Cybersecurity Literacy and Online Risk Management among First-Year IT Students

Eric B. Bulala[1], Mark Angelou A. Balonga[2], Alvin M. Boncales[3], Kristine T. Soberano[4]

State University of Northern Negros, Sagay, Negros Occidental, Philippines

DOI: https://doi.org/10.51244/IJRSI.2026.1304000071

Received: 04 April 2026; Accepted: 10 April 2026; Published: 30 April 2026

ABSTRACT

This research examined the cybersecurity literacy and online risk management behaviors of first-year Information Technology (IT) students at three colleges in the Philippines. The study's objectives were to evaluate students' understanding of cybersecurity threats, pinpoint prevalent risky online behaviors, and analyze the correlation between cybersecurity literacy and online risk management practices. A descriptive quantitative research design was utilized, and data were gathered from 250 first-year IT students through a structured questionnaire assessing cybersecurity knowledge and online risk management.

The results revealed that, despite students exhibiting a generally high degree of confidence in their ability to manage online risks, certain insecure practices persisted. Many respondents reported infrequent password updates (38% changing passwords only once a year and 29.6% rarely or never updating). The results also revealed that a large proportion of students entered the IT program with minimal formal cybersecurity training (32.4% had not taken any IT-related courses at all), as most respondents came from non-technical Senior High School strands (70%). Statistical analysis showed no significant differences in cybersecurity literacy and online risk management practices between male and female students ($p = 0.815$). Furthermore, Pearson correlation analysis revealed a statistically significant but weak positive relationship between cybersecurity literacy and online risk management ($r = 0.27$, $p = 0.001$).

The research findings indicated a discrepancy between students' self-assessed cybersecurity preparedness and their actual online behaviors. Specifically, students' expressed confidence did not always correlate with secure practices. Consequently, the study suggested incorporating practical, scenario-driven cybersecurity instruction into the foundational IT curriculum. This integration aimed to boost students' digital resilience and encourage safer online conduct.

Keywords: Cybersecurity, Cybersecurity literacy, Cybersecurity threats, IT students, Online risk management

INTRODUCTION

The rapid growth of digital technology has significantly changed how students learn, communicate, and manage information. First-year Information Technology (IT) students were among the most active users of online platforms because their academic work depended heavily on computers, mobile devices, and internet services. While technology provided convenience and access to knowledge, it also exposed users to cybersecurity threats such as phishing, malware, identity theft, and social engineering attacks. These risks highlighted the importance of cybersecurity literacy, defined as the knowledge, awareness, and skills required to recognize and respond to digital security threats (Aldawood et al., 2020; Alshammari et al., 2025; Ng et al., 2008).

Cybersecurity literacy was closely linked to online risk management, which referred to the ability of individuals to identify potential online dangers and apply preventive actions to reduce harm. Effective risk

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

management included secure password practices, safe browsing behavior, protection of personal data, and awareness of suspicious online activities (Aldawood et al., 2020; Concon et al., 2025). Despite belonging to a technology-related discipline, many beginning IT students entered college with uneven levels of cybersecurity knowledge. Early academic exposure did not always guarantee safe digital behavior, creating a gap between theoretical understanding and practical application.

Recent studies showed that university students often overestimate their cybersecurity competence while still engaging in unsafe practices. For example, research by Bashir et al. (2016) found that users who claimed high security awareness still demonstrated risky behaviors such as password reuse and ignoring security warnings. Similarly, some study reported that cybersecurity awareness significantly influenced online behavior, yet awareness alone did not consistently translate into secure actions (Djatsa, 2019; Saeed, 2023; Xue et al., 2021). These findings suggested that literacy and behavior had to be examined together rather than separately.

First-year students represented a critical group for investigation because they were transitioning from general digital use to professional technology training. During this stage, habits related to online safety were formed and reinforced. Understanding their current level of cybersecurity literacy could help educators design targeted interventions early in the curriculum. According to Furnell and Clarke (2012), early cybersecurity education improved long-term security practices by shaping user attitudes before unsafe behaviors became routine.

Objectives of the Study

The primary aim of this study was to explore and analyze first-year IT students' perceptions of online risk management and cybersecurity literacy with the intent of understanding their awareness, experiences, and behavioral responses to modern cybersecurity threats. The goal of the study was to determine how well the students were able to recognize and protect themselves from various technological and cybersecurity threats, including phishing, malicious software, and data exploitation. More significantly, the study aimed to draw attention to the "perception-performance gap" among students, examine relevant factors like age, gender, senior high school strand, previous IT-related courses, hours spent online daily, and password update frequency that might have made them more vulnerable to attacks, and assess how well-prepared they were to counter such threats. The survey data gathered from this particular student demographic offered the necessary information for curriculum enhancements and instructional practices that could better prepare upcoming IT professionals for online environments.

