

Cybersecurity Awareness and Preventive Practices Among Criminal Justice Students: Basis for an Evidenced Based Cyber Safety Education Framework

Romeo A. Gernale, Jr.

Doctor of Philosophy in Development Administration, Major in Security Development, Philippine Christian University, Dasmariñas, Cavite, Philippines

Email of Corresponding Author: eagleragernale@gmail.com

Publication history:

Received: August 8, 2026

Accepted: September 10, 2026

Revised: September 3, 2026

Published: September 11, 2026

International Journal of Sustainable and Integrated Studies, Vol. 1, No. 2, pp. 228–234, September 2026.

Abstract

This study assessed the cybersecurity awareness and cybersecurity preventive practices among Criminal Justice students at the ICI College of Criminal Justice Education as the basis for developing an Evidence-Based Cyber Safety Education Framework. A descriptive-correlational research design using a quantitative approach was employed. The respondents consisted of 270 Criminal Justice students selected through stratified random sampling. Data were gathered using a researcher-made questionnaire consisting of measures of cybersecurity awareness and cybersecurity preventive practices. The instrument demonstrated excellent reliability, with Cronbach's Alpha coefficients of 0.978 for cybersecurity awareness and 0.970 for cybersecurity preventive practices. Frequency and percentage distribution, weighted mean, Pearson Product-Moment Correlation Coefficient, and Multiple Linear Regression Analysis were used in analyzing the data. The findings revealed very high cybersecurity awareness and high levels of cybersecurity preventive practices among the respondents. A significant strong positive relationship existed between cybersecurity awareness and cybersecurity preventive practices ($r = 0.842$, $p = 0.000$). Regression analysis further showed that all four dimensions of cybersecurity awareness significantly predicted cybersecurity preventive practices, with phishing and online scam awareness emerging as the strongest predictor. Based on the findings, an Evidence-Based Cyber Safety Education Framework was developed to address identified areas for improvement and strengthen cybersecurity preparedness among Criminal Justice students. The study supports SDG 4, Quality Education, through strengthened cybersecurity education and digital competency, and SDG 16, Peace, Justice and Strong Institutions, through improved cybercrime preparedness and responsible digital behavior. Its sustainability contribution is primarily educational, technological, institutional, and governance oriented.

Keywords: Cybersecurity Awareness; Cybersecurity Behavior; Cybersecurity Preventive Practices; Criminal Justice Students; Cyber Safety Education Framework

1. Introduction

Cybersecurity has become an important concern as digital technologies increasingly support communication, education, business, governance, and public services. Greater dependence on internet-connected systems has also increased exposure to phishing, identity theft, ransomware, online fraud, data breaches, malware, and unauthorized access. The World Economic Forum (2023) identified cyber insecurity as a major global risk, while the International Telecommunication Union (2023) emphasized the importance of cybersecurity awareness and responsible digital behavior in protecting users from evolving cyber threats. In the Philippines, cybersecurity has

become a national priority through initiatives such as Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 (Republic Act No. 10175, 2012) and the National Cybersecurity Plan 2023–2028 of the Department of Information and Communications Technology (DICT, 2024). Despite these initiatives, unsafe online behaviors and inadequate preventive practices continue to expose users to cybersecurity risks. Higher education students are particularly exposed because of their extensive use of online learning systems, social media, cloud applications, digital communication, and internet-based academic resources. Studies indicate that students may possess cybersecurity awareness while remaining inconsistent in applying secure behaviors, including strong password management, privacy protection, and verification of suspicious links (Alotaibi & Al-Saadi, 2022; Saleh & Al-Mulhim, 2024). Criminal Justice students are especially important because they are future law enforcement practitioners, investigators, corrections professionals, and public safety personnel who may handle digital evidence, confidential information, cybercrime investigations, and technology-related offenses. The International Criminal Police Organization (INTERPOL, 2023) and the United Nations Office on Drugs and Crime (UNODC, 2023) emphasized the increasing need for criminal justice professionals with appropriate digital and cybersecurity competencies.

