



Level of Awareness of Accounting Students on Privacy, Cyberthreats, and Financial Data Protection in Dalubhasaang Politekniko ng Lungsod ng Baliwag

Article Record

Maricel Calimpusan^{§*}

*Corresponding Author



Mayriel T. Nocos



Charles Denzel P. Seradilla



Aileen S. Tanjoco



Charmaine R. Vistan



Cruz, Daniella Wjotilla E.



Myrna S.[§]

[§] Institute of Business and Accountancy, Dalubhasaang Politekniko ng Lungsod ng Baliwag, Baliwag, Philippines

RECEIVED

2026-04-20

ACCEPTED

2026-04-30

ONLINE PUBLISHED

2026-08-06

PEER REVIEW

Double Blind

Abstract

This paper set out to assess the degree of cybersecurity awareness among accounting undergraduate students at Dalubhasaang Politekniko ng Lungsod ng Baliwag, in the areas of privacy, cyber threats and financial data protection. The data were gathered by surveying 70 fourth-year students in four accounting programs by utilizing a survey questionnaire with stratified sampling by using a descriptive quantitative approach. The results showed that students tend to be highly aware of fundamental concepts of cybersecurity, including keeping personal and financial data secure, using secure passwords, and being able to identify such widespread threats as phishing and identity theft. They were however not well informed on advanced threats such as ransomware and denial-of-service (DoS) attacks. Another thing that emerged among students was that they want to acquire more knowledge on cybersecurity, especially concerning their future career, data protection duties, and regulatory compliance. All in all, the research paper results in the conclusion that although the accounting students have the background understanding of security in the cyber realm, further learning of the sophisticated threats is required. It suggests covering the subject of cybersecurity in the accounting course in order to prepare students to meet the digital needs of the job.

cybersecurity awareness

accounting students

privacy

cyber threats

financial data protection

AI USE STATEMENT

No generative AI was used for analysis or results.

FUNDING

No external funding was declared for this work.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

DATA AVAILABILITY

Not applicable for this article.

ETHICS

No ethics committee approval was required for this article type.

CONSENT

Not applicable for this article.

TRIAL REG.

Not applicable.

Crossref DOI: 10.34257/GJMBRG256422

How to Cite: Calimpusan et al. (2026). Level of Awareness of Accounting Students on Privacy, Cyberthreats, and Financial Data Protection in Dalubhasaang Politekniko ng Lungsod ng Baliwag. Global Journal of Management and Business Research, 26(1), 1-15. DOI: 10.34257/GJMBRG256422

LICENSE

© 2026 Global Journals. Open-access article under CC BY-NC-ND 4.0 International License.



Print ISSN 0975-5853



Online ISSN 2249-4588



Under the strict compliance and defined process of



METADATA CONTINUATION

AUTHOR CONTACT QR LEDGER

Maricel Calimpusan§*		Mayriel T. Nocos		Charles Denzel P. Seradilla		Aileen S. Tanjoco	
Charmaine R. Vistan		Cruz, Daniella Wjotilla E.					

ARCHIVAL RECORD

Level of Awareness of Accounting Students on Privacy, Cyberthreats, and Financial Data Protection in Dalubhasaang Politekniko ng Lungsod ng Baliwag

Maricel Calimpusan^{§*}, Mayriel T. Nocos[§], Charles Denzel P. Seradilla[§], Aileen S. Tanjoco[§], Charmaine R. Vistan[§], Cruz, Daniella Wjotilla E.[§], and Myrna S.[§]

Affiliations

[§] Institute of Business and Accountancy, Dalubhasaang Politekniko ng Lungsod ng Baliwag, Baliuag, Philippines

Abstract

This paper set out to assess the degree of cybersecurity awareness among accounting undergraduate students at Dalubhasaang Politekniko ng Lungsod ng Baliwag, in the areas of privacy, cyber threats and financial data protection. The data were gathered by surveying 70 fourth-year students in four accounting programs by utilizing a survey questionnaire with stratified sampling by using a descriptive quantitative approach. The results showed that students tend to be highly aware of fundamental concepts of cybersecurity, including keeping personal and financial data secure, using secure passwords, and being able to identify such widespread threats as phishing and identity theft. They were however not well informed on advanced threats such as ransomware and denial-of-service (DoS) attacks. Another thing that emerged among students was that they want to acquire more knowledge on cybersecurity, especially concerning their future career, data protection duties, and regulatory compliance. All in all, the research paper results in the conclusion that although the accounting students have the background understanding of security in the cyber realm, further learning of the sophisticated threats is required. It suggests covering the subject of cybersecurity in the accounting course in order to prepare students to meet the digital needs of the job.

Keywords: *cybersecurity awareness, accounting students, privacy, cyber threats, financial data protection*

* Corresponding Author
Maricel Calimpusan

DOI
10.34257/GJMBRG256422

1. Introduction

In the contemporary digital era, cybersecurity acts as a vital tool that shields computers and associated data from all sorts of online threats (George et al., 2023). As societies modernize, the field of study focused on cybersecurity concerns and protection has expanded considerably, with greater emphasis placed on the accounting discipline. There are concerns with storing sensitive financial data and information in decentralized computerized accounting systems, online transactions, and cloud-based financial management systems that have exacerbated the vulnerability of cyber threats and incidents, including phishing, malware, ransomware, and data breaches (Richardson, 2020; Von Solms & Langerman, 2020). Put simply, accountants keep and store confidential financial records, but practitioners encounter unique hurdles to protecting the integrity of accounting. Even though the emphasis on the importance of cybersecurity has increased, there has not been an equally increasing preparedness on the part of the growing population of students and professionals in the accounting area to guard against cyber threats (Al- Awadi & Renaud, 2020).

