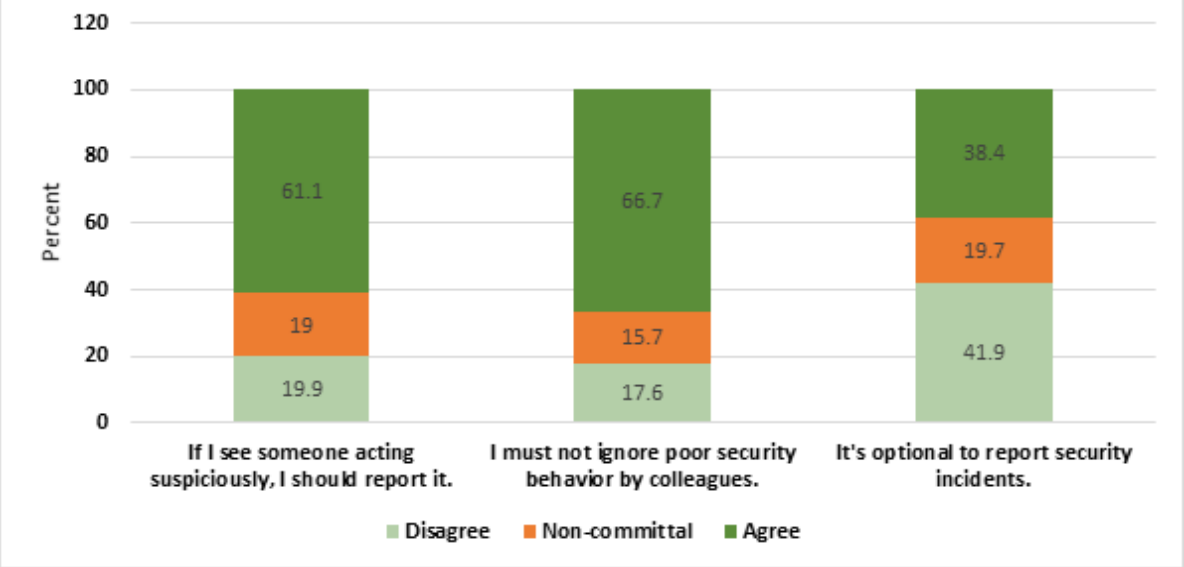

Figure 4. Shows the willingness of students to report security incidents

The survey findings among MUST students regarding incident reporting and security behavior reflect that the majority (~61%, see Figure 4) are willing to report suspicious behavior, indicating a positive attitude to security vigilance. These findings are in agreement with those of (Lamoreaux & Sulkowski, 2021). The author emphasizes that trust in the system is important to enhance the willingness of students to report any security threats. To be assured that what they report will be acted upon accordingly greatly influences the will to report. Students need to be connected to the university environment and trust its systems to facilitate reporting security threats. This also emphasizes the need for a security culture at institutions. Group dynamics also play a big role in promoting security vigilance (Robinson et al., 2022). It should be noted that the percentage of students who agree with the idea that reporting incidents is optional and those who are noncommittal is higher than those who consider it important. This implies that there is still a need for engagement with the students on the importance of security vigilance and pro-activeness. As emphasized by (Kovacevic et al., 2020; Setiawan & Rizal, 2024), improving students' knowledge, attitudes, and behavior regarding security is very crucial for security awareness, and this can be achieved through classroom interactions, training, workshops, etc. information security There needs to be a security culture that is instilled among the students so that they appreciate the value of security within and outside the university environment (Da Veiga, 2023; Wiley et al., 2020).

CONCLUSION

Security awareness is essential for academic institutions because of the vast amount of vital data they handle, the valuable infrastructure they use, and that they deal with students from diverse backgrounds. In this study, we evaluated the security awareness and incident reporting levels among students at Mbarara University of Science and Technology in Uganda, using a quantitative research approach.

Generally, the survey outcomes underscore several areas that need to be improved to bolster security awareness and preparedness among university students. We emphasize that security awareness training programs for both students and staff should be included in the University's security management plan and be executed accordingly. These trainings need to comprehensively address cyber and physical security awareness, secure password management practices, enhancing appropriate use of the different communication channels, and incident reporting.

Acknowledgment

We acknowledge the government of Uganda through the Directorate of Research and Graduate Training (DRGT) of Mbarara University of Science and Technology for funding.