The literature indicates that cybersecurity is both a technical and behavioral concern. Students' exposure to digital environments affects their perception of cyber risks and the effectiveness of cybersecurity education (Santelices, 2025). Interactive and game-based approaches can improve understanding of cyber risks and encourage safer practices (Kitaw Damenu et al., 2025), while increased cybersecurity knowledge may improve risk perception and responsible digital behavior (Ahamed et al., 2025). Research also demonstrates that awareness does not automatically result in secure behavior. Alotaibi and Al-Saadi (2022) found that students may understand common cyber threats but remain inconsistent in applying stronger security measures. Saleh and Al-Mulhim (2024) similarly identified a gap between cybersecurity knowledge and actual practices, emphasizing perceived risk and self-efficacy. Ahamed et al. (2025) and Fernandez and Tan (2025) further highlighted the importance of cybersecurity education, digital literacy, and institutional support. Within Criminal Justice education, cybersecurity competence is increasingly necessary because of the expanding role of digital technologies in investigation, digital evidence management, and cybercrime response (Commission on Higher Education [CHED], 2018). Practical training, simulation activities, curriculum integration, and institutional support have been identified as important mechanisms for strengthening cybersecurity competence (Yazon et al., 2022; Tick & Mai, 2024). Institutional policies and curriculum-based interventions are likewise important. Wijaya et al. (2025) emphasized institutional policies, resource allocation, faculty training, and stakeholder collaboration, while Espiritu and Jocson (2023) and Mahinay and Mamasalagat (2025) highlighted continuing challenges in cybersecurity awareness, enforcement, preparedness, and understanding of cybercrime protections. Evidence-based educational frameworks provide a structured means of aligning instructional interventions with empirical findings, assessment data, learner feedback, and measurable outcomes. Chen and Wang (2023), Kaur and Singh (2024), and Castillo and Navarro (2025) emphasized the value of data-driven evaluation, competency alignment, and continuous feedback in improving educational interventions.

Globally, increasing dependence on digital technologies has expanded cybersecurity risks and strengthened the need for responsible online behavior (World Economic Forum, 2023; International Telecommunication Union, 2023). Cybercrime continues to evolve, requiring criminal justice systems and professionals to develop appropriate digital competencies (INTERPOL, 2023; UNODC, 2023). Nationally, Philippine cybersecurity initiatives include the Cybercrime Prevention Act of 2012 (Republic Act No. 10175, 2012) and the National Cybersecurity Plan 2023–2028 (DICT, 2024). These measures seek to strengthen cyber resilience, prevention, governance, and public awareness. However, local studies indicate continuing challenges in cybersecurity awareness, enforcement, institutional preparedness, and understanding of cybercrime protections (Espiritu & Jocson, 2023; Mahinay & Mamasalagat, 2025). Within higher education, existing research has largely focused on general student populations and technology-related disciplines. Limited evidence specifically addresses the relationship between cybersecurity awareness and preventive practices among Criminal Justice students in the Philippine context.

The study is anchored on Protection Motivation Theory developed by Rogers (1975). The theory explains how individuals respond protectively when they recognize threats and perceive the need and ability to protect themselves. It involves threat appraisal, or assessment of the severity and likelihood of threats, and coping appraisal, or assessment of the effectiveness and feasibility of protective measures. In this study, cybersecurity awareness represents the independent variable and includes cyber threat awareness, password and account security awareness, privacy and information protection awareness, and phishing and online scam awareness. Cybersecurity preventive practices represent the dependent variable and include password management, online communication and social media practices, device and account security, and safe internet browsing. The study is also supported by the Knowledge–Behavior Perspective, which assumes that knowledge and awareness influence behavior. Together, these theoretical perspectives support the expectation that stronger cybersecurity awareness is associated with stronger preventive practices.