This gap in cybersecurity education highlights the importance of conducting field studies that measure the level of awareness among students in business-related programs, particularly accounting students of Dalubhasaang Politekniko ng Lungsod ng Baliwag,

who are expected to handle sensitive financial data in their future professions. Without adequate cybersecurity awareness and education, institutions and organizations may become more vulnerable to cyber threats, potentially resulting in financial losses, damaged business reputations, and disruptions to critical services, a concern emphasized by Von Solms and Van Niekerk (2013).

In particular, this investigation seeks to determine the awareness level of cybersecurity risks among accounting students, identify the specific cybersecurity threats most recognized by accounting students, examine the cybersecurity practices currently being used by accounting students to protect their personal and academic data, evaluate accounting students' understanding of the importance of cybersecurity in their future professional careers, and provide recommendations for enhancing cybersecurity awareness and practices among accounting students according to the study results.

This study on the Level of Awareness of Cybersecurity Risks Among Accounting Students at Dalubhasaang Politekniko ng Lungsod ng Baliwag reflects the contributions of several key individuals and institutions. The study adds knowledge on the preparedness of future accountants, as demonstrated by the findings. According to Dapital et. al (2024), considering that places or institutions can have various environments of cybersecurity, this

research study may contribute by generating institution-specific insights that will help improve cybersecurity awareness.

The recommended practices from the research outcomes will improve educators' and policymakers' work in developing programs designed to optimize responsible digital behavior and increase awareness of data protection practices. Additionally, the research centers on improving literacy around cybersecurity as part of an intended goal of enhancing the prepared accounting profession, where the work of the profession is ethical, secure, and competitive.

2. Review of Related Literature

2.1. Awareness of Cybersecurity

Cybersecurity awareness in the Philippines is still a developing topic as technology continues to impact education, business, and finance. Omorog and Medina (2020) pointed out that while the general population of Filipino internet users are aware of basic safety practices online, a large majority do not practice safety measures regularly to the extent that the user's personal and sensitive information can be compromised. This is particularly true for accounting students, whose future careers revolve around managing sensitive financial data that requires a high degree of security and ethical handling.

This is consistent with the work of Omorog and Medina (2018), where Filipinos showed inadequate internet security habits related to proper password protection, antivirus software usage, and sharing of personal information. Assessing the body of research, reassurance cannot be made that awareness leads to proper cyber behavior at all times, indicating the necessity to better educate cybersecurity at every level.

Moreover, recent findings from Purnell's (2023) World Economic Forum survey indicated that the Philippines ranked 27th globally in cybersecurity literacy, which is considered to be around an average level. While this demonstrates an average understanding of appropriate cybersecurity practices, it does indicate that literacy of application and depth of understanding still requires more literacy. Again, this demonstrates the need for cybersecurity awareness in higher education, especially accounting where prospective accountants deal with sensitive information digitally and financially.

2.2. Phishing Awareness

Despite being one of the most prevalent types of cyberattack, phishing, on a worldwide level, involves taking advantage of human behavior rather than technical flaws. The fact that people are the weakest link in the cybersecurity chain is further supported by the Verizon Data Breach Investigations Report 2024, which revealed that phishing was a factor in 36% of data breaches globally.

Phishing is among the most common types of cyberattacks. It may be tempting to think phishing can only happen in the micro or personal sense in each instance, but on the macro or global level phish is one type of cyberattack that does typically use, and exploit, the behavior of human individuals, and not exploiting, or taking advantage of technical vulnerabilities. The Verizon Data Breach Investigations Report 2024 found in its global report that 36% of data breaches contained some aspect of phishing specific type attacks, again reflecting a situation where users are statistically seen to be the weakest in the link of the cybersecurity chain.

2.3. CyberThreats (Malware and Ransomware)

Worldwide, malware and ransomware are some of the most harmful and damaging cyber threats to individual persons, organizations, and to critical infrastructure. As reported by IBM Security (2024), ransomware attacks increased 27% over the last two years and the financial and healthcare industries are the primary victims. Malware is often transferred to a user's devices through malicious downloads, email attachments, or compromised websites.

The human element, as illustrated by Bada et al. (2019), is a significant vulnerability being used and exploited by malware campaigns. Without the knowledge of these potential risks, it is believed that users are more likely to open a malicious attachment or simply disregard a security alert. Ransomware attacks specifically involve the attacker encrypting the victims' data, and demanding some type of payment for the decryption keys, leading to financial and operational chaos (Europol, 2023).

Publicly and more recent breaches like the MOVE it in the spring of 2023, show the rapid pace ransomware can hitch a ride on an international network and remarkably impact hundreds of organizations and thousands of users in moments. These types of incidents are given for a multitude of reasons and provide experts, as consistently suggested around the world, can curb infection and assist users to be better prepared against pending and evolving cybersecurity challenges, like ongoing education and consistent and continual repetitive updating of systems.

2.4. Privacy Awareness

Privacy awareness is the awareness of how to safeguard personal data from unauthorized access, use and disclosure. Social media is used widely both in society and on college campuses in particular. The growth of social media sites has generated new sets of problems and issues of which we contend as a society in the 21st century. Nowadays the college students are encountering a new type of risk for reputational harm or financial loss from social media as it is their primary way of communication as compared to previous generations (Bhatnagar and Pry, 2020).