MATERIALS AND METHODS

Research Design

This research employed a descriptive-quantitative research design to examine cybersecurity literacy and online risk management practices among first-year Information Technology (IT) students. The study aimed to collect quantitative data to determine the level of cybersecurity knowledge, awareness of online threats, and the extent to which students applied risk management strategies in their daily online activities. This design allowed the researcher to systematically measure students’ understanding of cybersecurity concepts, their exposure to online risks, and their behavioral responses to common cyber threats. Furthermore, the descriptive quantitative approach enabled the analysis of relationships between cybersecurity literacy and online risk management practices through statistical methods.

Population and Sampling

The sample comprised first-year IT students from three colleges, chosen through a stratified random sampling approach. This probability sampling method was implemented to guarantee proportional representation of all subgroups within the population, including gender and institutional affiliation, thus improving the sample's overall representativeness. A sampling frame was constructed using official enrollment records, and

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

participants were randomly selected within each stratum. The final sample included 250 students, with 119 males and 131 females. To be included in the study, participants had to be officially enrolled as first-year IT students at the participating institutions during the data collection period.

Research Instrument

The main data collection tool was a structured questionnaire divided into three parts:

1. Demographic Information (age, gender, senior high school strand, previous IT-related courses, hours spent online daily, and frequency of password updates),

2. Cybersecurity Literacy Assessment (multiple-choice and Likert-scale questions assessing cybersecurity knowledge), and

3. Online Risk Management Assessment (multiple-choice and Likert-scale questions assessing the level of online risk management)

Since the questionnaire was not standardized, it underwent a content validation process by three experts in cybersecurity and educational research. Their input was utilized to make sure that the content appropriately reflected the objectives of the study and to clarify any unclear topics. To evaluate reliability, a pilot study involving 20 students was carried out. The instrument demonstrated a satisfactory reliability value ($\alpha = 0.91$), showing consistency in the replies, when Cronbach's alpha was computed based on the results.

Data Collection Procedure

The survey for the three colleges was conducted online using Google Forms and, if necessary, on paper for individuals with limited internet access. Simple instructions and an informed consent form outlining the nature of the study, data confidentiality, and voluntary participation were given to the participants. The process of gathering data took two weeks.

Data Analysis

Quantitative data from the surveys were analyzed using Excel and SPSS version 25. Descriptive statistics (mean, frequency, and percentage) were used to summarize the demographic data of the respondents. Pearson correlation analysis was used to assess relationships between the level of cybersecurity literacy and online risk management. Tables and graphs were utilized to present data in an understandable and significant way.

Ethical Considerations

This study adhered to strict ethical standards to protect the rights and welfare of all participants. Before data collection commenced, informed consent was obtained from each student, ensuring they were fully aware of the research objectives, the voluntary nature of their involvement, and their freedom to withdraw at any moment without consequences. Participants' identity and confidentiality were safeguarded by refraining from requesting personal information and by securely storing the data. All answers were utilized for academic purposes and for compiled reporting to ensure no identification of participants. In order to comply with institutional and regulatory standards on research involving human subjects, the study received prior clearance from the relevant institutional assessment board or ethics committee at the school. Additionally, during the recruitment and data collection procedures, the study preserved participant privacy and refrained from utilizing force or inappropriate influence.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

