GAS Journal of Engineering and Technology (GASJET)

Volume 2, Issue 6, 2025 Journal Homepage: https://gaspublishers.com/gasjet-home/ ISSN: 3048-5800
Email: editor@gaspublishers.com

Cyber Literacy and Cyber Risk Mitigation Program of One Municipal College in the Philippines

Arcelie C. Arances[1], Aileen F. Concon, Franklin Lorican & Kristine Soberano

State University of Northern Negros, Sagay, Negros Occidental

Received: 29.07.2025 | **Accepted:** 19.08.2025 | **Published:** 19.08.2025

***Corresponding Author:** Aileen F. Concon

DOI: *10.5281/zenodo.16905221*

Abstract

Original Research Article

This research assesses the effect and implementation of a cyber-literacy and cyber risk prevention program for a local municipal college in the Philippines with the purpose of determining the most common cyber security threats, determining the level of cyber literacy of students and gauging the impact of awareness programs on online safety attitudes of respondents. Through a descriptive quantitative approach, information was gathered from 200 participants using a standardized questionnaire on cyber literacy, risk exposure, and program efficacy.

There were findings showing that while 75.5% of students were certain that they could protect their personal information online, such confidence was often negated by insecure behavior such as password reuse (35%), rarely changing passwords (63.5% changing once a year or never), limited knowledge about multi-factor authentication (43.5%), and poor skills in detecting phishing (32% unsure). The most prevalent student concerns were online safety on social media (79.5%), being scammed online (59%), defending devices (53.5%), managing passwords (50.5%), and recognizing phishing (47%). However, even though 51% of the interviewees had undergone formal cyber security training, 31.5% expressed that it was ineffective, reflecting the needs for more situation-based, relevant, and interactive training.

The report identifies a perception-performance gap in cyber security preparedness, whereby reported confidence is not always converting into secure behavior. The research suggests embedding regular, context-relevant cyber literacy training into the curriculum, including practice skills like phishing recognition, password habits, and secure device use. Improved development in these areas will not only improve individual digital resilience but also provide a blueprint for other educational institutions who wish to develop a stronger cyber security culture.

Keywords: Cyber Literacy, Cyber Risk, Cybersecurity Awareness, Risk Mitigation, Municipal College, Digital Safety, Cybersecurity Education, Information Security, Cyber Threats, Philippine Higher Education.

INTRODUCTION

In today's digitally driven learning environment, the institutions of higher learning are often confronted with an array of cyber threats that span phishing, malware attacks, data breaches, and cyber disinformation. Institutions of learning in developing nations like the Philippines do not have a functional cyber security infrastructure and capacity among their teaching staff, administrative personnel, and students. All these factors underscore the need for programs that enhance cyber literacy and manage cyber threats within the world of learning.

Park and Kim [1] introduce a building block conceptual view by conceptualizing cyber literacy as a multidimensional construct encompassing technical, ethical, and critical thinking capabilities in electronic spaces. Their research highlights how comprehension of these dimensions facilitates effective cyber security consciousness, especially when individuals can critically assess online threats.

To this, Hadlington [2] examines the human psychological aspects involved in risky cyber security behavior. The study links internet addiction and impulsivity to unsafe cyber security practices and identifies that user attitudes influence, to a considerable extent, how individuals approach secure or insecure online behavior. The implications of this result are that interventions need not only to educate in security skills but also to address behavioural inclinations.

Locally, Cruz and Medina [3] explored cyber security awareness of college students in the Philippines' selected provinces. They found an awareness-practice gap, indicating that the students know about cyber security but commonly fail to practice safe measures. This finding highlights the necessity for reinforcement and behaviour-oriented training within educational institutions.

To respond to these kinds of challenges, the Department of Information and Communications Technology (DICT) introduced a Cybersecurity Education and Awareness Program in 2022. It seeks to enhance national cyber security capability through community outreach, digital literacy training, and awareness campaigns [4]. It endorses that awareness needs to be developed comprehensively by policy-supported measures and education.

