ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 6 (June 2026)

Information Assurance and Security Knowledge as a Predictor of Cybersecurity Protection Practices Among BSIT Students

Michael R. Mades[1*], Rizza Mae Brao-Yruma[1,2], Anndrea Fatimah E. Fermin[1,3], Erwin B. Bautro[1,4], Joshua L. Nieves[1,5] and Joel San Pascual Jr.[1]
[1]*Colegio de Montalban, Rodriguez, Rizal, Philippines*
[*]*michael.mades@pnm.edu.ph*, [2]*rizza.mae.brao@pnm.edu.ph*, [3]*anndrea.fatimah.fermin@pnm.edu.ph*, [4]*erwin.bautro@pnm.edu.ph*, [5]*joshua.llave.nieves@pnm.edu.ph*

Date Submitted:
April 18, 2026

Date Accepted:
May 24, 2026

Date Published:
June 09, 2026

DOI:
10.5281/zenodo.20603065

ABSTRACT

Cybersecurity awareness and responsible online behavior are essential competencies among information technology students because of their extensive use of digital technologies and increasing exposure to cyber threats. This study examined the relationship between Information Assurance and Security (IAS) knowledge and cybersecurity protection practices among third-year Bachelor of Science in Information Technology (BSIT) students at Colegio de Montalban. A quantitative descriptive-correlational design was employed among 50 students enrolled in the Information Assurance and Security 2 course during Academic Year 2025-2026. Convenience sampling was used, and data were gathered through a researcher-developed online questionnaire validated by information technology instructors and research specialists. The instrument obtained a Cronbach's alpha coefficient of .979. Weighted mean, ranking, and Pearson product-moment correlation coefficient were used. Respondents demonstrated a high level of IAS knowledge ($M = 3.31$) and strong cybersecurity protection practices ($M = 3.27$). Confidentiality, Integrity, and Availability received the highest IAS-knowledge mean ($M = 3.32$), while Malware Awareness received the lowest ($M = 3.28$). Phishing Awareness and Response ranked highest among cybersecurity protection practices ($M = 3.33$), whereas Safe Browsing Practices and Device Security Practices received the lowest means ($M = 3.24$ each). IAS knowledge had a statistically significant and very strong positive relationship with cybersecurity protection practices, $r(48) = .95$, $p < .001$. The findings support the continued strengthening of cybersecurity instruction through laboratory activities, simulations, practical exercises, institutional awareness programs, and curriculum review. Because the measures were self-reported and the sample was limited to one institution, the results should be interpreted within the defined scope of the study.

Keywords: *BSIT students, cybersecurity awareness, cybersecurity protection practices, digital citizenship, Information Assurance and Security, phishing awareness*

INTRODUCTION

Digital technologies have transformed how individuals communicate, learn, work, and manage information. Higher education institutions increasingly use learning-management systems, cloud services, collaboration platforms, social media, and virtual learning environments. These systems improve access and efficiency but also increase exposure to phishing attacks, malware infections, data breaches, identity theft, ransomware, and other forms of cybercrime.

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 6 (June 2026)

Human behavior remains a critical factor in cybersecurity. Even when technical safeguards are available, users may remain vulnerable because of weak passwords, unsafe browsing, inappropriate disclosure of personal information, failure to update devices, or an inability to recognize social-engineering attacks. University students are particularly exposed because they frequently use personal devices, institutional systems, email, cloud storage, and social-networking platforms for academic and personal purposes.

Information Assurance and Security focuses on protecting information and information systems from unauthorized access, modification, disclosure, disruption, or destruction. Its foundational concepts include Confidentiality, Integrity, and Availability; malware awareness; authentication and access control; and data protection and privacy. BSIT students are expected to understand these principles and apply them in their daily digital practices as future information-technology professionals.