RESULTS AND DISCUSSION

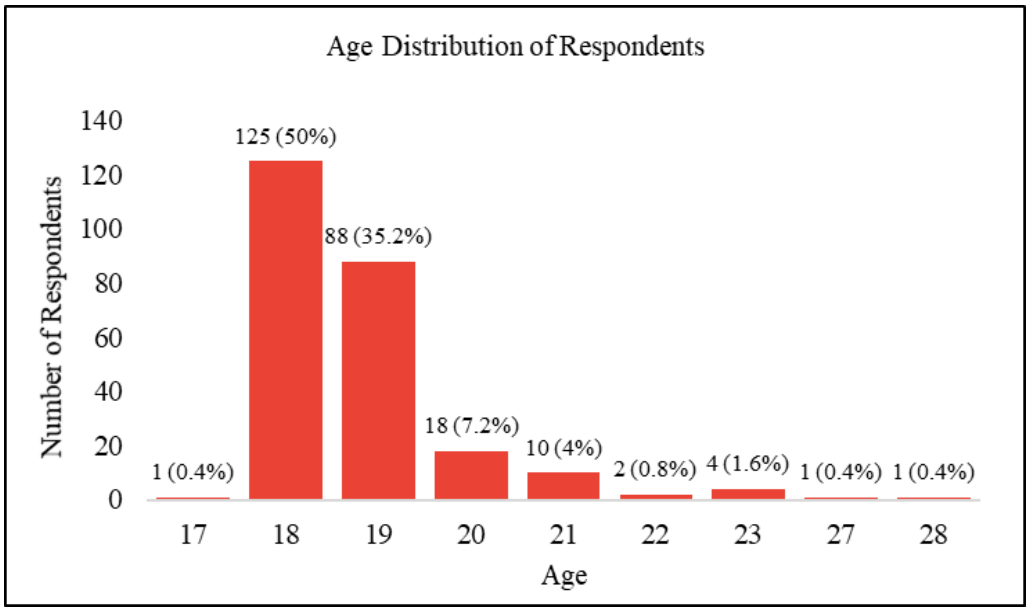

Figure 1. Age Group Analysis

The age distribution revealed that the majority of participants were 18 years old (50%), followed closely by those aged 19 (35.2%) and 20 (7.2%). This confirmed that a vast majority of the respondents fit the typical age profile for students in their first year of college. This early stage in their academic journey typically corresponded with limited formal instruction in applied cybersecurity concepts. According to Abdulla et al. (2023), younger populations had higher levels of digital engagement, but they often lacked the intellectual growth and practical skills required to identify and effectively mitigate the impact of social engineering techniques. These observations underscored the necessity of incorporating practical cybersecurity instruction at an early stage within the academic curriculum. This approach aimed to furnish students with essential digital defense strategies prior to their advancement in their academic pursuits.

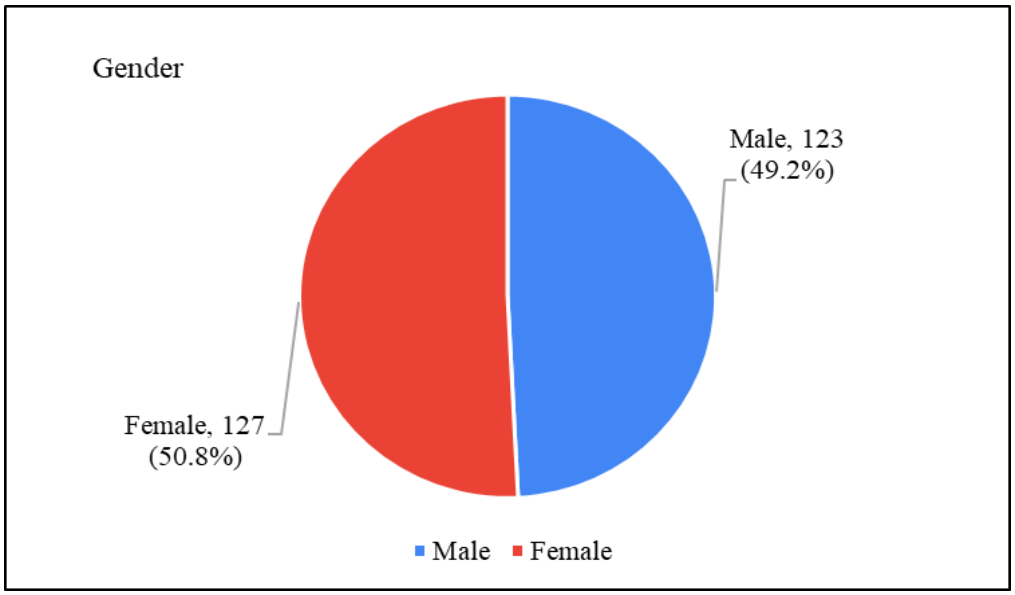

Figure 2. Gender Group Analysis

The respondents' gender distribution revealed an almost equal representation, with 50.8% identifying as female (n=127) and 49.2% identifying as male (n=123). Gender and cybersecurity literacy or risk management practices did not significantly correlate, according to statistical analysis (chi-square tests) ($p > 0.05$). This supported the findings of Albladi and Weir (2018), who came to the conclusion that gender had no impact on one's overall level of digital resilience or vulnerability to social engineering attacks. Therefore, rather than

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

making assumptions about digital literacy based on gender identity, awareness initiatives and training programs for first-year IT students should be created to address all genders equally and concentrate on developing technical proficiency.

