Journal of Critical Social Sciences and Review (JCSSR)

RESEARCH ARTICLE
VOLUME NO. 1, ISSUE NO. 1, 2026 (MARCH)

The Human Firewall: Evaluation of Cybersecurity Awareness Among Students of Bulacan State University

Boris Palao[1], Niño Andrea Cruz[2], Gillian Lhord Lualhati[3], Emmanuel Pascual[4*], John Maverick Santos[5]

[1]*Engineering Department, Faculty, Bulacan State University, Philippines*
[234*5]*Engineering Department, Student, Bulacan State University, Philippines*

Received: 03/23/2026 Revised: 03/25/2026 Accepted: 03/27/2026 Published: 03/30/2026

ABSTRACT

In the age of swift digital transformation, the number and complexity of cyberattacks have reached bizarre levels, targeting individuals and organizations alike. This study evaluates the level of cybersecurity awareness and extent of cybersecurity education among students of Bulacan State University, focusing on their demographic profile in terms of gender, academic year level, and internet access devices, while also studying the relationship between awareness and education. Using a quantitative research design, 75 students were surveyed through a structured questionnaire adopted from established research instruments, using a 5-point Likert scale. Descriptive and inferential were used to analyze data, with results showing a high level of cybersecurity awareness and education among students. Results show that female students have slightly higher levels of cybersecurity education compared to male students. However, a gap remains in the day-to-day practices of students' security habits, specifically regarding secure password implementation and cautiousness with suspicious links. While the gender gaps were small, they highlighted the need for consistent practice and greater technical confidence. Correlation analysis also shows a strong positive correlation ($r = 0.648$, $p < 0.01$) between cybersecurity awareness and education, highlighting the impact of previous structured learning on students' protective behaviors. The study concludes that effective cybersecurity education initiatives that are included in the curriculum are crucial in giving students the information and abilities they need to identify, prevent, and react to cyberthreats. These results have important implications for institutions of higher learning, emphasizing the value of developing a digitally resilient culture that equips students to securely and responsibly navigate the complexity of today's evolving digital world

Keywords: Cyberattacks, Cybersecurity Awareness, Cybersecurity Education, Bulacan State University, Protection Motivation Theory

Corresponding Author: **Emmanuel P. Pascual*
E-mail address: emmanmaja12@gmail.com

INTRODUCTION

In the age of swift digital transformation, the number and complexity of cyberattacks have reached bizarre levels, targeting individuals and organizations alike. A cyber- attack is an intentional and malicious effort made by a person or an organization to break the information system of others (Mtair & AL-Hawamleh, 2023). The growth of cyber- attack, which continually advances new attack types, tools, and techniques that allow attackers to infiltrate more complex or well-controlled environments and produce more damage and even remain untraceable (Li & Liu, 2021). Cyberattacks are the world's biggest threat to commerce when it comes to criminal growth (Viraja et al, 2021). Despite the benefits of the advancement of technology, people are more vulnerable to cyberattacks.

Despite the growing level of cyber-attacks, many people are still vulnerable because they are unable to distinguish the signs of a breach or have an inadequate technical vocabulary to identify the threats. Malware is a common tool for performing these attacks in cyberspace, undeniably leading to damages, physical and/or economic, and there have been cases where the damages were so widespread and severe (Mtair & AL- Hawamleh, 2023). According to a study, usually students aged between 20 to 26 are using the internet for extended periods of time for browsing, downloading, and uploading information. As a result, they are a more vulnerable state for cyber-attacks (Rajeswari Raju et al, 2022). The more the public uses the internet and shares data, the more it's dangerous to lack awareness about the dangers of cyber-attacks (Klein et al, 2020).

The recent studies (Rajeswari Raju et al., 2022; Klein et al., 2020) indicate that due to the growing use of the internet, students are more vulnerable to cyberattacks. According to one study, it was found that cybersecurity awareness and education are positively correlated, which suggests that educational mediation would enhance the capability of students to identify and respond to cyberattacks (Santelices, 2025; Raju, 2022). There are still gaps in students' academic understanding. They must be practical, especially when it comes to maintaining passwords and conscious suspicious connections (Chou, 2021). Research indicates that cybersecurity awareness does not correlate with the year of study of the students, suggesting that a selective educational intervention is needed in the instructional process.