Previous studies have emphasized the importance of cybersecurity education. Alharbi and Tassaddiq (2021) reported that university students may understand basic cybersecurity concepts while still demonstrating gaps in secure behavior. Alqahtani (2022) found that password, browser, and social-media security influence student cybersecurity awareness. Fattah et al. (2023) likewise emphasized the role of knowledge, attitudes, behaviors, and training in cybersecurity awareness. Despite the growing literature, limited local evidence has examined whether knowledge gained through formal IAS coursework is associated with cybersecurity protection practices among BSIT students. This study therefore assessed students' IAS knowledge, described their cybersecurity protection practices, examined the relationship between the two variables, and developed evidence-based recommendations for cybersecurity education.

Literature Review

Information Assurance and Security

Information Assurance and Security encompass the policies, technologies, procedures, and user practices used to protect digital information. The Confidentiality, Integrity, and Availability framework provides the basic foundation for protecting data from unauthorized disclosure, inappropriate modification, and disruption of access. Authentication, access control, data privacy, and risk recognition strengthen the practical application of these principles.

Cybersecurity Protection Practices

Cybersecurity protection practices refer to the behaviors individuals use to protect accounts, devices, personal information, and digital resources. These behaviors include strong and unique passwords, multi-factor authentication, safe website verification, careful downloading, responsible social-media use, software updates, device protection, and the ability to recognize and respond to phishing attempts. Khader et al. (2021) emphasized the importance of cybersecurity-awareness frameworks within academic environments because human factors remain an important source of cybersecurity vulnerability.

Cybersecurity Awareness Among University Students

Cybersecurity awareness involves both knowledge and behavioral application. Alharbi and Tassaddiq (2021) found that awareness gaps remained among university students. Alqahtani (2022) reported that password security, browser security, and social-media security contributed to cybersecurity-awareness levels. Fattah et al. (2023) further explained that education and training opportunities can strengthen students' cybersecurity awareness and practices.

Knowledge and Protective Behavior

The source manuscript anchored the study in the Knowledge-Attitude-Behavior model, which assumes that increased knowledge supports the development of appropriate attitudes and behaviors. Within cybersecurity education, the model suggests that students who understand threats and protection strategies are more likely to apply secure online practices. Ahamed et al. (2026) reported an association between cybersecurity knowledge and online behavior among Generation Z university students, reinforcing the importance of cybersecurity education.

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 6 (June 2026)

METHODS

Research Design

The study employed a quantitative descriptive-correlational design. The descriptive component determined the respondents' IAS knowledge and cybersecurity protection practices. The correlational component examined the strength and direction of the relationship between the two variables without establishing causation.

Research Locale

The study was conducted at Colegio de Montalban in Rodriguez, Rizal, Philippines. The respondents were third-year BSIT students enrolled in Information Assurance and Security 2 during Academic Year 2025-2026.

Participants and Sampling Technique

The target population consisted of 230 third-year BSIT students enrolled in the IAS 2 course. A total of 50 students participated. Convenience sampling was employed based on accessibility, availability, and willingness to participate. The source manuscript appropriately recognizes that this non-probability sampling technique limits the generalizability of the findings.

Research Instrument

A researcher-developed questionnaire was used. The IAS-knowledge section assessed Confidentiality, Integrity, and Availability; Malware Awareness; Authentication and Access Control; and Data Protection and Privacy. The cybersecurity-protection-practices section assessed Password Management Practices, Safe Browsing Practices, Social Media Security Practices, Device Security Practices, and Phishing Awareness and Response.

The items were rated using a four-point scale: 3.26-4.00, Strongly Agree; 2.51-3.25, Agree; 1.76-2.50, Disagree; and 1.00-1.75, Strongly Disagree. The forced-choice scale was intended to minimize neutral responses.

Validity and Reliability

Information technology instructors and research specialists reviewed the instrument for clarity, relevance, appropriateness, and alignment with the study objectives. The instrument obtained a Cronbach's alpha coefficient of .979, indicating excellent internal consistency.

Data Gathering Procedure

The researchers informed respondents of the objectives, procedures, and significance of the study. After informed consent was secured, the questionnaire was administered electronically through Google Forms. The responses were reviewed, encoded, organized, and prepared for analysis.