Lastly, the study of Ng, Kankanhalli, and Xu [5] applies the Health Belief Model to computer security behavior, showing that perceptions of threat seriousness and self-efficacy affect an individual's propensity to engage in safe cyber security behaviors. Their study indicates that increasing personal motivation and belief in being able to ward off threats may contribute to improved compliance with secure practices.

OBJECTIVE OF THE STUDY

The aim of this research is to evaluate the impact of the Cyber Literacy and Cyber Risk Mitigation Program conducted in one of the Municipal Colleges in the Philippines. It seeks to establish the level of cyber literacy among students currently, identify the most prevalent cyber threats that are being faced by the community within the college, and determine how the program affects participants' awareness, knowledge, and behavior concerning cyber security. Additionally, the research aims to offer proposals on how to improve and maintain cyber risk mitigation programs in the same local educational institutions.

MATERIALS AND METHODS

Research Design

This research will employ a descriptive quantitative research design. It seeks to provide quantitative data gathering the extent of cyber literacy, cyber risk exposure, and perceived effectiveness of cybersecurity awareness programs among the students of One Municipal College in the Philippines. The design enables the researcher to examine relationships among variables and provides statistical information regarding trends and patterns of cyber security awareness and conduct.

Population and Sampling

The target population is the **college students**. A **stratified random sampling technique** will be used to ensure that participants are proportionally selected from different departments and year levels. An estimated sample size of **200 participants** will be chosen to represent both groups effectively.

Research Instrument

The main data collection tool will be a **structured questionnaire** divided into four parts:

1. **Demographic Information** (age, gender, role, department/year level),
2. **Cyber Literacy Assessment** (multiple-choice and Likert-scale questions assessing cybersecurity knowledge),
3. **Cyber Risk Exposure** (self-reported experiences with cyber threats and risky behaviors),
4. **Awareness Program Evaluation** (feedback on existing programs and perceived effectiveness).

The questionnaire will be validated through expert review and pilot-tested on a small group before full deployment.

Data Collection Procedure

The survey will be administered online through Google Forms and, if needed, in paper form to those with restricted internet access. The participants will be provided with uncomplicated instructions and an informed consent from describing the nature of the study, confidentiality of the data, and voluntary participation. The data gathering process will run for two weeks.

Data Analysis

Data collected will be computed using descriptive statistics (mean, percentage, and standard deviation) to quantify the cyber literacy and risk exposure level. Correlational analysis (e.g., Pearson correlation)

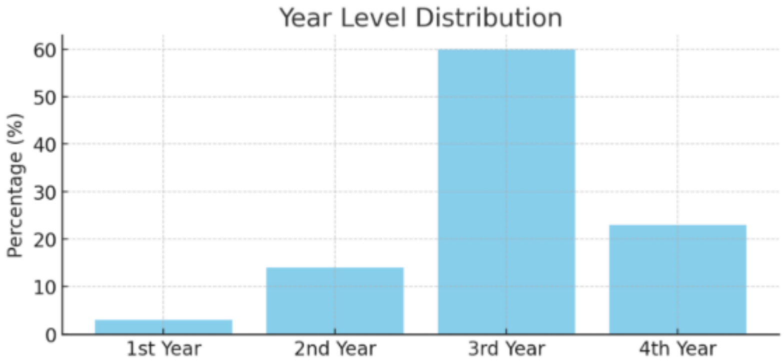
will further be applied to explore the correlation between cyber literacy and cyber risk. Presentation of data will be achieved using tables, graphs, and charts for easier understanding.

Ethical Considerations

This research will observe stringent ethical practices to safeguard the rights and well-being of all the respondents. Before data are collected, informed consent from each student will be secured, with them clearly understanding the research purpose, the voluntary nature of participation, and the right to withdraw at any time without penalty. The anonymity and confidentiality of participants will be ensured by not requesting personally identifiable information and by saving the data securely. All answers will be utilized for academic purposes and for aggregated reporting to ensure no identification of participants. The study will also obtain a prior approval from the relevant institutional review board or ethics committee at the school to abide by institutional and legal requirements on human subject research. The study will also maintain the privacy of participants and refrain from any coercion or undue influence in the process of recruitment and data collection.