Existing studies have extensively investigated cybersecurity awareness, digital literacy, and online safety among university students, but comparatively fewer studies have examined Criminal Justice students as a distinct academic population. Existing literature also provides limited evidence concerning whether cybersecurity awareness translates into actual preventive practices within Criminal Justice education. Studies have identified a

continuing knowledge-behavior gap, with students sometimes demonstrating adequate knowledge while engaging in unsafe practices (Zhang et al., 2023). Local research has likewise focused more strongly on cybercrime awareness, legal frameworks, and public understanding than on the personal cybersecurity practices of Criminal Justice students. The present study therefore examines cybersecurity awareness and preventive practices among Criminal Justice students, determines their relationship, identifies the dimensions of awareness that predict preventive practices, and develops an evidence-based Cyber Safety Education Framework.

The study is naturally aligned with SDG 4 – Quality Education because it supports the strengthening of cybersecurity education, digital competencies, and student preparedness. It is also relevant to SDG 16 – Peace, Justice and Strong Institutions, particularly through its focus on Criminal Justice education, responsible digital behavior, cybercrime preparedness, information protection, and institutional cybersecurity governance.

The study contributes primarily to educational, technological, institutional, and governance sustainability. Its proposed framework provides an evidence-based basis for strengthening cybersecurity education and preventive behavior among future Criminal Justice professionals. It also supports institutional efforts to promote responsible digital practices, information protection, cybersecurity preparedness, and continuous educational improvement.

2. Material and methods

2.1 Research Design

The study employed a descriptive-correlational research design using a quantitative approach. The descriptive component determined the levels of cybersecurity awareness and cybersecurity preventive practices, while the correlational component examined the relationship between the two variables. The quantitative approach enabled the collection and statistical analysis of measurable data without manipulating the study variables. The design established associations and predictive relationships but did not establish causal relationships.

2.2 Locale of the Study

The study was conducted among Criminal Justice students at the ICI College of Criminal Justice Education during Academic Year 2025–2026.

2.3 Respondents of the Study

The study involved 270 Criminal Justice students. The population consisted of 754 students exposed to digital learning environments, online academic platforms, internet-based communication systems, and social media. The respondents represented first- through fourth-year students.

2.4 Sample and Sampling Procedure

Stratified random sampling was employed to provide proportional representation according to year level. The manuscript reports a computed sample size of 266 using Slovin's Formula with a 5% margin of error; however, 270 respondents participated during the actual data-gathering process. The final distribution consisted of 67 first-year, 51 second-year, 95 third year, and 57 fourth-year respondents.

2.5 Research Instrument

A researcher-made questionnaire was used. It contained 56 indicators divided equally between cybersecurity awareness and cybersecurity preventive practices. Cybersecurity awareness covered cyber threat awareness, password and account security awareness, privacy and information protection awareness, and phishing and online scam awareness. Preventive practices covered password management, online communication and social media practices, device and account security, and safe internet browsing. A five-point Likert scale was used. The questionnaire underwent face and content validation by experts in Criminal Justice, Information Technology, and quantitative research. A pilot test involving 30 students was conducted. Cronbach's Alpha yielded coefficients of 0.978 for cybersecurity awareness and 0.970 for cybersecurity preventive practices, both interpreted as Excellent Reliability.

2.6 Data Gathering Procedure

The researcher secured approval from the concerned authorities before conducting the study. Qualified respondents were informed of the purpose and objectives of the research, and participation was voluntary. The questionnaire was administered through Google Forms. Respondents were assured of confidentiality and anonymity. After collection, responses were automatically recorded and organized, then checked, tabulated, encoded, and prepared for statistical analysis. Ethical procedures included informed consent, voluntary participation, confidentiality, anonymity, and protection of respondents' information. The study also observed the Data Privacy Act of 2012 (Republic Act No. 10173).

2.7 Data Analysis Techniques

Frequency and percentage distribution were used to describe the respondents according to year level. Weighted mean was used to determine the levels of cybersecurity awareness and preventive practices. Pearson Product-Moment Correlation Coefficient was used to determine the relationship between cybersecurity awareness and

preventive practices. Multiple Linear Regression Analysis was used to determine which dimensions of cybersecurity awareness significantly predicted preventive practices. Hypotheses were tested at the 0.05 level of significance.