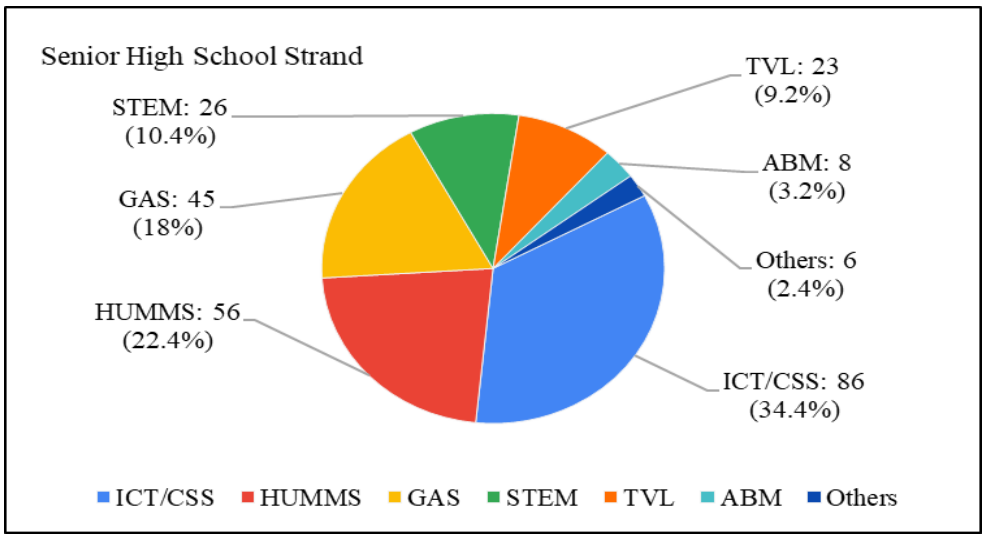

Figure 3. SHS Strand Group Analysis

The analysis of the respondents' backgrounds in Senior High School indicated diverse academic backgrounds, with the majority coming from the ICT/CSS strand (34.4%, n=86), followed by the HUMSS strand (22.4%, n=56). The remaining respondents were from the GAS (18%, n=45), STEM (10.4%), TVL (9.2%), and ABM (3.2%) strands, respectively. This was significant because the wide range of academic backgrounds indicated that over 70% of the respondents in the 1st-year of the IT course originated from non-technical fields and might have depended on informal exposure and experiences with computer technology instead of formal training in computer security. The difference in academic backgrounds among respondents was linked to the "perception-performance gap," indicating that individuals from non-technical fields might have had significant self-efficacy in utilizing computer technology while lacking awareness of advanced cyber threats (Javier, 2023). The varied academic backgrounds of the respondents indicated that individuals from diverse backgrounds exhibited inconsistent cybersecurity behaviors, requiring a formal security course to address the literacy gap among them (Saeed, 2023).

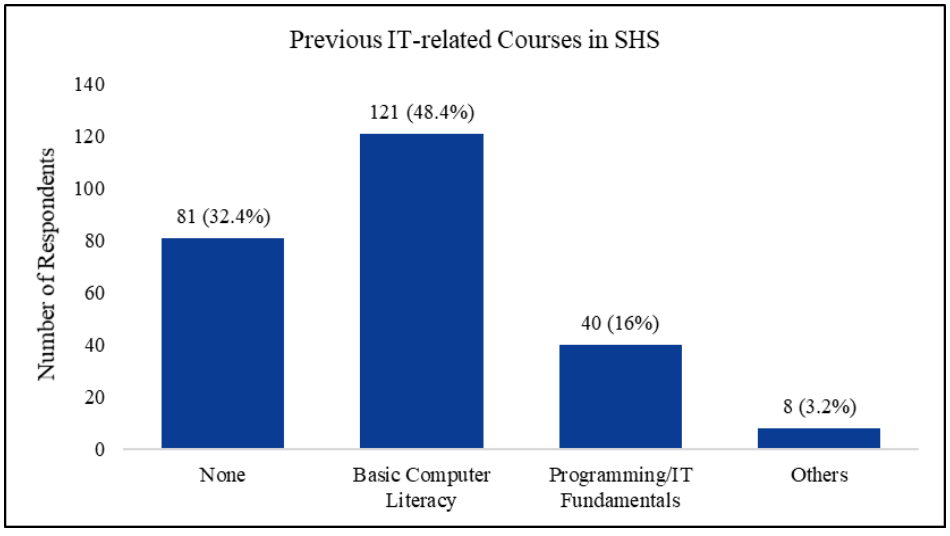

Figure 4. Previous IT-related Courses in SHS Group Analysis

The survey of the students' previous academic exposure to Information Technology showed that a large number of them only had basic skills when they started the program. Thus, 48.4% (n=121) said they had only taken Basic Computer Literacy courses, and 32.4% (n=81) said they had not taken any IT-related courses at all. Also, only a small group of 16% (n=40) had any experience with Programming or IT Fundamentals. This

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

data suggested a substantial "technical baseline gap" among first-year students, where the majority might have been proficient in general device usage but lacked formal training in the systemic security principles required for effective risk management. This lack of specialized prior instruction often resulted in higher susceptibility to cyber threats, as students without a rigorous technical foundation might have struggled to distinguish between safe digital practices and effective social engineering techniques (Saeed, 2023). Consequently, these findings highlighted the necessity for introductory IT courses to prioritize comprehensive cybersecurity training that compensates for the varying levels of prior technical exposure among freshmen (Javier, 2023).