Research Gap(s)

Cyberattacks target higher educational institutions, making cybersecurity awareness and resilience a need for students. However, insufficient research exists on cybersecurity awareness, attitudes, and resilience among students in higher education.

Theoretical Framework

A foundational framework for understanding why individuals accept or reject security measures is Protection Motivation Theory (PMT). PMT was first created to forecast health-related behaviors, but it has been successfully modified for cybersecurity to examine how users react to

online dangers (Boss et al., 2023; Marikyan & Papagiannidis, 2023). Rough Set Theory is applied to address the problem of classifying cyber-attacks within network security (Amin et al, 2015). Building an effective human firewall requires more than just theoretical knowledge. According to the Instance-Based Learning Theory (IBLT), the accumulation of diverse, real-world events is retained in memory, which builds cognitive ability to identify anomalies, such as phishing emails (Dutt et al., 2012). When a student comes across a possible threat, the brain uses similar examples from the past to assess the current circumstance. A student lacks the instances necessary to identify risks in the actual world if their education is limited to just lectures. The Cyber Kill Chain becomes a crucial teaching tool in this situation. The structure, which was created by Lockheed Martin (n.d), divides an attack into seven separate stages: Command and Control, Reconnaissance, Weaponization, Delivery, Exploitation, Installation, and Actions on Objectives. Institutions can efficiently use IBLT by training students to break the chain as early as possible, especially during the "Delivery" stage, where human interaction is typically required. Before the "Exploitation" stage can start, students receive the cognitive instances necessary to identify and neutralize threats by simulating the delivery of harmful payloads.

Objectives

This study aims to evaluate the level of cybersecurity awareness and the extent of cybersecurity education among students of Bulacan State University. Specifically, this study seeks to answer the demographic profile of the students, their level of cybersecurity awareness, their extent of cybersecurity education, and whether there is a significant relationship between awareness and education.

METHODOLOGY

Research Design

The study employs a quantitative descriptive research design. The method is applicable for the study as the main goal is to provide an accurate description of the level of cybersecurity awareness of students and perceptions regarding common cyber-attacks. The researchers gathered primary data directly from the participants to ensure current and context-specific insights.

Participants and Sampling Technique

The target population of this study was currently enrolled students of Bulacan State University for the Academic Year 2025-2026. A sample size of 75 students was utilized. The researchers used convenience sampling, allowing participants to be chosen based on availability.

Instrument

The instrument utilized is a structured survey questionnaire composed of 4 sections: Informed Consent and Introduction, Demographic Information, Cybersecurity Awareness, and Cybersecurity Education.

Data Gathering Procedure

The researchers digitally distributed the survey questionnaire to the students of Bulacan State University using Google Forms. The questionnaire utilized closed and 5-point Likert-scale questions.

Data Analysis Procedure

The data was analyzed using frequency and percentage for demographics. The weighted mean and verbal interpretation were the primary tools for assessing awareness and education levels. ANOVA was utilized to compare groups across gender, academic year level, and device usage.

Ethical Consideration

Throughout the whole research process, strict ethical guidelines were followed, especially when it came to the use of human subjects. Before accessing the survey, participants had to complete an informed consent form that made sure they understood the goal of the study and their right to withdraw at any time. All gathered primary data was anonymized in accordance with the Data Privacy Act of 2012 and safely kept in secure digital lockers that were only accessible by the primary researchers. This ensured confidentiality and prevented unwanted data access.

RESULTS

Demographic Profile

The respondents are fairly balanced, with 41 males (55%) and 34 females (45%). Third-year students contribute the largest segment with 39% (29 students), followed by second-year students with 28% (21 students), first-year students with 20% (15 students), and fourth-year students with 13% (10 students). Regarding internet access, 97% of the students use mobile phones.