3. Results and Discussion

3.1 Cybersecurity Awareness

3.1.1 Cyber Threat Awareness

The respondents obtained a composite mean of 4.22, interpreted as Very High, for cyber threat awareness. Awareness of phishing, malware, ransomware, and identity theft obtained the highest mean of 4.31, while awareness of fake websites and deceptive advertisements obtained the lowest mean of 4.11, although it remained High. The findings indicate strong awareness of common cyber threats but comparatively lower awareness of sophisticated forms of online deception. This is consistent with Zhang et al. (2023) and Yazon et al. (2022), who reported substantial cybersecurity awareness among university students. The comparatively lower recognition of sophisticated threats supports the findings of Saleh and Al-Mulhim (2024), who noted that conceptual awareness does not always translate into the ability to identify complex online threats.

3.1.2 Password and Account Security Awareness

Password and account security awareness obtained a composite mean of 4.27, interpreted as Very High. Awareness of strong and unique passwords and securing online accounts obtained the highest mean of 4.40. Awareness of two-factor authentication and regular password updating obtained the lowest means of 4.10. The results suggest that respondents understood basic password protection but were comparatively less familiar with advanced and continuing account-security measures. Fernandez and Tan (2025) emphasized the importance of protecting credentials and personal information, while Alotaibi and Al-Saadi (2022) and Romero and Dela Cruz (2026) similarly found lower awareness or adoption of advanced measures such as multi-factor authentication and password updating.

3.1.3 Privacy and Information Protection Awareness

Privacy and information protection awareness obtained a composite mean of 4.22, interpreted as Very High. Protecting confidential information during online transactions and digital communications obtained the highest mean of 4.30. Awareness of public Wi-Fi risks obtained the lowest mean of 4.12. The results indicate strong general awareness of personal information protection, but comparatively lower awareness of risks associated with public networks, social media oversharing, and routine privacy management. The findings are consistent with Lund, Anderson, Roeschley, and Hossain (2025), who found that stronger privacy literacy is associated with greater awareness of personal information protection and privacy management.

3.1.4 Phishing and Online Scam Awareness

Phishing and online scam awareness obtained a composite mean of 4.26, interpreted as Very High. Awareness of scams requesting confidential personal or financial information obtained the highest mean of 4.32, while awareness of phishing techniques commonly used in online scams and cyber fraud obtained the lowest mean of 4.20. The findings show that respondents recognized common phishing and scam risks but were comparatively less familiar with the specific techniques used in sophisticated phishing activities. This supports Saleh and Al-Mulhim (2024), who reported that general awareness of phishing and online scams may not correspond to deeper understanding of how sophisticated attacks are executed.

3.2 Cybersecurity Preventive Practices

3.2.1 Password Management Practices

Password management practices obtained a composite mean of 4.28, interpreted as Always. Avoiding password sharing obtained the highest mean of 4.45, while regular password updating obtained the lowest mean of 4.08. The results indicate strong implementation of basic password protection practices. However, routine password updating and two-factor authentication were less consistently practiced. These findings are consistent with Alharbi et al. (2021), Du, Yang, and Liu (2023), and Goliath, Tsibolane, and Snyman (2024), which identified stronger implementation of basic password practices compared with some advanced account-security measures.

3.2.2 Online Communication and Social Media Practices

Online communication and social media practices obtained a composite mean of 4.34, interpreted as Always. Avoidance of suspicious online accounts, advertisements, and links obtained the highest mean of 4.42. Regular review and management of privacy settings obtained the lowest mean of 4.20 and was interpreted as Often. The findings indicate generally responsible online communication and social media behavior. However, privacy-setting management was less consistent. This supports Baleid (2026), Goliath, Tsibolane, and Snyman (2024), and Du, Yang, and Liu (2023), who emphasized that students may demonstrate responsible online interaction while remaining less consistent in routine privacy-management activities.

3.2.3 Device and Account Security Practices

Device and account security practices obtained a composite mean of 4.32, interpreted as Always. The use of passwords, PINs, or biometrics obtained the highest mean of 4.46, while antivirus or security software utilization obtained the lowest mean of 4.18 and was interpreted as Often. The findings demonstrate strong device and account protection practices but comparatively lower use of additional security software. Tick and Mai (2024) similarly reported positive device-protection behaviors among university students, while Dunder et al. (2025) and Ovi et al. (2025) identified less consistent implementation of additional or layered security measures.