Privacy awareness on the part of university staff and all students is positively associated with compliance to existing data protection laws such as the Data Privacy Act. The higher the relevance of the audience to the organization or program, the greater the privacy awareness, which is seen in overall data management activities, lawfulness of data processing, and reporting obligations for breaches. Awareness programs are key to enhanced privacy protection policies in academic institutions and elsewhere (Miano, 2025).

2.5. Password Management

Password management is an essential aspect of cyber awareness that is often missed. A weak or reused password remains the most common cause of unauthorized access and data breaches (IBM Security, 2024). Shay et al. (2019) discovered users prefer convenience over security by reusing passwords across accounts or using predictable passwords. This practice puts users at risk of credential-stuffing attacks through compromised passwords from a breach applied to other services.

According to Aloul (2021), awareness programs should teach password creation, however, it should also communicate password hygiene regarding reusing passwords, enabling password managers, and updating each credential regularly. Continual password management is one of the pillars of personal and organizational cybersecurity resilience.

2.6. Cybersecurity in Financial Data Protection

The protection of financial data is the core of the trust in any digital finance system. Shillair et al. (2022) concluded that individuals who had a higher awareness of cybersecurity engaged in safer online financial behavior, such as checking payment portals and avoiding dubious apps. In the context of accounting education, Niemimaa and Niemimaa (2017) stated it is important to understand that an awareness of cybersecurity is technical, but is also ethical in value, for it is about understanding the value of client confidentiality in a digitized world, as well as professional responsibility.

Systems of cyber risks are direct factors influencing consumer trust and institutional stability systems. As digital banking and e-wallet services like GCash, Maya, and online payment systems continue to expand, the demand for financial consumer literacy of cybersecurity for consumers and finance professionals becomes more pressing.

2.7. Importance of Cybersecurity Awareness among Accounting Students

Cyberattacks can happen as a result of humans making errors, whether it is clicking on harmful links or opening attachments from unknown senders. According to Rebele and St. Pierre (2019) there is resistance to change by accounting academics, and accounting academics lack competency in fields such as cybersecurity. The lack of competency in accounting academics may lead to cybersecurity also not being taught in accounting education. Hackers often will attempt to acquire sensitive financial information that includes the company's operational information, transactional information, and personal information on clients (Eliza et al. 2024).

Accounting students need to be ready for a digital world, and accounting programs must be able to prepare students for that transition, as employers want work-ready candidates. Accounting students should gain knowledge on cybersecurity, so that it becomes a holistic area of knowledge, allowing them to more effectively assist in developing and implementing strong security strategies, and ultimately helping to protect their organization from the ever-growing threat of a cyber-attack, or other, larger cyber risks (Tauchman, 2021).

The main objective of the study is to assess the level of awareness of accounting students on privacy, cyber threats, and financial data protection in Dalubhasaang Politekniko ng Lungsod ng Baliwag.

1. What is the profile of accounting students in terms of:
 - (a) Academic program
 - (b) Gender
 - (c) Type of device used
 - (d) Frequently used online platform
2. What is the level of awareness of accounting students on the following:
 - (a) Privacy
 - (b) Cyberthreats
 - (c) Financial Data Protection
3. What is the perception of accounting students on the importance of cybersecurity in their future profession?
4. What is the perception of accounting students on the importance of cybersecurity training in the accounting curriculum?

3. Theoretical and Conceptual Framework

The research study adopted the Technology Threat Avoidance Theory (TTAT) formulated by Liang and Xue (2009). TTAT is a well-recognized framework that provides insight into how individuals evaluate and cope with information security challenges. As stated in the theory, individuals' motivation to avoid IT-related threats is influenced by the two primary cognitive processes, (1) threat appraisal and (2) coping appraisal.

Threat appraisal involves evaluating how serious a perceived risk through cybersecurity (e.g., data breaches, phishing assaults and malware) could be, and how likely an individual feels a given threat has a chance of occurring. In the case of accounting students, they are considering how much risk the threat of a cyberattack on their academic work would create if it were to happen to them in terms of the damage to their academic work, the malignancy to their personal information, or the impact on their future job responsibilities.

Coping appraisal involves assessing the perceived effectiveness of their security behaviors (response efficacy), the confidence in their ability to perform such actions (self-efficacy), and the perceived challenges or sacrifices associated with carrying them out (response cost). Accounting students' coping appraisal may involve how to create a password that is adequately strong, learning to identify a phishing email, setting up multifactor authentication, or even taking an active role in a cybersecurity training program.

As explained by Liang and Xue (2009), avoidance behavior is produced when individuals perceive both an intrinsic threat and an available coping strategy. Subsequently, to understand what awareness of cybersecurity entails for accounting students, it needs to be viewed through the lens of understanding both the threats and the confidence and ability to deal with those threats.

3.1. Conceptual Framework

The conceptual framework describes the multiple stages taken by the researchers in order to gather data to respond to the research questions.

The conceptual framework of this study illustrates the relationship between the level of awareness of accounting students and the risks associated with cybersecurity. The independent variable of the study is the level of awareness of accounting students, while the dependent variables are the awareness of privacy, awareness of cyber threats, and the protection of financial data.