Results and Discussion

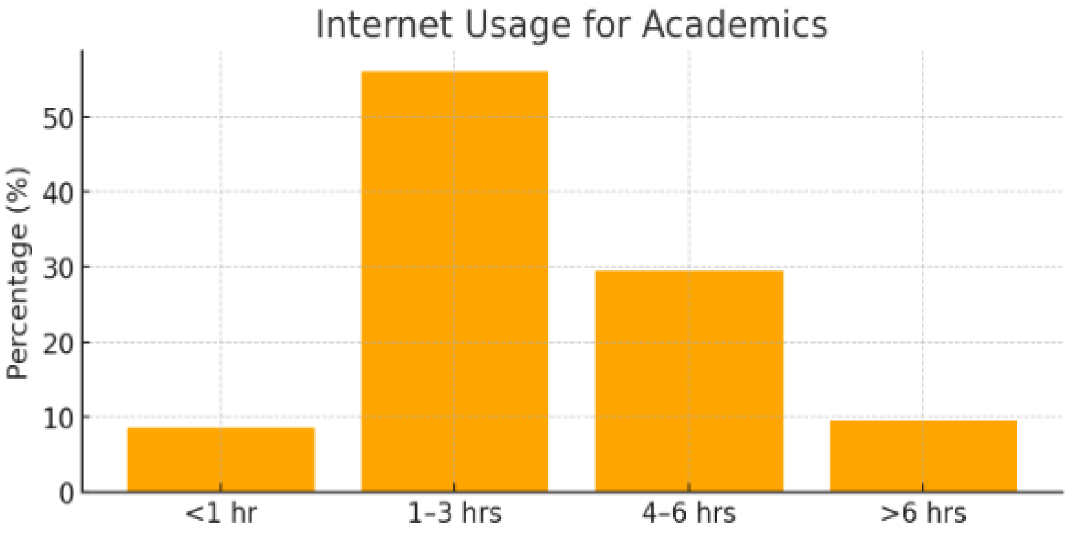
Figure1. Year Level Distribution Analysis



A whopping majority of the students—60% of the respondents—are on their third year of study, based on the respondents' distribution by year level. Such a trend indicates that the study mostly represents the views and behaviors of students who have overall progressed in their academic pursuits. Research, capstone projects, internships, and specialized courses are generally more typical among upper-level students, and they all require regular use of digital platforms for collaboration, data gathering, and output dissemination.

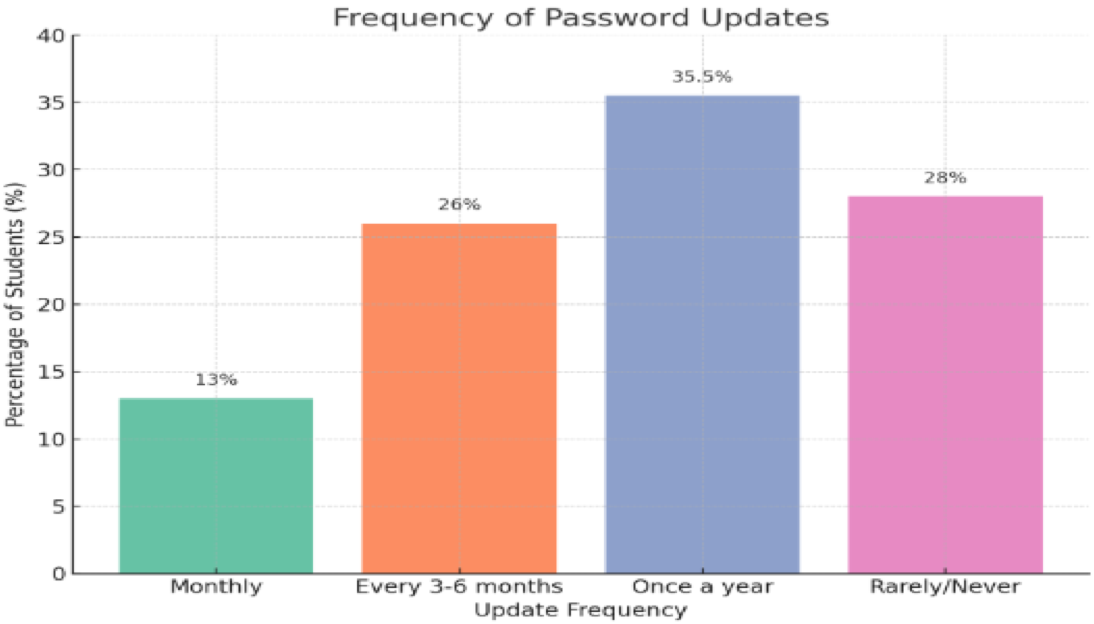
A high sample size of third-year respondents confirms the idea that students are better habituated to technology, both the usage and the incorporation of digital devices in study habits. Such exposure is generally associated with heightened sensitivity about cyber-attacks; however, if needed cyber hygiene and literacy are not developed, it can actually heighten vulnerability. The exposure to digital technology among student's increases as they move along the levels of higher learning, enhancing their confidence and preparedness towards online learning paradigms, as indicated in earlier research like Callo & Yazon [6]. Since they had received more academic loads, digital technologies, and e-learning requirements, the research discovered that third- and fourth-year students were better qualified and more confident in utilizing digital platforms compared to first- and second-year students.