Table 1

Summary of Cybersecurity Awareness and Education Levels

Variable	General Weighted Mean	Qualitative Interpretation
Cyber Awareness (Overall)	**4.52**	**Strong Agree**
Highest: Recognition of phishing/malware	4.6	Strong Agree
Lowest: Cautiosness with links/passwords	4.4	Strong Agree
Cybersecurity Education (Overall)	**4.3**	**Strong Agree**
High: Desire for real-world applications	.4.6	Strong Agree
Lowest: Perceived effectiveness of training	3.7	Agree

Level of Cybersecurity Awareness

Table 1 shows that overall cybersecurity awareness of students yielded a general weighted mean of 4.52, which can be interpreted as "Strongly Agree". Across all year levels and internet access devices, awareness levels are relatively consistent. Attributes regarding the recognition of phishing emails, understanding malware, and knowledge of data privacy received the highest weighted mean of 4.6. On the other hand, attributes regarding to real-world applications, such as cautiousness with suspicious links (4.4) and using secure passwords (4.3) received a lower weighted mean.

Level of Cybersecurity Education

Students have a positive perception of their cybersecurity education with an overall mean of 4.3, which can be interpreted as "Strongly Agree". According to the findings, female students are more educated about cybersecurity than male students. Additionally, when it comes to cybersecurity education, students in the higher year levels demonstrate increased response scores regarding cybersecurity education. Attributes regarding to previous formal cybersecurity education scored lower at 3.6 to 3.7. On the other hand, attributes related to the necessity for practical, real-world application and digital citizenship scored higher with 4.6 to 4.7.

Table 2

Relationship Between Cybersecurity Awareness and Education

Correlations

			Awareness	Education
Spearman's rho	Awareness	Correlation Coefficient	1.000	.648**
		Sig. (2-tailed)	.	.000
		N	75	75
	Education	Correlation Coefficient	.648**	1.000
		Sig. (2-tailed)	.000	.
		N	75	75

**. Correlation is significant at the 0.01 level (2-tailed).

Table 2 presents that cybersecurity awareness and education have a significant positive correlation ($r = 0.648$, $p<0.01$). According to the findings, female students and students in the higher year levels indicated slightly higher levels of previous cybersecurity education. This strong correlation extends current literature by proving that structured formal education directly improves danger recognition abilities in university settings. It is clear from translating this to Instance-Based Learning Theory that students' cognitive capacity to recognize and prevent cyberattacks improves in accordance with the number of educational experiences or exposures to cybersecurity ideas they received throughout their academic career.

DISCUSSIONS

Interpretation of the Current Cybersecurity Landscape

Gender does not appear to have a significant effect on general cybersecurity awareness in this context, as seen by the small variances in the general weighted mean across variables. Similarly, general cybersecurity awareness is not greatly impacted by the kind of gadget used to access the internet. However, given that 97% of students use mobile phones, it is imperative to raise awareness of the particular risks associated with mobile devices.

The findings show an obvious gap between theoretical knowledge and real-world application. Although students showed a strong theoretical understanding of malware and data privacy (4.6), their daily security habits, such as using secure passwords (4.3) and avoiding suspicious links (4.4), still remain vulnerable. By showing that students need further assistance with their operational digital hygiene even when they have the technical language to recognize threats, this finding immediately fills the research gap. These findings are in line with Protection Motivation Theory (PMT), which suggests that although students recognize the severity of cyberthreats, improvements are still necessary to increase their self-efficacy in carrying out preventive behavioral actions. This also aligns with the previous comparison studies, such as Zwilling et al. (2020), in which they discovered that strong theoretical knowledge does not always translate into secure behavioral practices.

The "Knowing-Doing" Gap in Digital Hygiene

A critical synthesis of findings shows that students have a significant "knowing-doing" gap, also known as the intention-behavior gap (Zou et al., 2023). The lower scores found in practical implementation, such as password security (4.3) and avoiding suspicious links (4.4), contrast dramatically with the high weighted mean for theoretical concepts, such as understanding of malware and data privacy (4.6). The difference is a clear example of cognitive conflict that is frequently present in contemporary academic settings that rely heavily on technology. Students have a fundamental understanding of how online systems function because they are constantly exposed to digital tools. However, demanding everyday practices are not often the result of this theoretical mastery.