The conceptual framework of the study acts as a guide in examining the linkage between the level of awareness of accounting students and their awareness of the cybersecurity issues associated with the accounting profession. In addition, the conceptual frame-

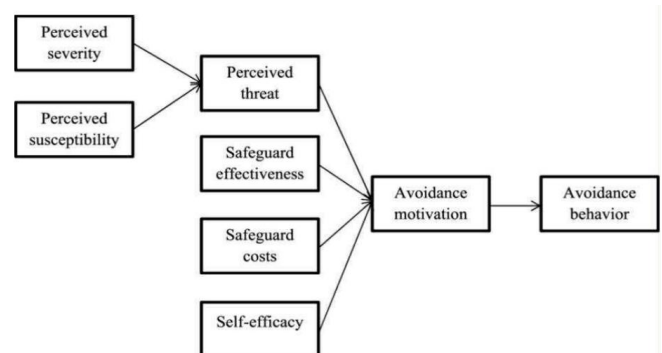


Figure 1. Theoretical Framework

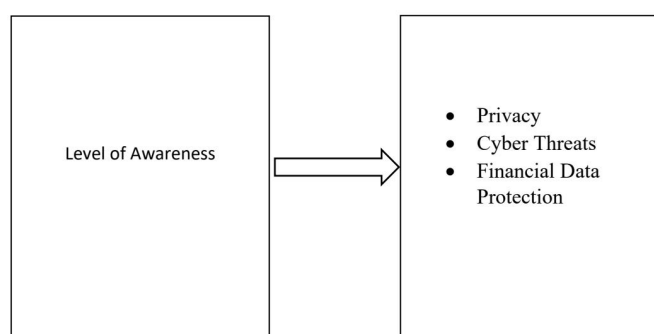


Figure 2. Conceptual Framework

work of the study shows the linkage between the level of awareness of accounting students at Dalubhasaang Politekniko ng Lungsod ng Baliwag and their capacity to identify cyber threats, safeguard personal and financial data, and protect sensitive accounting data. The conceptual framework of the study will enable the study to evaluate the overall level of awareness of accounting students on cybersecurity.

4. Method

This chapter outlines the research methodology. The research design includes sampling, data collection methods and analysis procedures and the ethical considerations involved in conducting the research.

4.1. Research Design

This study uses a descriptive method of quantitative research design to gain a detailed understanding of the level of awareness on cybersecurity risks among accounting students in Dalubhasaang Politekniko ng Lungsod ng Baliwag. According to Creswell (2014), a quantitative research design is used to examine relationships among variables using statistical analysis, allowing researchers to measure attitudes, behaviors, or opinions numerically. The descriptive method involves gathering information about the students' knowledge, perception, preparedness, and protective behavior toward various cybersecurity risks without manipulating any variables.

The respondents were given a survey questionnaire to complete in order to collect data for this study. Closed-ended questions will be included in the survey to gather quantitative information on accounting students' awareness of cybersecurity risks like ransomware, phishing, hacking, identity theft, and data breaches. The tool will be meticulously designed to guarantee that the replies gathered are precise, trustworthy, and adequate for examination.

4.2. Sampling

A stratified sample of potential participant groups was selected from Dalubhasaang Politekniko ng Lungsod ng Baliwag, which allowed for equal representation of all potential participant groups in data collection. The total target population consisted of fourth-year students, who were identified as having sufficient academic maturity and experience to participate in the evaluation of their cybersecurity awareness levels.

The specific programs included the Accounting Students in the area of study of Accounting: BSA, BSMA, BSAIS, and BSIA which represented four very similar accounting programs and allowed the researchers to collect opinions from the full range of the accounting area of study. Fourth year students were

selected for this group because of the advanced coursework and practical experience and they would therefore be able to provide knowledgeable and relevant opinions to address the research objectives and provide adequate and trustworthy data for the future career in the field of cybersecurity.

4.3. Respondents/Participants

The researchers focused on accounting students enrolled in Dalubhasaang Politekniko ng Lungsod ng Baliwag. A total of 70 accounting students participated in the study. These participants were taken from different academic programs, including Bachelor of Science in Accountancy (BSA), Bachelor of Science in Management Accounting (BSMA), Bachelor of Science in Accounting Information System (BSAIS), and Bachelor of Science in Internal Auditing (BSIA).

Table 1. Distribution of Participants According to Academic Program

Academic Program	Year Level	Number of Participants
Bachelor of Science in Accountancy (BSA)	4	7
Bachelor of Science in Management Accounting (BSMA)	4	21
Bachelor of Science in Accounting Information System (BSAIS)	4	19
Bachelor of Science in Internal Auditing (BSIA)	4	23
TOTAL		70

4.4. Instrument

In this research study, the researchers created a survey questionnaire that measures the degree of knowledge of the accounting students of Dalubhasaang Politekniko ng Lungsod ng Baliwag regarding the threat of cybersecurity. The design of the questionnaire was developed carefully to achieve the study's objective. It will collect appropriate information concerning how the students view cybersecurity awareness both in an educational setting and on a professional level.

The survey consisted of 4 parts with 54 total questions. The first section acquired demographic data regarding the participants. In the second portion, the respondents assessed whether they were aware or not of cybersecurity using a 1 (not aware) - 4 (very much aware) scale, and indicated whether they agreed or disagreed with a statement using 1 (strongly disagree)- 5 (strongly agree) scales for each of the questions. The objective was to evaluate the participants' understanding of Cybersecurity concepts and how they rated the importance of these concepts for them now and as they pursue their respective degree programs and future employment opportunities.