Figure2. Internet Usage for Academic Analysis



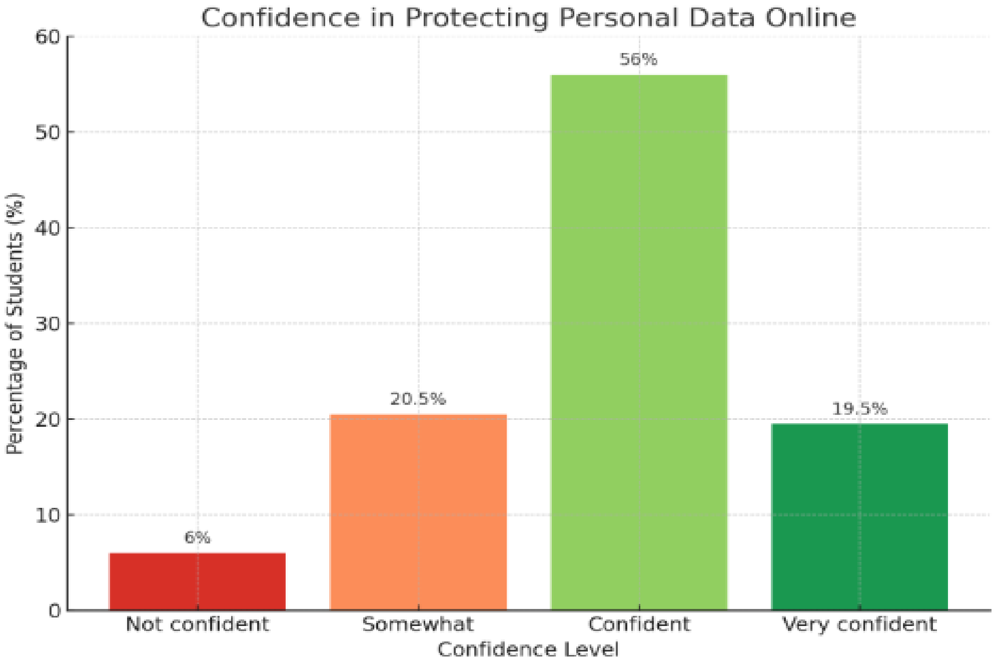
The survey results reveal that over 95% of students dedicate a meaningful portion of their day to academic internet usage, with most clustering in the 1–3 hour range. This suggests that digital access is integral to students' academic routines—supporting research, content creation, communication, and submission of assignments. Students investing more than 4 hours daily online for academic work likely face both increased efficiency and potential digital stress. Giraya et al.[8], observed that Filipino students are heavily reliant on digital devices, with daily usage spanning both academic and leisure purposes. The study found a direct correlation between times spent online and heightened digital stress, reflecting the impact of extended screen exposure. Importantly, while high usage implies increased academic engagement, it also correlates with greater exposure to cyber risks—particularly if students engage in multitasking across academic, entertainment, and social platforms without adequate digital literacy.