The concept of cognitive fatigue, more especially security fatigue, can be used to explain this occurrence (Stanton et al., 2016). Constant verification and data exchange are necessary when navigating challenging academic assignments, using many digital platforms for cooperation. Students may prioritize convenience over security by recycling passwords or ignoring security alerts in an attempt to lessen digital barriers (Stanton et al., 2016). As a result, the vulnerability is not a lack of consciousness but rather a gradual decline in alertness. In order to address this, educational intervention must concentrate on simplifying how to easily protect against cyberattacks using tools like password managers and automatic multi-factor authentication (MFA).

Impact of Education Intervention

A strong positive correlation ($r = 0.648$) between cybersecurity awareness and education demonstrates the critical role that education programs play in improving threat recognition. According to the data, students in the higher year levels reported having received more cybersecurity education, which is consistent with greater awareness. By demonstrating that formal, structured education directly improves danger recognition abilities in academic settings, this strong correlation adds to the body of existing research. By connecting this to Instance-Based Learning

Theory, it is clear that students' cognitive capacity to recognize and prevent cyberattacks develops in accordance with the number of educational instances or real-world exposures to cybersecurity concepts they receive throughout their academic careers. The necessity of switching from solely theoretical lectures to practical, simulation-based training techniques is further emphasized by the respondents' strong demand for real-world application (4.7).

CONCLUSIONS

Summary and Recommendations

The majority of responders are mobile-centric, according to the results, indicating that vulnerabilities are more likely to arise from mobile-specific attacks than from conventional desktop threats. Although students show strong awareness of the main threats, there remains a gap in their daily security practices, particularly in using secure passwords and avoiding suspicious links. The strong correlation between education and awareness, which relies on the Protection Motivation Theory, suggests that students need practical, experience-based training to develop real digital resilience rather than just theoretical precautions.

Certain policy initiatives must be implemented in order to improve the students' readiness. To create early defensive behaviors, it is advised that the university administration require a specialized, one-unit practical cybersecurity hygiene course to be incorporated into the first-year curriculum. Additionally, network administrators should implement automated password rotation procedures for student portals across the whole university and start concentrated awareness efforts about the risks associated with unprotected campus networks and mobile device security, since most students are mobile-centric.

However, the results' applicability to other degree programs or the overall university population may be limited by the convenience sample of 75 students, which could introduce response bias. Furthermore, perceived awareness rather than real technical proficiency under attack situations can be measured by using self-reported survey data. By going beyond questionnaires and implementing empirical, practical testing, such as campus-wide simulated phishing attacks or digital hygiene inspections, to see how students actually apply their theoretical knowledge in real-time threat scenarios, future research should expand these findings.

Author Contributions

Author's 1 initials: B.P Author's 2 initials: N.A.C Author's 3 initials: G.L.L Author's 4 initials: E.P.P Author's 5 initials: J.M.S

Conceptualization: Boris Palao, Nino Andrea A. Cruz, Gillian Lhord D. Lualhati, Emmanuel P. Pascual, John Maverick Y. Santos
Software: Emmanuel P. Pascual
Validation: Boris Palao, Emmanuel P. Pascual
Formal Analysis: Boris Palao, Nino Andrea A. Cruz, Gillian Lhord D. Lualhati, Emmanuel P. Pascual, John Maverick Y. Santos
Data Curation: Nino Andrea A. Cruz, Gillian Lhord D. Lualhati, Emmanuel P. Pascual, John Maverick Y. Santos
Preparation of the original draft: Nino Andrea A. Cruz, Gillian Lhord D. Lualhati, Emmanuel P. Pascual, John Maverick Y. Santos
Drafting-Revision and Editing: Boris Palao, Nino Andrea A. Cruz, Gillian Lhord D. Lualhati, Emmanuel P. Pascual, John Maverick Y. Santos

Visualization: Boris Palao, Nino Andrea A. Cruz, Gillian Lhord D. Lualhati, Emmanuel P. Pascual, John Maverick
Y. Santos
Supervision: Boris Palao, Emmanuel P. Pascual

Declaration of Generative AI Utilization

During the preparation of this manuscript, the authors used Gemini AI. The tool was used solely to improve clarity, grammar, and overall readability. The authors reviewed and revised the output as necessary and take full responsibility for the content of the manuscript.

Funding

No funding was received for this study.