Data Analysis

Weighted mean was used to summarize IAS knowledge and cybersecurity protection practices. Ranking was used to identify the relative standing of dimensions and indicators. Pearson product-moment correlation coefficient was used to determine the relationship between IAS knowledge and cybersecurity protection practices at the .05 level of significance.

Ethical Consideration

Participation was voluntary, and informed consent was obtained before data collection. No personally identifiable information was collected. Responses were kept confidential, securely stored, and reported only in aggregate form.

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 6 (June 2026)

RESULTS AND DISCUSSION

Information Assurance and Security Knowledge

Table 1. *Overall Level of Information Assurance and Security Knowledge*

IAS Knowledge Dimension	Weighted Mean	Interpretation	Rank
Confidentiality, Integrity, and Availability	3.32	Strongly Agree	1
Authentication and Access Control	3.315	Strongly Agree	2
Data Protection and Privacy	3.31	Strongly Agree	3
Malware Awareness	3.28	Strongly Agree	4
Grand mean	3.31	Strongly Agree	

The respondents demonstrated a consistently high level of IAS knowledge, with a grand mean of 3.31. Confidentiality, Integrity, and Availability ranked first (M = 3.32), while Malware Awareness ranked last (M = 3.28). The narrow range of scores indicates balanced foundational knowledge across the four dimensions.

Table 2. *Selected IAS-Knowledge Indicators Requiring Continued Reinforcement*

Domain	Selected Indicator	Weighted Mean	Interpretation
CIA principles	Identifying situations where CIA principles may be compromised	3.24	Agree
Malware awareness	Identifying different types of malwares	3.18	Agree
CIA principles	Keeping information confidential from unauthorized users	3.44	Strongly Agree
Malware awareness	Understanding how malware infects devices	3.38	Strongly Agree

The item-level findings identify practical improvement areas. Students reported strong understanding of confidentiality and malware-infection pathways, but their ratings were lower for recognizing situations in which CIA principles could be compromised and identifying different malware types. Practical risk-identification activities may help strengthen these competencies.

Cybersecurity Protection Practices

Table 3. *Overall Level of Cybersecurity Protection Practices*

Cybersecurity Protection-Practice Dimension	Weighted Mean	Interpretation	Rank
Phishing Awareness and Response	3.33	Strongly Agree	1
Social Media Security Practices	3.29	Strongly Agree	2
Password Management Practices	3.27	Strongly Agree	3
Safe Browsing Practices	3.24	Agree	4.5
Device Security Practices	3.24	Agree	4.5
Grand mean	3.27	Strongly Agree	

The respondents demonstrated strong cybersecurity protection practices, with a grand mean of 3.27. Phishing Awareness and Response received the highest mean (M = 3.33), while Safe Browsing Practices and Device Security Practices shared the lowest mean (M = 3.24). The results suggest that students were capable of recognizing phishing threats but would benefit from continued reinforcement of browsing, device, and network-security practices.

ISSN: 3116-3475
International Journal
of Education, Research, and Innovation Perspectives
Volume 2 Issue 6 (June 2026)

Relationship Between IAS Knowledge and Cybersecurity Protection Practices

Table 4. *Pearson Correlation Between IAS Knowledge and Cybersecurity Protection Practices*

Variables	Pearson r	p-value	Interpretation	Decision
IAS knowledge and cybersecurity protection practices	.95	< .001	Very strong positive relationship	Reject H0

Pearson correlation analysis revealed a statistically significant and very strong positive relationship between IAS knowledge and cybersecurity protection practices, $r(48) = .95$, $p < .001$. The null hypothesis was rejected. Students who reported stronger cybersecurity knowledge also reported stronger cybersecurity-protection behaviors.

The very high coefficient should be interpreted carefully. Both variables were measured using the same self-report questionnaire and similar response formats, which may increase common-method bias. The cross-sectional correlational design also does not establish causation. Objective skills tests, behavioral observations, or simulated phishing activities would strengthen future validation.