3.2.4 Safe Internet Browsing Practices

Safe internet browsing obtained a composite mean of 4.35, interpreted as Always. Verification of website legitimacy before entering sensitive information obtained the highest mean of 4.42. Avoidance of public Wi-Fi during sensitive online transactions obtained the lowest mean of 4.19 and was interpreted as Often. The findings indicate that respondents generally practiced cautious internet browsing. However, public-network security was comparatively weaker. This is consistent with Al-Janabi and Al-Shourbaji (2016) and Tick and Mai (2024), who reported lower consistency in avoiding potentially unsafe network connections.

3.3 Relationship Between Cybersecurity Awareness and Preventive Practices

The Pearson Product-Moment Correlation analysis produced $r = 0.842$ with $p = 0.000$, indicating a statistically significant strong positive relationship between cybersecurity awareness and cybersecurity preventive practices. Consequently, the null hypothesis stating that there is no significant relationship between the two variables was rejected. The result indicates that respondents with higher cybersecurity awareness tended to demonstrate stronger preventive practices. This is consistent with Ahamed (2024), Gustara (2025), and Sittitiamjan (2025), whose findings associated cybersecurity knowledge and awareness with stronger protective online behavior. However, the relationship should not be interpreted as evidence that awareness alone automatically produces secure behavior because behavioral, motivational, technological, and environmental factors may also influence cybersecurity practices.

3.4 Predictors of Cybersecurity Preventive Practices

Multiple Linear Regression Analysis showed a strong relationship between the awareness dimensions and preventive practices, with $R = 0.861$ and $R^2 = 0.741$. The model therefore accounted for 74.1% of the variance in cybersecurity preventive practices. The adjusted R^2 was 0.736, while the F-value was 189.472 with $p = 0.000$, indicating that the regression model was statistically significant. All four cybersecurity awareness dimensions significantly predicted preventive practices. Phishing and online scam awareness was the strongest predictor ($\beta = 0.337$, $p = 0.000$), followed by password and account security awareness ($\beta = 0.314$, $p = 0.000$), cyber threat awareness ($\beta = 0.241$, $p = 0.000$), and privacy and information protection awareness ($\beta = 0.205$, $p = 0.001$). The results support the Knowledge–Behavior Perspective by demonstrating that cybersecurity awareness is significantly associated with preventive behavior. They also emphasize the importance of phishing detection, scam recognition, password security, cyber threat recognition, and privacy protection in cybersecurity education.

3.5 Evidence-Based Cyber Safety Education Framework

The proposed Evidence-Based Cyber Safety Education Framework was derived from the empirical findings. Although the respondents demonstrated very high cybersecurity awareness and consistently practiced preventive measures, comparatively lower results were observed in two-factor authentication, password updating, privacy-settings management, antivirus or security-software utilization, and avoidance of public Wi-Fi during sensitive transactions. The framework therefore emphasizes targeted interventions addressing these identified areas. These include phishing awareness campaigns, scam-detection workshops, cyber fraud simulations, two-factor authentication training, password-management programs, privacy and social-media security workshops, device-security and malware-prevention training, and safe internet-connectivity seminars. The framework also emphasizes continued integration of cyber safety activities into Criminal Justice programs and student-development initiatives.

4. Conclusion & Recommendations

The study concluded that Criminal Justice students demonstrated very high cybersecurity awareness across cyber threat awareness, password and account security awareness, privacy and information protection awareness, and phishing and online scam awareness. They also consistently practiced cybersecurity preventive measures involving password management, online communication and social media, device and account security, and safe internet browsing. A significant strong positive relationship existed between cybersecurity awareness and preventive practices, while all four awareness dimensions significantly predicted preventive practices, with phishing and online scam awareness emerging as the strongest predictor. Based on these findings, an Evidence-Based Cyber Safety Education Framework was developed to address identified areas for improvement and strengthen cybersecurity education, responsible digital behavior, and cybersecurity preparedness among Criminal Justice students.