REFERENCES

A Comprehensive Review on Cyber-Attacks in Power Systems: impact analysis, Detection, and Cyber Security. (2024). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/10418207

Al-Hawamleh, A. M. (2023). Predictions of cybersecurity experts on future Cyber-Attacks and related cybersecurity measures. International Journal of Advanced Computer Science and Applications, 14(2). https://doi.org/10.14569/ijacsa.2023.0140292

Arpaci, I., Aslan, O., & Oner, I. E. (2025). Cybersecurity Awareness Scale (CSAS) for Social Media Users: Development, Validity and Reliability study. Information Development. https://doi.org/10.1177/02666669251336562

Aslan, Ö., Aktuğ, 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. https://doi.org/10.3390/electronics12061333

Chou, T., & Mohammed, T. (2024). Self-assessment of knowledge levels in the subjects of cyber attacks and defense in a Cybersecurity Awareness Education workshop. 2021 ASEE Virtual Annual Conference Content Access Proceedings. https://doi.org/10.18260/1-2--37705

Classification of cyber attacks based on rough set theory. (2015, November 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/7351952

Cyber Kill chain. (n.d.-a). Lockheed Martin. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Goliath, S., Tsibolane, P., & Snyman, D. (2025). Exploring the Cybersecurity-Resilience Gap: An analysis of student attitudes and behaviors in higher education. In Communications in computer and information science (pp. 185–195). https://doi.org/10.1007/978-3-032-09660-9_19

Koduru, S. S., Machina, V. S. P., & Madichetty, S. (2023). Cyber Attacks in Cyber-Physical Microgrid Systems: A Comprehensive review. Energies, 16(12), 4573. https://doi.org/10.3390/en16124573

Lejarraga, T., Dutt, V., & Gonzalez, C. (2010). Instance-based learning: a general model of repeated binary choice. Journal of Behavioral Decision Making, 25(2), 143–153. https://doi.org/10.1002/bdm.722

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. https://doi.org/10.1016/j.egyr.2021.08.126

Marikyan, D., & Papagiannidis, S. (2023, August 1). Protection Motivation Theory: A review. University of Bristol. https://research-information.bris.ac.uk/en/publications/protection-motivation-theory-a-review/

Memon, M. A., Thurasamy, R., Ting, H., & Cheah, J. (2025). Convenience sampling: a review and guidelines for quantitative research. Journal of Applied Structural Equation Modeling, 9(2), 1–15. https://doi.org/10.47263/jasem.9(2)01

Navarra, L. W. (2025). The national security concerns of the Philippines: A students' perspective. Pantao, International Journal of the Humanities and Social Sciences, 4(4). https://doi.org/10.69651/pijhss0404541

Raju, R., Rahman, N. H. A., & Ahmad, A. (2022). Cyber Security Awareness in Using Digital Platforms Among Students in A Higher Learning Institution. Asian Journal of University Education, 18(3). https://doi.org/10.24191/ajue.v18i3.18967

Santelices, R. B. (2025). A Students' perspective on cybersecurity awareness and education. International Journal of Research and Innovation in Social Science, IX(IIIS), 7976–7988. https://doi.org/10.47772/ijriss.2025.903sedu0597

Siedlecki, S. L. (2019). Understanding descriptive research designs and methods. Clinical Nurse Specialist, 34(1), 8–12. https://doi.org/10.1097/nur.0000000000000493

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. IT, 18(5), 26–32. https://doi.org/10.1109/mitp.2016.84

Viraja, V. K., & Purandare, P. (2021). A qualitative research on the impact and challenges of cybercrimes. Journal of Physics Conference Series, 1964(4), 042004. https://doi.org/10.1088/1742-6596/1964/4/042004

Washington, M. A. (n.d.). A system approach for mitigating phishing attacks to secure confidential data in university enterprise information systems. https://eric.ed.gov/?q=vector&pg=13&id=ED634521

Zając, H. D., Li, D., Dai, X., Carlsen, J. F., Kensing, F., & Andersen, T. O. (2023). Clinician-

Facing AI in the Wild: Taking stock of the sociotechnical challenges and opportunities for HCI. ACM Transactions on Computer- Human Interaction, 30(2), 1–39. https://doi.org/10.1145/3582430

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative study. Journal of Computer Information Systems, 62(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269