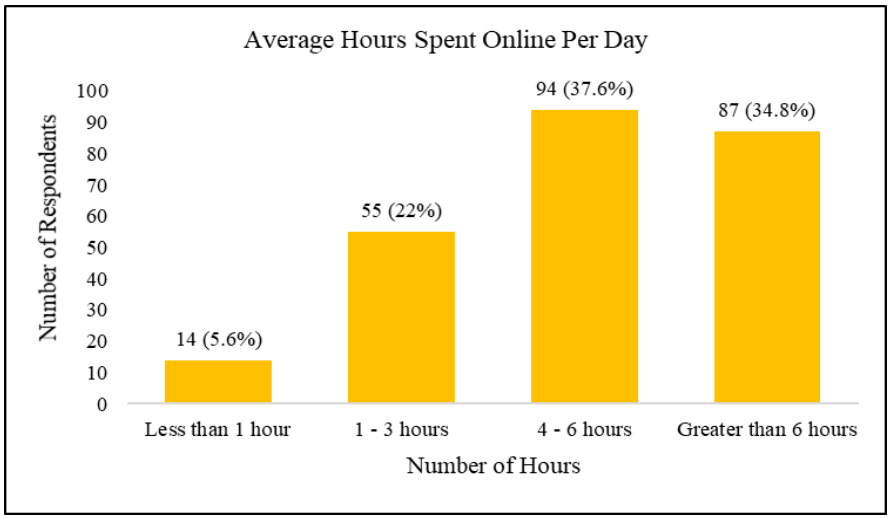

Figure 5. Average Hours Spent Online Per Day Group Analysis

The data regarding the respondents' daily digital engagement revealed that a vast majority of the students were highly active online, with 37.6% (n=94) spending 4–6 hours per day and 34.8% (n=87) spending more than 6 hours per day on the internet. In total, over 72% of the first-year IT students were online for at least four hours daily, significantly increasing their potential exposure to various cyber threats. The participants' academic backgrounds showed that they had been highly involved with technology without having any official training in cybersecurity. This made the environment extremely vulnerable to social engineering attacks and data breaches. Alshammari et al. (2025) found that spending more time on digital platforms, especially social media, made people more likely to be attacked online if they didn't know how to protect themselves. Consequently, the results highlighted that the students' significant internet usage demanded immediate response through practical literacy training to reduce the hazards related to their extended online engagement (Aldawood et al., 2020).

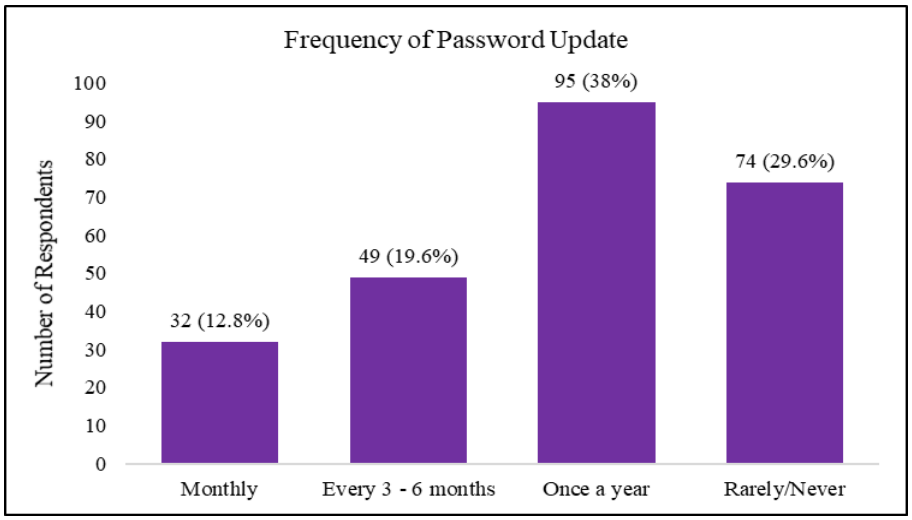

Figure 6. Password Update Frequency Group Analysis

The data regarding the frequency of password updates highlighted a concerning trend in digital safety among the respondents. As shown in the graph, only a minority practiced frequent security maintenance, with 12.8% (n=32) updating passwords monthly and 19.6% (n=49) doing so every 3–6 months. A significant majority,

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

however, reported infrequent updates, with 38% (n=95) changing passwords only once a year, and 29.6% (n=74) rarely or never updating them at all. This collective data indicated that nearly 68% of the participants maintained low-frequency password habits, which was a major vulnerability in the context of credential-based cyberattacks. According to industry security standards, static or infrequently changed passwords provided attackers with extended windows of opportunity for unauthorized access, particularly if those credentials had been compromised in previous data breaches. This high reliance on long-term, stagnant passwords among first-year IT students—despite their daily engagement with digital tools—suggested a significant gap between theoretical knowledge and actionable security behaviors. These findings reiterated the critical need for integrating practical, routine-based security education into the foundational IT curriculum, emphasizing that password maintenance was a non-negotiable aspect of professional digital resilience (Aldawood et al., 2020; Alshammari et al., 2025).