Figure 3. Password Update Frequency Analysis



The findings of the survey indicate that the majority of students do not have the practice of regular password updates. Just 13% of students update their password every month, and 28% hardly or never update them. The most popular practice, with 35.5% of the participants, is to update passwords annually. Such a trend indicates a poor cyber hygiene culture, which may put students into unnecessary risk in case of combination with password reuse (already practiced by 35% of the respondents). The use of infrequent password changes is most risky in the current threat environment, where breaches and credential dumping are the orders of the day. The attackers tend to count on users' behaviors of keeping the same or like passwords for extended periods of time. In addition, the National Institute of Standards and Technology [9], suggests that users reset passwords according to risk events, e.g., after documented breaches or indicators of compromise, instead of on random schedules. For most people, however, regular updating is a good preventive habit—particularly within educational settings where personal, academic and institutional information meet.

Figure4. Confidence in Protecting Personal Data Online Analysis



The survey finds that significant portion of students—75.5%—claimed to feel confident or very confident in defending their online personal information. Yet, in such high self-reported confidence, it diverges from a number of the most important measures of insecure digital practice:

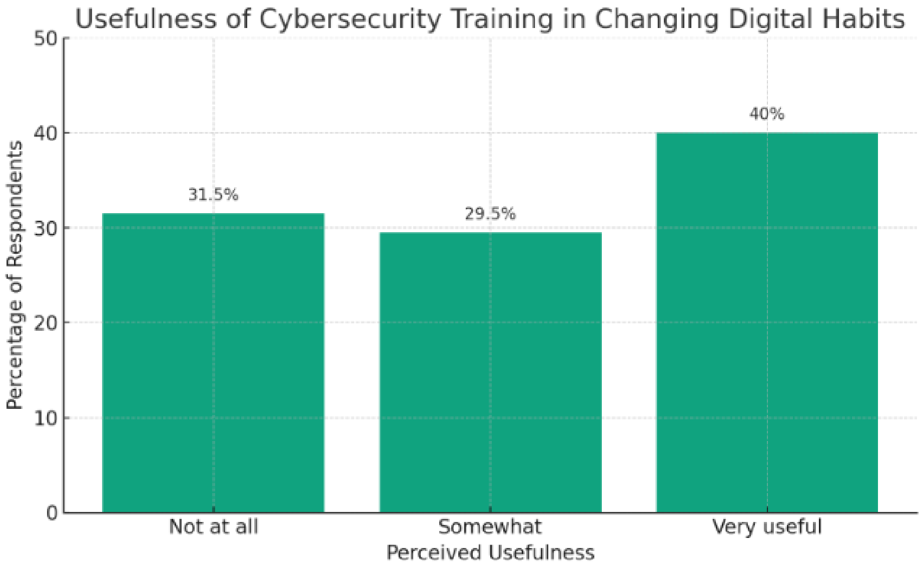
35% reported sharing passwords, a familiar weak point making multiple accounts vulnerable to breach if just one is compromised.
32% were uncertain on whether they could identify phishing attempts, indicating poor readiness for actual attacks. 43.5% were unaware of multi-factor authentication (MFA), which is an underpinning layer of digital protection.

This inconsistency between perceived ability and real-world cyber security habits is reflected in research within the academic literature. A study conducted by Xue et al. [10], highlighted that overestimation of cyber security self-efficacy may cause an illusion of protection unless it is supported by knowledge or action. In the same vein, Hadlington and Murphy [11], discovered that people tend to overestimate their technical skills, especially in situations where threats are not encountered directly or are abstract.

In this regard, students' confidence can originate more from repeated visits to digital platforms than from an in-depth awareness of cyber risk avoidance. Knowledge of social media, e-commerce, or cloud storage does not necessarily translate into skills in recognizing threats or handling information securely.