5. Results and Discussion

This chapter presents the results of the data gathered from graduating accounting students of Dalubhasaang Politekniko ng Lungsod

ng Baliwag regarding their level of awareness of cybersecurity and their perception of the importance of cybersecurity training in the accounting curriculum.

Table 2. Distribution of Respondents According to Their Academic Program

Academic Program	Frequency	Percentage %
BS in Accountancy	7	9.90
BS in Management Accounting	21	29.60
BS in Internal Auditing	23	33.70
BS in Accounting Information System	19	26.80
TOTAL	70	100

Most respondents in the study came from BS in Internal Auditing (33.7%, 23 students), followed by BS in Management Accounting (29.6%, 21 students), BS in Accounting Information Systems (26.8%, 19 students), and BS in Accountancy (9.9%, 7 students). Overall, the participants represent various accounting-related programs, offering diverse perspectives. Registrar records from Dalubhasaan ng Politekniko ng Lungsod ng Baliwag also show that Internal Auditing and Management Accounting have the highest number of graduates, while Accountancy has the fewest.

Table 3. Distribution of Respondents According to Gender

Gender	Frequency	Percentage %
Male	16	22.50
Female	54	77.50
TOTAL	70	100

Out of the 70 total respondents, 54 were females and thus made up 77.50% of the total group and 16 were males. Therefore, this data shows that most participants in the study are female. According to the official records from the registrar's office, the number of females enrolled is greater than the number of males.

Table 4. Devices Used by the Respondents for Accessing Digital Platforms

Device Used the Most	Frequency	Percentage %
Computer	16	22.86
Laptop	37	52.86
Tablet	18	25.71
Smartphone	62	88.57
TOTAL (Multiple Selection)	70	100

Most respondents primarily use smartphones, with 62 (88.57%) reporting usage, making it the most common device due to its convenience and accessibility. Laptops rank second with 37 users (52.86%), followed by tablets with 18 users (25.71%). Computers are the least used, with 16 respondents (22.86%). These results highlight the dominance of smartphones as the main tool for online access, consistent with DataReportal (2024), which notes that smartphones are the primary means of internet use in the Philippines due to their affordability and widespread availability.

Table 5. Online Platforms Frequently Used by the Respondents

Online Platform	Frequency	Percentage %
Social media	68	97.14
Online Banking	30	42.86
Email	39	55.71
Learning Management System (LMS)	46	65.71
Cloud Storage	33	47.14
TOTAL (Multiple Selection)	70	100

An analysis of the responses of the total of 70 people found that social media was the dominant medium identified, 68 respondents (97.14% of respondents). The next-most popular medium is the learning management system (LMS), with 46 respondents (65.71%) responding. Other identified media were email (39 responses, 55.71%), cloud storage (33 responses, 47.14%), and online banking (30 responses, 42.86%). The high rate of use of social media among participants may be related to how important they are for communication, information-sharing, and networking among participants. These findings are backed up by the Data Reportals (2024) report. It states that people in the Philippines use media a lot and a big part of those who use the internet are active on these platforms.

The findings show that respondents generally have a high level of awareness regarding online privacy, social media behavior, and cybersecurity practices. They understand the risks of oversharing personal information, such as identity theft and online harassment, and are knowledgeable about privacy settings and responsible social media use. Supporting studies (Bada et al., 2019; Dela Rosa, 2025) also confirm that increased awareness leads to safer online behavior among students.

However, while students are aware of website tracking technologies like cookies (WM = 3.37), their understanding of how these systems work may be limited. Respondents also recognize risks related to public Wi-Fi and shared devices, showing awareness of potential cyber threats like hacking and unauthorized access.

In terms of protection, students are familiar with cybersecurity measures such as password managers, two-factor authentication, and data backups, which help safeguard their accounts and information. They are also aware of laws that protect personal data. Overall, the results highlight strong cybersecurity awareness among respondents, but emphasize the need for continuous education to further strengthen safe and responsible online behavior.

The findings show that accounting students have a generally high level of awareness of cyber threats (WM = 3.37), indicating they are fairly knowledgeable about risks affecting personal data, devices, and internet use. The highest awareness is seen in identity theft (3.64) and the risks of sharing personal information on social media (3.63), suggesting strong sensitivity to privacy-related threats.

Students are also aware of various cyber risks such as hacking, AI-driven attacks, malware, data breaches, insider threats, and social engineering, which is important given their future roles in handling financial and digital systems. However, awareness is slightly lower for more technical threats like ransomware

Table 6. Level of Awareness of Respondents on Privacy Awareness

Statement	Weighted Mean	Interpretation
I am aware of the risks involved in sharing personal information on social media platforms.	3.81	Strongly Aware
I am aware of privacy settings on social media and how to adjust them for better protection.	3.64	Strongly Aware
I am aware of the potential consequences of oversharing location or personal details online.	3.81	Strongly Aware
I am aware of how cookies and online trackers can affect my privacy.	3.37	Strongly Aware
I am aware of how public Wi-Fi networks can pose risks to my personal data.	3.46	Strongly Aware
I am aware that password managers can securely store and generate unique passwords.	3.51	Strongly Aware
I am aware that privacy laws (e.g., Data Privacy Act) exist to protect personal information.	3.57	Strongly Aware
I am aware that enabling two-factor authentication (2FA) adds extra security.	3.49	Strongly Aware
I am aware of the importance of backing up personal data securely.	3.66	Strongly Aware
I am aware of the risks of using shared computers for accessing personal accounts.	3.69	Strongly Aware
TOTAL	3.60	Strongly Aware