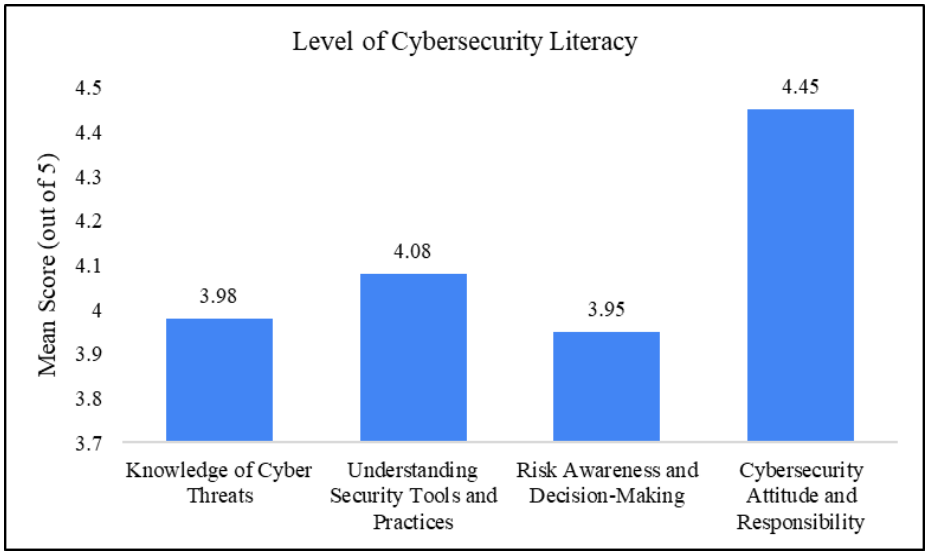

Figure 7. Level of Cybersecurity Literacy

An analysis of respondents' cybersecurity literacy levels offered essential insights into their preparation, showing that although students generally demonstrated a high-level Cybersecurity Attitude and Responsibility (4.45), their actual understanding was rather deficient. These results indicated that students were eager to act ethically and understood the importance of cybersecurity, but they didn't have the technical knowledge they needed to deal with complicated threats. The lower scores in "Risk Awareness and Decision-Making" (3.95) and "Knowledge of Cyber Threats" (3.98) showed a big gap: students knew that security was important, but they had trouble using that knowledge to see threats in real time. This difference was frequent among people who were just starting to learn about IT, where they were more interested in theory than in technical skills. Alnifie and Kim (2023) stated that this "intention-behavior" gap happened because people often didn't realize how complex social engineering attacks were and instead relied on general attitudes instead of specialized, defensive technical skills.

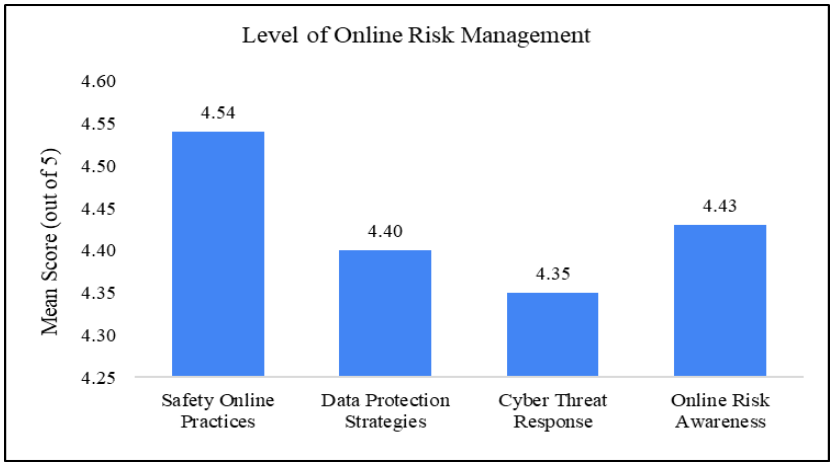

Figure 8. Level of Online Risk Management

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

The analysis of the respondents' level of online risk management indicated a generally high level of self-reported proficiency across several key areas. The data showed that the mean scores were distributed as follows: The highest score was 4.54 for Safety Online Practices, followed by 4.43 for Online Risk Awareness, 4.40 for Data Protection Strategies, and 4.35 for Cyber Threat Response. These results implied that students possessed confidence in their risk management capabilities; however, it was crucial to acknowledge that these statistics reflected subjective self-evaluations rather than objectively quantified technical proficiency. The high ratings in all areas suggested that the respondents had a strong sense of their own competence. This meant that they saw themselves as proactive users of their digital safety in the online environments they often used. Bandura (1997) claimed that individuals possessing high perceived self-efficacy—the belief in one's ability to perform necessary behaviors for achieving particular performance outcomes—frequently demonstrated enhanced confidence in dealing with environmental challenges, despite the necessity for further skill refinement through structured practice.