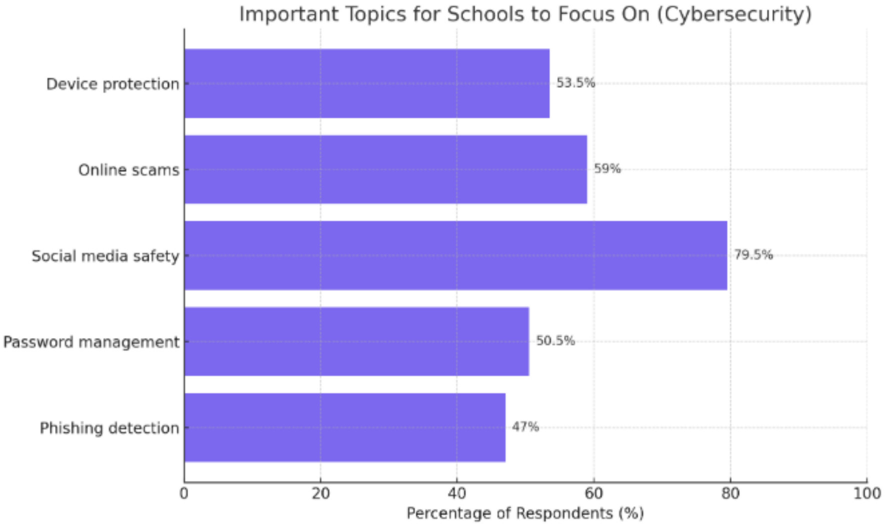
This discrepancy underlines the necessity for experiential, situation-based digital safety learning, such as simulations for phishing, social engineering, and password compromise. Consistent with associated literature, in today's digitally reliant world, even the self-assured user is still susceptible to attacks because of system, network, or user bad habits.

Figure5. Usefulness of Cyber Security Training in Changing Digital Habits Analysis



Out of 200 formal cyber security training recipients, 40% found it very helpful in altering their online behaviors, 29.5% found it somewhat helpful, whereas 31.5% indicated that it was not helpful at all. This breakdown shows a tendency towards mixed attitudes of training effectiveness, with almost one-third of trained students not perceiving significant change in behavior. This implies that training programs, as potentially powerful drivers of positive change in cybersecurity behavior, depend on their design, delivery, and contextual applicability for success. The 40% who rated the training as "very useful" might have been engaged by interactive or scenario-based modules focusing directly on actual cyber threats. On the other hand, the 31.5% who rated it as "not useful" might have received generic, one-size-fits-all type sessions lacking in relevance or interest. This corroborates with research by Kritzinger and von Solms [12], which highlighted that the success of cyber security awareness programs largely relies on user participation and context-based content. According to them, training needs to be tailored to users' roles, IT habits, and online environments for enhanced retention and behavioral take-up.

Figure6. Important Topics for Schools to Focus on (Cybersecurity) Analysis



Most participants (79.5%) highlighted social media safety as the most critical issue, which may be influenced by their regular use of sites such as Facebook, TikTok, and Instagram, as witnessed in previous survey answers. High exposure to privacy violation and cyber bullying cases on social media sites may be a likely reason for this priority.

Online fraud was in the second position (59%) reflecting increased awareness of cybercrime like false promotions, internet fraud, and identity theft. This fear is not misplaced, considering that cyber scams are becoming more sophisticated and target students.

Device protection (53.5%) and password management (50.5%) were also considered to be of the utmost importance. This indicates that students realize the need for protecting personal devices and managing authentication credentials, but might need stronger scaffold instruction in best practices.

Notably, detection of phishing (47%)—while a critical aspect of cyber risk—was more disparaged than social media and device issues. It is likely that this is evidence of a knowledge deficit regarding the relationship between compromised devices or accounts and phishing and, more generally, the need for highlighting such a relationship in cyber security education.

Overall, the figures indicate a profoundly strong student interest in practical, real-world cyber security skills as opposed to theoretical concepts. Curriculum would be enriched by focusing on real-world scenarios that accord with students' internet experiences.