Table 7. Level of Awareness of Respondents on Cyber Threats

Statement	Weighted Mean	Interpretation
I am aware of the risks involved in sharing personal information on social media.	3.63	Strongly Aware
I am aware that malicious software (viruses, spyware) can put personal data at risk.	3.41	Strongly Aware
I am aware of ransomware, which locks files and demands payment to restore access.	3.06	Aware
I am aware of data breaches where hackers expose private records.	3.39	Strongly Aware
I am aware that hacking involves unauthorized access to computer systems or data.	3.51	Strongly Aware
I am aware of identity theft, where stolen personal information is used fraudulently.	3.64	Strongly Aware
I am aware that social engineering involves manipulating individuals into divulging data.	3.33	Strongly Aware
I am aware that DDoS attacks disrupt websites or networks for extortion purposes.	2.97	Aware
I am aware of insider threats where a person with access could leak data or install malware.	3.34	Strongly Aware
I am aware of AI-driven attacks (phishing bots, deepfakes) used for financial fraud.	3.44	Strongly Aware
TOTAL	3.37	Strongly Aware

(3.06) and DDoS attacks (2.97), indicating a need for deeper understanding in these areas.

Overall, the results highlight that while students demonstrate good cybersecurity awareness especially in personal data protection, continuous education is necessary to strengthen their knowledge of more complex cyber threats and promote safer online behavior.

Table 8. Level of Awareness of Respondents on Financial Data Protection

Statement	Weighted Mean	Interpretation
I am aware of the need to protect financial information from unauthorized access.	3.73	Strongly Aware
I am aware of the risks involved in the online handling of financial information.	3.69	Strongly Aware
I am aware of basic procedures for protecting financial data (strong passwords, etc.).	3.63	Strongly Aware
I am aware of the importance of encryption to safeguard financial data.	3.64	Strongly Aware
I am aware of the implications that cybersecurity concerns can have on financial statements.	3.51	Strongly Aware
I am aware that sharing financial information through unsecured channels can compromise data.	3.66	Strongly Aware
I am aware of the need to back up financial and accounting data to prevent data loss.	3.63	Strongly Aware
I am aware of the importance of access controls in limiting who can view financial data.	3.67	Strongly Aware
I am aware of the importance of verifying emails and links before accessing financial data.	3.67	Strongly Aware
I am aware that failure to protect financial data may result in audit issues.	3.67	Strongly Aware
TOTAL	3.65	Strongly Aware

The results show that respondents are highly aware of how to protect their financial data, with a strong overall awareness level (WM = 3.65). They understand the importance of safeguarding financial and accounting information, using strong passwords, secure networks, and data encryption, as well as recognizing the risks of online transactions.

Respondents also demonstrate broader cybersecurity knowledge, including identifying threats like identity theft, fraud, and data loss, as well as practicing safe behaviors such as verifying email sources, controlling data access, and backing up information. Their consistently high responses suggest they are well-prepared to apply secure practices in real-life situations.

Overall, the findings confirm that students have strong awareness of financial data protection, supported by studies like Alampay et al. (2020), which highlight increased cybersecurity awareness among Filipino students due to greater use of digital technologies.

The findings show that accounting students strongly recognize the importance of cybersecurity for their future careers, with an overall high agreement (WM = 3.77). They believe that cybersecurity knowledge is essential for protecting the integrity of accounting records, securing confidential financial data, ensuring ethical practices, and complying with accounting standards.

Students also agree that cybersecurity awareness helps prepare them for professional responsibilities and enables them to handle financial information safely. Their consistently high ratings indicate that they understand the role of cybersecurity in maintaining trust, credibility, and protection against potential digital threats in accounting systems.

Overall, the results highlight that students view cybersecurity as a critical skill for success in the accounting profession, supported by studies showing that increased awareness and training improve preparedness for real-world cyber risks.

The results show that graduating accounting students strongly agree on the importance of integrating cybersecurity training into the accounting curriculum, with an overall weighted mean of 3.71. All statements received high ratings, with the highest at 3.81, indicating strong support for cybersecurity education.

Students consistently recognize that cybersecurity training is essential for developing the skills needed to protect financial systems and meet professional and employer expectations. Even the lowest-rated statement still falls under "Strongly Agree," reinforcing the overall positive perception.

Table 9. Perception of Accounting Students on the Importance of Cybersecurity in the Future Profession

Statement	Weighted Mean	Interpretation
Knowledge in cybersecurity is important for future careers as accounting professionals.	3.76	Strongly Agree
Cybersecurity awareness can help accounting students perform future duties more effectively.	3.71	Strongly Agree
Cybersecurity has an important role in maintaining trust and integrity in accounting.	3.74	Strongly Agree
Accounting jobs often require handling sensitive info; thus, knowledge is important.	3.79	Strongly Agree
Lack of cybersecurity knowledge may contribute to ethical lapses in accounting.	3.76	Strongly Agree
Understanding the importance of cybersecurity is essential for reliable accounting info.	3.81	Strongly Agree
Accounting students benefit from understanding risks associated with digital systems.	3.73	Strongly Agree
Implementing cybersecurity best practices helps comply with principles, laws, and regulations.	3.79	Strongly Agree
Understanding cybersecurity enables accountants to respond to breaches more effectively.	3.77	Strongly Agree
Cybersecurity knowledge is important for safeguarding financial records and info systems.	3.79	Strongly Agree
TOTAL	3.77	Strongly Agree