Summary of Key Findings

In conclusion, the study revealed that while first-year IT students demonstrated a high level of self-assessed confidence in protecting their personal data, this confidence did not always result in reliable, safe online behavior. Most of the people in the program came from a non-technical Senior High School strand and spent a lot of time online every day. This showed that it was important to improve their basic cybersecurity skills. It showed big gaps in important areas like password hygiene and responding to active threats, even if participants thought they were good at managing their own risks. These results showed that there was a need for scenario-based, focused cybersecurity training programs. These programs should not only teach students how to use technology safely, but also how to do so in a way that fits with their usual online experiences. Also, to help students get better at using digital technology in a world that was becoming more complex and dangerous, it was important to close the gap between how they thought and how they performed.

Correlation of the Level of Cybersecurity Literacy and Online Risk Management

Using Pearson's r correlation coefficient, the statistical analysis found an r value of 0.27 with a p-value of 0.001. This showed a statistically significant, weak positive correlation between the students' level of cybersecurity literacy and their online risk management behaviors. The relationship was statistically significant, which meant that the correlation was unlikely to have happened by chance. However, the low r-value showed that having more theoretical knowledge about cybersecurity did not strongly lead to better risk management habits in real life.

Source of Relationship	N	Comp r-value	p-value	Interpretation
Cybersecurity Literacy vs. Online Risk Management	250	0.27	0.001	Weak Positive Correlation

Table 1. Relationship Between Cybersecurity Literacy and Online Risk Management

The findings showed a weak but significant relationship between cybersecurity literacy and online risk management behaviors ($r = 0.27$), meaning that higher knowledge does not strongly lead to safer practices.

Several factors contributed to this phenomenon. Initially, students might exhibit overconfidence in their capabilities, assuming their security is assured despite deficient practices. Furthermore, convenience and established routines frequently take precedence over security awareness, thereby fostering risky behaviors like password reuse. Thirdly, a lack of practical experience results in students possessing theoretical knowledge of cybersecurity while finding it challenging to implement in practical scenarios (Zwilling et al., 2020). Finally, social and environmental influences, including peer conduct and inadequate institutional support, also impact their security practices.

Overall, the results suggested that cybersecurity behavior is influenced not only by knowledge but also by attitudes, habits, and environmental factors, highlighting the need for more practical and behavior-focused cybersecurity education (Parikh & Nimbekar, 2023).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue IV April 2026

Statistical Analysis

The Chi-square test performed on the survey data revealed that there was no significant association between gender and preferred frequency of password updates ($p > 0.05$), nor between the respondents' SHS strand and the extent of their previous IT-related coursework ($p > 0.05$). Likewise, independent t-tests revealed no significant differences in cybersecurity literacy and online risk management practices between male and female first-year IT students ($p = 0.815$), indicating that gender did not significantly influence students' cybersecurity knowledge and online safety behaviors. However, the correlation analysis between Cybersecurity Literacy and Online Risk Management yielded a Pearson's r of 0.27 with a p-value of 0.001. This showed that there was a statistically significant, though weak, positive relationship.

Implication & Interpretation

The data implied a need for:

- Cybersecurity education that was tailored to students' real-life situations and went beyond just teaching them about theory. This became especially important because there was a weak correlation between their literacy scores and how well they really managed risk.

- Emphasis on threat detection and password management, considering students' overconfident attitude that was not supported by students' behaviors, such as updating passwords.

- Interventions at higher academic levels, as students were more susceptible to online risks due to academic demands and interactions with others.

The difference between what students thought they were ready for and what they actually did showed that confidence was not a good way to tell if someone was ready for cyber threats. This was supported by research done by Xue et al. (2021), which implied that when individuals lacked formal training, they tended to overestimate their cybersecurity competency. This implied that educational institutions should have provided students with constant training on cybersecurity to ensure that confidence was translated into competency (Concon et al., 2025).

Limitations of the Study

Despite its contributions, this study has several limitations that should be acknowledged.

1. The study used self-reported data, which may introduce response bias as participants could overestimate their cybersecurity knowledge and practices.

2. Its cross-sectional design limits causal conclusions and only shows relationships at a single point in time.

3. The sample was limited to three colleges, which may reduce the generalizability of the findings.

4. The quantitative approach did not explore deeper psychological or behavioral factors influencing cybersecurity practices.

5. The study relied on self-reports and did not include objective measures of actual cybersecurity skills or real-world behavior.

CONCLUSION

The study found that first-year IT students generally demonstrated good awareness of cybersecurity and recognized the importance of protecting personal data online. However, despite their confidence in managing online risks, many students still practiced unsafe behaviors such as infrequent password updates and limited caution when dealing with suspicious links. The results also showed that many respondents entered the IT

program with limited formal cybersecurity training. Statistical analysis revealed no significant differences between male and female students in terms of cybersecurity literacy and online risk management. Although a significant relationship existed between cybersecurity literacy and risk management practices, the correlation was weak, indicating that knowledge alone did not always lead to safe online behavior.

RECOMMENDATION

The study made the following recommendations:

1. Educational institutions should strengthen cybersecurity education at the early stage of the IT curriculum.

2. Practical training, cybersecurity simulations, and awareness programs should be implemented to help students apply their knowledge in real-world situations.