The study recommends strengthening cybersecurity education within Criminal Justice programs through regular awareness activities, workshops, training, and practical interventions focusing on phishing detection, online scam prevention, password security, privacy protection, safe internet practices, two-factor authentication, security software, and public-network safety. Educational institutions may utilize the proposed Evidence-Based Cyber Safety Education Framework as a guide, subject to further validation and evaluation, while strengthening cybersecurity policies, technological safeguards, institutional coordination, and collaboration among administrators, faculty members, Information Technology personnel, and student-support units. Similar studies and further evaluation of the framework may also be conducted among other academic disciplines, institutions, and locations.

5. Compliance with ethical standards

The study complied with established ethical standards and research protocols. Prior approval was obtained from the concerned authorities of the ICI College of Criminal Justice Education before data collection. Respondents were informed of the study's purpose and nature, and their participation was voluntary, with the right to decline or withdraw at any time without penalty. Informed consent was secured prior to participation. The confidentiality and anonymity of respondents were strictly maintained, and no personally identifiable information was disclosed. The collected data were used solely for academic and research purposes and were accessible only to the researcher and authorized personnel. Data handling, storage, and processing also complied with the provisions of the Data Privacy Act of 2012 (Republic Act No. 10173).

REFERENCES

- Ahamed, B. (2024). Empowering students for cybersecurity awareness: Understanding the role of cybersecurity knowledge, password security, and self-perception of skills among university students. *SAGE Open*, 14(1). <https://doi.org/10.1177/21582440241228920>
- Ahamed, F., Rahman, M., & Karim, R. (2025). Cybersecurity awareness, social networking behavior, and online safety practices among Generation Z university students. *International Journal of Information Security and Privacy*, 19(1), 1–18. <https://doi.org/10.4018/IJISP.2025010101>
- Alharbi, T., Alshammari, R., Alenazi, M., Alghazzawi, D., & Cheng, L. (2021). Assessment of cybersecurity awareness among students and staff at Majmaah University. *Future Internet*, 13(2), 23. <https://doi.org/10.3390/fi13020023>
- Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. *Journal of Information and Knowledge Management*, 15(1), 1650007. <https://doi.org/10.1142/S0219649216500076>
- Alotaibi, F., & Al-Saadi, A. (2022). Cybersecurity awareness and safe online behavior among undergraduate students in Saudi Arabia. *Education and Information Technologies*, 27(8), 11245–11263. <https://doi.org/10.1007/s10639-022-11018-5>
- Baleid, H. M. (2026). Cybersecurity in higher education: A systematic review of threats, awareness, and protective practices. *Journal of Science and Technology*.
- Castillo, R., & Navarro, P. (2025). Iterative evidence collection and continuous feedback in digital learning environments. *Journal of Educational Innovation and Research*.
- Chen, L., & Wang, H. (2023). Formative assessment, student feedback, and evidence-based educational frameworks in digital learning. *Educational Assessment and Technology Journal*.
- Commission on Higher Education. (2018). CHED Memorandum Order No. 5, series of 2018: Policies, standards, and guidelines for the Bachelor of Science in Criminology program. Commission on Higher Education.
- Department of Information and Communications Technology. (2024). National cybersecurity plan 2023–2028. Department of Information and Communications Technology.
- Du, X., Yang, J., & Liu, Y. (2023). A survey of cybersecurity awareness among university students. In *Proceedings of the International Conference on Educational Technology and Information Systems*. Atlantis Press.
- Dunder, I., Seljan, S., & Odak, M. (2025). Information security awareness in the university environment: A focus on undergraduates. *TEM Journal*, 14(2), 1621–1628. <https://doi.org/10.18421/TEM142-59>
- Espiritu, P. G. G., & Jocson, J. C. (2023). Navigating cybersecurity challenges in the era of digital transformation: Threats and mitigation strategies in the Philippines. *International Journal of Progressive Research in Science and Engineering*, 4(11), 10–23.
- Fernandez, M., & Tan, J. (2025). Digital literacy and cybersecurity practices among college students in metropolitan universities. *Journal of Cybersecurity Education, Research and Practice*, 2025(1), 45–61.
- Goliath, S., Tsibolane, P., & Snyman, D. (2024). Exploring the cybersecurity-resilience gap: An analysis of student attitudes and behaviors in higher education. *arXiv*. <https://arxiv.org/abs/2411.03219>
- Gustara, M. (2025). Analysis of cybersecurity awareness and behavior among university students. *Indonesian Journal of Integrated Science Education*.