Summary of Key Findings

In summary, the research showed that although students demonstrate a high rate of self-assessed confidence in safeguarding their personal information online, this confidence does not always reflect in safe digital behaviors. The majority of the subjects were third-year students, who were mostly engaged in online learning activities, further substantiating the rationale to address their cyber security readiness. Substantial gaps were observed in critical domains such as password hygiene, awareness of multi-factor authentication and phishing, despite the majority of students having received formal cyber security training. Additionally, students indicated practical subjects—cyber security education on social media safety, online fraud, protection of devices, security for passwords, and phishing identification—as the most important areas wherein schools should set their priorities on education on cyber security. These findings underscore the urgent need for scenario-based, focused cyber security training initiatives that not only cultivate technical competence but also instill secure online practices aligned with students' typical digital experiences. Closing the perception-performance gap is essential to enable students to become proficient in a more sophisticated and high-risk digital world. Moreover, the students identified pertinent concerns—online fraud, safety on social media, device protection, password care, and phishing identification—as being the most critical domains on which schools need to invest their cyber security education efforts. These findings underscore the critical importance of scenario-specific, focused cyber security training programs that not only cultivate technical proficiency but also nurture secure online behaviors in line with students' normal online experiences. Bridging the gap between perceived and actual capability is crucial in empowering students to excel in an increasingly sophisticated and high-risk digital landscape.

Perceptions of Preparedness and Importance

The results of the survey indicate that although students are high on confidence in handling personal information protection—that 75.5% of them expressed confidence or very high confidence—this confidence is not always matched with secure digital behaviors. The topmost cyber security issues of concern for students were:

- Social Media Safety (79.5%)
- Online Scams (59%)
- Device Protection (53.5%)
- Password Management (50.5%)
- Phishing Detection (47%)

These priorities reflect students' awareness of common, tangible threats encountered in their digital routines, particularly within social media environments.

Common Threats and Information Sources

Some key gaps in cyber behavior and literacy were found:

- Reuse of Passwords: 35% confessed to having the same password for multiple accounts, making them more vulnerable to credential-based attacks.
- Rare Password Changes: 63.5% change passwords merely once a year or seldom/never, making them less resistant to breaches.
- Limited Knowledge of MFA: 43.5% lacked awareness of multi-factor authentication, exposing accounts to unauthorized access.
- Phishing Identification: 32% did not know how to identify phishing attempts, indicating a deficiency in hands-on threat identification abilities.

Students most frequently use social media as their primary online space, where they perceive that they are most threatened but can also fail to see more profound, technical threats such as phishing and credential compromise.

Statistical Analysis

The year level split—60% third-year students—implies that the survey is representative of views of fairly senior learners who have had extensive digital exposure. In addition:

- 95% of the students used the internet daily for academic use, with 56% of them using it 1-3 hours a day online.

- While 51% of them received formal cyber security training, 31.5% of them considered it to be not helpful, suggesting that the delivery and effectiveness of training could be inconsistent.

These figures demonstrate a reliance on Internet sites for academic pursuits but a mixed outcome in the realm of cyber literacy and Internet security practices.

Implications and Interpretation

The data suggest a clear need for:

- **Customized, scenario-based cyber security education** that moves beyond theoretical concepts and addresses the digital behaviors students regularly engage in.
- **Greater emphasis on threat detection and password hygiene**, given that many students display overconfidence that is not matched by their reported behaviors.
- **Targeted interventions at higher academic levels** where students are more engaged online and exposed to more sophisticated cyber threats due to their academic workloads and social interactions.

The gap between perceived preparedness and actual secure behavior indicates that confidence alone is not a reliable predictor of cyber readiness. This supports findings from Xue et al. [10] and Hadlington & Murphy [11], who both noted that individuals often overestimate their cyber security competence when they lack formal, practical training.

Educational institutions should, therefore, incorporate continuous, practical cybersecurity programs that evolve with students' digital maturity and exposure, ensuring that confidence is backed by competence.