3. Students should also be encouraged to adopt stronger security practices, such as regular password updates and the use of multi-factor authentication.

4. Future research may explore cybersecurity literacy among students from other disciplines or institutions to better understand factors influencing online risk management behaviors. The research may also adopt mixed-method approaches to gain deeper insights into behavioral aspects of cybersecurity practices.

Proposed Intervention: The Cybersecurity Competency-Based Integration Model (CCBIM)

This model is designed to be integrated into the foundational semester of an Information Technology program. It specifically addresses the "technical baseline gap" where 70% of students originate from non-technical backgrounds.

Phase	Instructional Focus	Pedagogical Method	Outcome Goal
Phase I: Diagnostic	Baseline Assessment of Literacy & Risk	Pre-program competency screening and demographic profiling.	Identification of "Technical Baseline Gaps" in high-risk groups.
Phase II: Theoretical	Systemic Security Principles & Threats	Interactive lectures on the OSI model, phishing, and malware.	Conversion of general "Cybersecurity Attitude" into foundational knowledge.
Phase III: Practical	Scenario-Driven Simulations	Simulated environments for threat detection and password management.	Reduction of the "Intention-Behavior Gap" through hands-on application.
Phase IV: Behavioral	Routine Reinforcement & Maintenance	Gamified challenges and mandatory periodic security audits.	Establishment of long-term digital resilience and non-negotiable security habits.

Table 2. Proposed Curriculum Integration Framework for First-Year IT Students

REFERENCES

1. Abdulla, R. M., Faraj, H. A., Abdullah, C. O., Amin, A. H., & Rashid, T. A. (2023). Analysis of social engineering awareness among students and lecturers. IEEE Access, 11, 101098–101111. https://doi.org/10.1109/access.2023.3311708
2. Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. Human-Centric Computing and Information Sciences, 8(1). https://doi.org/10.1186/s13673-018-0128-7
3. Aldawood, H., Alashoor, T., & Skinner, G. (2020). Does awareness of social engineering make employees more secure? International Journal of Computer Applications, 177(38). https://www.ijcaonline.org/archives/volume177/number38/aldawood-2020-ijca-919891.pdf

4. Alnifie, K. M., & Kim, C. (2023). Appraising the manifestation of optimism bias and its impact on human perception of cyber security: A meta-analysis. Journal of Information Security, 14(2), 93–110. https://doi.org/10.4236/jis.2023.142007
5. Alshammari, S. S., Soh, B., & Li, A. (2025). Understanding social engineering victimisation on social networking sites: A comprehensive review of factors influencing user susceptibility to cyber-attacks. Information, 16(2), 153. https://doi.org/10.3390/info16020153
6. Bandura, A. (1997). Self-efficacy: The exercise of control. W. H. Freeman.
7. Bashir, M., Wee, C., Memon, N., & Guo, B. (2016). Profiling cybersecurity competition participants: Self-efficacy, decision-making, and interests predict effectiveness of competitions as a recruitment tool. Computers & Security, 65, 153–165. https://doi.org/10.1016/j.cose.2016.10.007
8. Concon, A. F., Arances, A. C., Lorican, F., & Soberano, K. (2025). Cyber literacy and cyber risk mitigation program of one municipal college in the Philippines. GAS Journal of Engineering and Technology, 2(6), 21–29. https://gaspublishers.com/wp-content/uploads/2025/08/Cyber-Literacy-and-Cyber-Risk-Mitigation-Program-of-One-Municipal-College-in-the-Philippines.pdf
9. Djatsa, F. (2019). How perceived benefits and barriers affect millennial professionals' online security behaviors. Journal of Information Security, 10(4), 278–301. https://doi.org/10.4236/jis.2019.104016
10. Furnell, S., & Clarke, N. (2012). Power to the people: The evolving recognition of human aspects of security. Computers & Security, 31(8), 983–988. https://doi.org/10.1016/j.cose.2012.01.008
11. Javier, D. R. C. (2023). Awareness of senior high school students on digital literacy skills: A qualitative study. ResearchGate. https://www.researchgate.net/publication/369243517
12. Ng, B., Kankanhalli, A., & Xu, Y. (2008). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010
13. Parikh, V., & Nimbekar, M. (2023). Socializing the Impact: An analysis of the theory of planned behavior's influence on increasing university students' cybersecurity awareness. Journal of Community and Development, 4(2), 139–156. https://doi.org/10.47134/comdev.v4i2.162
14. Saeed, S. (2023). Education, online presence and cybersecurity implications: A study of information security practices of computing students in Saudi Arabia. Sustainability, 15(12), 9426. https://doi.org/10.3390/su15129426
15. Xue, B., Warkentin, M., Mutchler, L. A., & Balozian, P. (2021). Self-efficacy in information security: A replication study. Journal of Computer Information Systems, 63(1), 1–10. https://doi.org/10.1080/08874417.2021.2015725
16. 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