Table 10. Perception of Graduating Accounting Students on the Importance of Cybersecurity Training in the Accounting Curriculum

Statement	Weighted Mean	Interpretation
Cybersecurity training should be a required component for all graduating students.	3.76	Strongly Agree
Without training, accounting students may be less prepared for digital threats.	3.61	Strongly Agree
Cybersecurity training would improve students' ability to identify and prevent fraud.	3.79	Strongly Agree
Including cybersecurity in the core curriculum would enhance accounting education quality.	3.64	Strongly Agree
Making cybersecurity core would better align education with industry demands.	3.63	Strongly Agree
Accounting students must learn about cybersecurity to safely handle financial data.	3.70	Strongly Agree
Cybersecurity training increases students' confidence in using digital systems.	3.76	Strongly Agree
Cybersecurity evolves rapidly, and training must encourage continuous education.	3.70	Strongly Agree
Cybersecurity training would make accounting classes more relevant to real-life.	3.70	Strongly Agree
Cybersecurity Education is important to reduce instances of errors or risk.	3.81	Strongly Agree
TOTAL	3.71	Strongly Agree

6. Conclusion

The researchers arrived at the following conclusions upon analyzing the gathered summary of findings:

The study shows that accounting students of Dalubhasaang Politekniko ng Lungsod ng Baliwag have a strong awareness of online privacy, common cyber threats, and the protection of financial data. They understand risks such as identity theft, hacking, and data breaches, and are knowledgeable about securing personal and financial information through passwords, encryption, and access control.

However, their awareness is lower when it comes to more complex threats like ransomware and DDoS attacks, indicating a need for deeper learning in these areas. Students also recognize the importance of cybersecurity in their future careers, believing it is essential for protecting financial data, ensuring accuracy and credibility, and complying with regulations. Furthermore, they strongly support integrating cybersecurity training into the accounting curriculum to better prepare them for real-world challenges.

Overall, while students demonstrate high awareness and positive attitudes toward cybersecurity, continuous education and curriculum integration are necessary to equip them with the skills needed to address evolving cyber threats.

7. Recommendation

After considering the foregoing findings and conclusions of the study, the following recommendations are presented:

1. **To Institutions:** It is recommended to organize regular (e.g. annual or per semester) training, seminars, webinars and hands-on simulation to increase awareness about cybersecurity among accounting students and include evaluation methods to measure students' cybersecurity knowledge and skills after training. Institutions can also collaborate with student-led organizations to develop and host corporate-wide events such as IBA style inter-departmental Cybersecurity Quiz Competition and/or workshops, and/or awareness events to promote active engagement. Additionally, Institutions should also ensure that faculty members are equipped with proper training in cybersecurity to effectively deliver instructions.
2. **To Graduating Accounting Students:** They are encouraged to actively pursue continuous professional development related to cybersecurity by obtaining certification, online courses, studying textbook references, and participating in continuing education seminars. This will help them stay updated with evolving cyber threats and security practices in the accounting profession.
3. **To Future Researchers:** It is recommended that they conduct similar studies involving a larger sample size, different academic programs, or other higher education institutions to further validate the findings. Researchers can also investigate other factors related to cybersecurity in the educational setting including the use of technological tools for developing cybersecurity skills, compliance results of educational institutions with the use of policies, and the effectiveness of training delivered to students on cyber safety and security.

■ ACKNOWLEDGMENT

The successful execution of this study was accomplished with the encouragement and support of many people and institutions, for which the researchers are forever grateful.

The researchers would like to start by thanking Almighty God for his continual guidance and blessing throughout this study.

To the Research Adviser, Mr. Jared P. Manalastas, LPT, MAED, for his invaluable guidance, support, and encouragement throughout the completion of this study.

To the research instrument validators, Mr. Renz V. Canlas, Ms. Ma. Niña A. Adriano, MPA, MALLE, and Ms. Analiza V. Verdillo, for their valuable time, expertise, and insightful recommendations in evaluating the survey questionnaire, which significantly enhanced the quality, clarity, and validity of the research instruments used in this study.

The researchers want to express a deep appreciation to the Dean of Institute of Business and Accountancy, Dean Ma. Socorro N. Bartolome, CPA, DBA, and Mr. Michael Angelo M. Manayao, CPA, MBA, CAP, Program Director of BSA, BSAIS, BSMA, and BSIA, for their invaluable support, guidance, and academic leadership, which greatly contributed to the successful conduct of this research study.

To Respondents who participated in this study. Their willingness to share their time, effort, and honest responses made this research possible.

To Families, for being a constant source of support and encouragement. Their sacrifices, unwavering support, and belief have greatly contributed to the researchers' determination to complete this study.

Finally, to the Researchers: Maricel C. Calimpusan, Daniella Wjotilla E. Cruz, Myrna S. Marcelo, Mayriel T. Nocos, Charles Denzel P. Seradilla, Aileen S. Tanjoco, and Charmaine R. Vistan for their dedication, teamwork, and collaborative efforts, which contributed significantly to the successful completion of this study.