Proposed Cybersecurity Education Enhancement Plan

Table 5. *Proposed Cybersecurity Education Enhancement Priorities*

Priority Area	Objective	Recommended Activities	Expected Outcome
Malware classification and response	Strengthen recognition of malware types and infection pathways.	Hands-on malware-identification cases and guided incident-response activities	Improved threat-recognition skills
CIA risk identification	Improve recognition of confidentiality, integrity, and availability risks.	Scenario-based exercises and case analysis	Stronger practical application of IAS principles
Safe browsing and network security	Reinforce careful website verification, downloading, and public-network use.	Browser-security checklists and simulated risky-link activities	Safer browsing behavior
Device security	Strengthen update, backup, access-control, and protection routines.	Device-hardening laboratory exercises and security-audit checklists	Improved device resilience
Phishing simulations	Sustain the strongest practice area through applied testing.	Periodic phishing-recognition simulations and reflective debriefing	Improved response to social-engineering threats
Institutional awareness	Extend cybersecurity education beyond IAS courses.	Seminars, digital-safety campaigns, and peer-led awareness activities	Stronger institutional cybersecurity culture

CONCLUSION

Third-year BSIT students at Colegio de Montalban demonstrated a high level of IAS knowledge and strong cybersecurity protection practices. Confidentiality, Integrity, and Availability emerged as the strongest IAS-knowledge dimension, while Malware Awareness remained the lowest-rated dimension. Phishing Awareness and Response emerged as the strongest cybersecurity-protection practice, whereas Safe Browsing and Device Security received the lowest ratings. IAS knowledge was significantly and positively associated with cybersecurity protection practices. These findings support continued cybersecurity education that combines conceptual knowledge with simulations, laboratory exercises, practical risk-identification activities, and institutional digital-safety initiatives. The results should remain limited to the study setting because the sample was small, convenience-based, and reliant on self-reported perceptions.

Recommendations

1. Faculty members may integrate scenario-based activities, cyber-threat case studies, simulations, and laboratory exercises into IAS courses to strengthen practical cybersecurity application.
2. Students may receive additional activities on malware classification, CIA-risk identification, safe browsing, device hardening, network security, backups, and software updates.
3. Higher education institutions may conduct cybersecurity-awareness campaigns, seminars, and digital-safety programs for the broader academic community.
4. Curriculum developers may review IAS-related course content regularly to maintain alignment with emerging cyber threats, industry standards, and technological developments.
5. Future researchers may use larger samples, probability sampling, multiple institutions, objective knowledge tests, behavioral measures, simulated phishing exercises, and longitudinal or mixed-method designs.
6. The authors may verify the questionnaire's subscale reliability coefficients and examine common-method bias before final journal submission because both major variables were assessed through the same self-report instrument.

References

Ahamed, B., Polas, M. R. H., Falahat, M., & Karim, R. (2026). Cybersecurity knowledge, social networking, and awareness among Gen Z university students. Discover Education, 5, Article 77.

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2), Article 23.

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

Bottyan, L. (2023). Cybersecurity awareness among university students. Journal of Applied Technical and Educational Sciences, 13(3).

Creswell, J. W., & Creswell, J. D. (2023). Research design: Qualitative, quantitative, and mixed methods approach (6th ed.). SAGE Publications.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. American Journal of Theoretical and Applied Statistics, 5(1), 1-4.

Fattah, A., Wagimin, & Nurlia. (2023). Enhancing cybersecurity awareness among university students: A study on the relationship between knowledge, attitude, behavior, and training. JSI: Jurnal Sistem Informasi, 15(1), 3139-3149.

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

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. Information, 12(10), Article 417.

Taherdoost, H. (2022). What is the best response scale for survey and questionnaire design? Review of different lengths of rating scale, attitude scale, and Likert scale. International Journal of Academic Research in Management, 11(1), 1-10.