- International Criminal Police Organization. (2023). Annual report 2023. <https://www.interpol.int/en/Resources/Documents/Annual-Report-2023>
- International Telecommunication Union. (2023). Global cybersecurity index 2023. International Telecommunication Union.
- Kaur, P., & Singh, R. (2024). Competency-based education and evidence-based instructional frameworks in higher education. *International Journal of Educational Development*.
- Kitaw Damenu, T., Gökbay, İ. Z., Covaci, A., & Li, S. (2025). Cyber security educational games for children: A systematic literature review. *arXiv*. <https://doi.org/10.48550/arXiv.2508.17414>
- Lund, B. D., Anderson, B., Roeschley, A., & Hossain, G. (2025). Understanding the relationship between personal data privacy literacy and data privacy information sharing by university students. *Journal of Information Science*. <https://doi.org/10.1177/01655515251379049>
- Mahinay, J., & Mamasalagat, T. (2025). Cybercrime awareness and netizen experiences: The Philippine context. *International Journal of Research and Innovation in Social Science*, 9(9), 4339–4354.
- Ovi, T. R., Atikuzzaman, M., & Islam, M. M. (2025). Smartphone security behavior among university students: An empirical study in a public university in Bangladesh. *Global Knowledge, Memory and Communication*. <https://doi.org/10.1108/GKMC-11-2024-0804>
- Republic Act No. 10173, Data Privacy Act of 2012. (2012). Official Gazette of the Republic of the Philippines.
- Republic Act No. 10175, Cybercrime Prevention Act of 2012. (2012). Official Gazette of the Republic of the Philippines.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>
- Romero, R. M., & Dela Cruz, K. J. (2026). Technical self-efficacy and advanced identity protection practices among Filipino collegiate students. *Philippine Journal of Development Administration*, 31(1), 72–88.
- Saleh, A., & Al-Mulhim, N. (2024). Cybersecurity awareness, self-efficacy, and preventive online behavior among college students. *Computers & Security*, 137, 103620. <https://doi.org/10.1016/j.cose.2023.103620>
- Santelices, R. B. (2025). A students' perspective on cybersecurity awareness and education. *International Journal of Research and Innovation in Social Science*, 9(3S), 7976–7988.
- Sittitiamjan, K. (2025). Bridging the gap: How knowledge, attitudes, and practices shape cybersecurity awareness in Thai education. *European Journal of Educational Research and Practice*.
- Tick, A., & Mai, T. T. (2024). Cyber security awareness and the behaviors of higher education students using smartphones in Vietnam. *Acta Polytechnica Hungarica*, 21(12), 111–131.
- United Nations Office on Drugs and Crime. (2023). Education for justice (E4J) cybercrime module series. United Nations Office on Drugs and Crime.
- Wijaya, R. R., Putri, F. A., & Karya, S. (2025). Measuring employee information security awareness in personal data protection compliance. In *2025 1st International Conference on Emerging Trends in Information Systems and Informatics (ICETISI)*. IEEE. <https://doi.org/10.1109/ICETISI67983.2025.11405918>
- World Economic Forum. (2023). Global risks report 2023 (18th ed.). World Economic Forum.
- Yazon, A. D., Ang-Manaig, K., Tesoro, J. F., & Buama, C. A. (2022). Cyber literacy and cyber risk mitigation program of a municipal college in the Philippines. *International Journal of Advanced Research in Management and Social Sciences*, 11(3), 45–59.
- Zhang, Y., Gupta, B., & Kaur, P. (2023). Cybersecurity awareness and behavior: A systematic review of higher education studies (2021–2023). *Computers & Security*, 129, 103212.