REFERENCES

1. Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939–953.
2. Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2), 23.
3. Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences*, *12*(5), 2589.
4. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003.
5. Arend, I., Shabtai, A., Idan, T., Keinan, R., & Bereby-Meyer, Y. (2020). Passive and not active-risk tendencies predict cyber security behavior. *Computers & Security*, *97*, 101964.
6. Aslan, Ö., Aktug, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.
7. Barakovic, S., & Barakovic Husic, J. (2023). Cyber hygiene knowledge, awareness, and behavioral practices of university students. *Information Security Journal: A Global Perspective*, *32*(5), 347–370.
8. Chapman, J. (2019). *How Safe is Your Data?: Cyber-security in Higher Education*.
9. Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, *13*(4), 192.
10. Da Veiga, A. (2023). A model for information security culture with creativity and innovation as enablers–refined with an expert panel. *Information & Computer Security*, *31*(3), 281–303.
11. Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, 101713.
12. Dash, B., & Ansari, M. F. (2022). *An effective cybersecurity awareness training model: First defense of an organizational security strategy*.
13. Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences*, *11*(10), 4580.
14. Ekpoh, U. I., Edet, A. O., & Ukpong, N. N. (2020). Security challenges in Universities: Implications for safe school environment. *Journal of Educational and Social Research*, *10*(6), 112–112.
15. Franchina, L., Inzerilli, G., Scatto, E., Calabrese, A., Lucariello, A., Brutti, G., & Roscioli, P. (2021). Passive and active training approaches for critical infrastructure protection. *International Journal of Disaster Risk Reduction*, *63*, 102461.
16. Garba, A., Sirat, M. B., Hajar, S., & Dauda, I. B. (2020). Cyber security awareness among university students: A case study. *Science Proceedings Series*, *2*(1), 82–86.
17. González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), 4759.
18. Hall, R. C., Hoppa, M. A., & Hu, Y.-H. (2023). An Empirical Study of Password Policy Compliance. *Journal of The Colloquium for Information Systems Security Education*, *10*(1), 8–8.
19. Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Braghin, C., Damiani, E., Koshutanski, H., Tsakirakis, G., Hildebrandt, T., & others. (2021). The threat-arrest cyber range platform. *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 422–427.
20. Hina, S., & Dominic, P. D. D. (2020). Information security policies' compliance: A perspective for higher education institutions. *Journal of Computer Information Systems*.
21. Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N.-L., & Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates.

Education and Information Technologies, *28*(1), 439–470.

22. Hu, S., Hsu, C., & Zhou, Z. (2022). Security education, training, and awareness programs: Literature review. *Journal of Computer Information Systems*, *62*(4), 752–764.
23. Jamal, H., Algeelani, N. A., & Al-Sammarraie, N. (2024). Safeguarding data privacy: Strategies to counteract internal and external hacking threats. *Computer Science and Information Technologies*, *5*(1), 46–54.
24. Kasowaki, L., & Ali, K. (2024). *Cyber Hygiene: Safeguarding Your Data in a Connected World*. EasyChair.
25. Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security*, *106*, 102267.
26. Kovacevic, A., Putnik, N., & Toškovic, O. (2020). Factors related to cyber security behavior. *IEEE Access*, *8*, 125140–125148.
27. Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management*, *34*(6), 1597–1629.
28. Kuraku, S., Kalla, D., Samaah, F., & Smith, N. (2023). Cultivating Proactive Cybersecurity Culture among IT Professional to Combat Evolving Threats. *International Journal of Electrical, Electronics and Computers*, *8*(6).
29. Lamoreaux, D. J., & Sulkowski, M. L. (2021). Crime Prevention through Environmental Design in schools: Students' perceptions of safety and psychological comfort. *Psychology in the Schools*, *58*(3), 475–493.
30. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186.
31. Maddireddy, B. R., & Maddireddy, B. R. (2022). Real-Time Data Analytics with AI: Improving Security Event Monitoring and Management. *Unique Endeavor in Business & Social Sciences*, *1*(2), 47–62.
32. Mofokeng, J. T., Nkosikhona Simelane, N., & Mofokeng, L. (2023). Student safety and security for sustainable and inclusive residences: A Cross-Sectional Study. *OIDA International Journal of Sustainable Development*, *16*(04), 11–28.
33. Moghayedi, A., Michell, K., Le Jeune, K., & Massyn, M. (2024). Assessing the influence of technological innovations and community-based facilities management on the safety and security of universities. A case study of an open campus. *Facilities*, *42*(3/4), 223–244.
34. Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security*, *92*, 101731.
35. Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382.
36. Robinson, S. R., Casiano, A., & Elias-Lambert, N. (2022). "Is it my responsibility?": A qualitative review of university students' perspectives on bystander behavior. *Trauma, Violence, & Abuse*, *23*(1), 117–131.
37. Rosin, F., Forget, P., Lamouri, S., & Pellerin, R. (2022). Enhancing the decision-making process through industry 4.0 technologies. *Sustainability*, *14*(1), 461.
38. Sawyer, B. D., & Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. *Human Factors*, *60*(5), 597–609.
39. Setiawan, B., & Rizal, M. A. (2024). Measurement of Information Security and Privacy Awareness in College Students after the Covid-19 Pandemic. *Procedia Computer Science*, *234*, 1396–1403.
40. Shah, A. (2024). *Cybercrime Chronicles: Exploring the Evolving Landscape of Challenges in the Digital Era*.
41. Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: A comparison between smartphones and computers. *Education and Information Technologies*, *26*(2), 1721–1736.
42. Thompson, J. D., Herman, G. L., Scheponik, T., Oliva, L., Sherman, A., Golaszewski, E., Phatak, D., & Patsourakos, K. (2018). Student misconceptions about cybersecurity concepts: Analysis of think-aloud interviews. *Journal of Cybersecurity Education, Research and Practice*, *2018*(1), 5.

43. Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2), 39.
44. Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, *88*, 101640.
45. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97.