Conclusion and Recommendation

This research uncovered a key disconnect between students' self-assessed cyber security capability and their demonstrated online safety behavior. While most indicated they are confident to keep their online information private, practices like updating passwords seldom, reusing passwords, minimal multi-factor authentication awareness, and ineffective phishing detection suggest that this confidence is frequently misplaced. Students listed foremost among their concerns issues of social media safety, online fraud, protecting devices, and passwords, but most felt current cyber security training was only somewhat successful. These results emphasize that cyber literacy is not so much a question of consciousness but needs constant, scenario-driven education that is specific to the actual digital behaviors of students. Enhancing cyber hygiene, promoting skills of critical threat recognition, and mapping training on students' daily online behavior are critical in bridging the perception–performance gap and equipping them for an increasingly sophisticated cyber threat landscape.

Against this backdrop, it is recommended that schools and universities develop and employ scenario-based cyber security training based on real-world simulations, such as phishing detection training and password breach attack training, to maximize students' threat-response capabilities. Cyber literacy must be included in the curriculum throughout all year levels to ensure that learning is continuous and cumulative. Training sessions need to target the high-risk areas the students have identified, such as social media safety, protection from online scams, device security, password security, and phishing identification. Awareness campaigns need to be undertaken on a regular basis to instill good cyber hygiene measures like making special passwords, changing them regularly, and using multi-factor authentication (MFA). Additionally, training material must be rendered relevant and interesting through gamification, peer sessions, and case studies to enhance involvement and retention. Finally, institutions should implement ongoing monitoring and assessment of students' cybersecurity behaviors and cyber literacy to gauge the program's effectiveness and make timely improvements.

REFERENCES

[1] J. Park and H. Kim, "Understanding digital literacy in the context of cybersecurity awareness," *Journal of Educational Computing Research*, vol. 58, no. 4, pp. 789–806, 2020. https://doi.org/10.1177/0735633120905100

[2] L. Hadlington, "Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors," *Heliyon*, vol. 3, no. 7, e00346, 2017. https://doi.org/10.1016/j.heliyon.2017.e00346

[3] M. A. Cruz and J. C. Medina, "Cybersecurity awareness among college students in selected provinces in the Philippines," *Philippine Journal of Educational Technology*, vol. 7, no. 1, pp. 45–53, 2018.

[4] Department of Information and Communications Technology (DICT), "Cybersecurity education and awareness program," 2022. [Online]. Available: https://dict.gov.ph/cybersecurity

[5] B.-Y. Ng, A. Kankanhalli, and Y. Xu, "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems*, vol. 46, no. 4, pp. 815–825, 2009. https://doi.org/10.1016/j.dss.2008.11.010

[6] E. C. Callo and A. D. Yazon, "Exploring the factors influencing the readiness of faculty and students on online teaching and learning as an alternative delivery mode for the new normal," *Universal Journal of Educational Research*, vol. 8, no. 8, pp. 3504–3515, 2020. doi: 10.13189/ujer.2020.080826.

[7] L. Y. C. Chang and N. Coppel, "Building cyber security awareness in a developing country: Lessons from Myanmar," *Computers & Security*, vol. 97, 101959, 2020. doi: 10.1016/j.cose.2020.101959.

[8] L. Giray, J. Nemeño, J. Braganaza, S. M. Lucero, and R. Bacarra, "A survey on digital device engagement, digital stress, and coping strategies among college students in the Philippines," *International Journal of Adolescence and Youth*, 2024. doi: 10.1080/02673843.2024.2371413.

[9] National Institute of Standards and Technology (NIST), *Digital Identity Guidelines*, NIST Special Publication 800-63B, 2022. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63b.html

[10] Y. Xue, X. Luo, and M. Warkentin, "Self-efficacy in information security: A replication study," *Computers in Human Behavior*, vol. 144, 107693, 2023. doi: 10.1016/j.chb.2022.107693.

[11] L. Hadlington and K. Murphy, "Is media multitasking good for cybersecurity?" *Cyberpsychology, Behavior, and Social Networking*, vol. 21, no. 3, pp. 168–172, 2018. Available: https://pubmed.ncbi.nlm.nih.gov/29638157

[12] E. Kritzinger and S. H. von Solms, "Cyber security for home users: A new way of protection through awareness enforcement," *Computers & Security*, vol. 29, no. 8, pp. 840–847, 2010. doi: 10.1016/j.cose.2010.08.001.