■ REFERENCES

- [1] Ahamed, B., Polas, M. R. H., Falahat, M., Rahman, M. M., & Khan, A. M. (2025). Cybersecurity knowledge, social networking, and awareness among Generation Z university students. *Journal of Information Systems and e-Business Management*, 23, 122. <https://link.springer.com/article/10.1007/s44217-025-01084-3>
- [2] Alabab, J. R., Cruz, M. A., & Villamor, K. L. (2024). Cybersecurity awareness of college students in a private higher education institution. *CGCI International Journal of Advances in Management and Technology*, 6(1), 45-56.
- [3] Alipio, M. M. (2022). Cybersecurity awareness of college students in a private higher education institution in the Philippines. *International Journal of Advanced Management and Technology*, 1(1), 1-9. <https://www.cgciijamet.org/index.php/cgciijamet/article/view/26>
- [4] Aloul, F. (2021). The importance of password security: Practices and user behavior analysis. *International Journal of Information Security and Cybercrime*, 10(3), 37-46.
- [5] Alshammari, R., Alabdulwahab, A., & Alshahrani, A. (2021). Assessment of cybersecurity awareness among undergraduate students. *Information*, 12(2), 23. <https://www.mdpi.com/2504-2289/5/2/23>
- [6] Bada, A., Sasse, M. A., & Nurse, J. R. C. (2019). Cybersecurity awareness campaigns: Why do they fail to change behavior? *Computers & Security*, 87, 101579. <https://scite.ai/reports/cyber-security-awareness-campaigns-why-908QExl4>

- [7] Booc, N. B. B. (2021). Cybersecurity awareness and behavior of senior high school students in Davao City. *European Journal of Applied Science and Technology*, 4(3), 112-120. <https://ejaset.com/index.php/journal/article/view/49>
- [8] Camti, R. L., Balangcod, K. A., & Ulep, J. P. (2025). Exploring cybersecurity strategies and awareness in the University of the Cordilleras. *SSRN*.
- [9] De Ramos, M. C., & Esponilla, F. T. (2022). Cybersecurity program for Philippine higher education institutions. *International Journal of Educational Research and Evaluation*, 8(3), 34-49.
- [10] Dela Cruz, J. P., & Santos, R. L. (2024). Examining cybersecurity awareness among college students in Laguna, Philippines. *International Journal of Future Management Research*, 3(1), 45-58. <https://www.ijfmr.com/papers/2025/3/41945.pdf>
- [11] Europol. (2023). Internet organized crime threat assessment (IOCTA) 2023. <https://www.europol.europa.eu/publications-events/main-reports/internetorganised-crime-threat-assessment-iocta-2023>
- [12] Florendo, A. P., Dizon, R. M., & Hernandez, L. S. (2025). Examining cybersecurity awareness among college students in selected higher education institutions in Laguna. *International Journal for Multidisciplinary Research*, 7(2), 1-12.
- [13] Moallem, A. (2020). *Cybersecurity awareness among students and faculty*. Routledge. <https://www.routledge.com/Cybersecurity-Awareness-Among-Students-and-Faculty/Moallem/p/book/9780367144074>
- [14] National Institute of Standards and Technology. (2023). Digital identity guidelines: Authentication and lifecycle management (SP 800-63B). <https://csrc.nist.gov/pubs/sp/800/63/b/upd2/final>
- [15] Palarca, J. M., & Flores, E. C. (2020). Cybersecurity awareness and educational outcomes of learners in Philippine public schools. *International Journal of Innovative Science and Research Technology*, 5(8), 890-896.
- [16] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., & McCormac, A. (2019). The human aspects of information security: Awareness, behavior and culture. *Computers & Security*, 85, 102-112.
- [17] Payne, B. R., Abegaz, T., & Antonia, M. (2021). Raising cybersecurity awareness among college students through experiential learning. *Journal of Cybersecurity Education, Research and Practice*, 2021(1), 1-12.
- [18] Reyes, J. A., & Maligaya, K. D. (2022). A students' perspective on cybersecurity awareness and education at Catanduanes State University. *International Journal of Research in Information Science and Technology*, 6(2), 15-25.
- [19] Santelices, J. M. (2025). A students' perspective on cybersecurity awareness and education. In *Proceedings of the International Conference on Emerging Trends in Information Security*. SSRN.
- [20] Symantec. (2023). Internet security threat report 2023. <https://www.broadcom.com/company/newsroom/pressreleases?filtr=security>
- [21] Verizon. (2024). 2024 data breach investigations report. <https://blog.qualys.com/qualysinsights/2024/05/01/verizons-2024-dbir-unpacked-from-ransomware-evolution-to-supply-chain-vulnerabilities>
- [22] Yoon, C., & Rolland, E. (2015). Internet security and privacy awareness among college students. *Journal of Information Privacy and Security*, 11(2), 74-88. <https://doi.org/10.1080/15536548.2015.1073517>
- [23] BTECH Baliwag - Office of the Registrar. (2025). Student demographic profile. <https://btech.edu.ph>
- [24] Philippine Statistics Authority (PSA). (2024). National ICT Household Survey 2024. <https://psa.gov.ph/content/percentage-households-internet-connection-increased-488-percent-2024-two-every-three>
- [25] Philippine Statistics Authority (PSA). (2025). Internet Usage and Device Statistics. <https://newsbytes.ph/2025/07/23/ph-internet-access-usage-soared-in-2024-govtsurvey/>
- [26] DataReportal. (2024). Digital 2024: Philippines. <https://datareportal.com/reports/digital-2024-philippines>
- [27] Department of Information and Communications Technology. (n.d.). ICT statistics. <https://dict.gov.ph/ictstatistics/>
- [28] Philippine Statistics Authority. (n.d.). Information and communications technology (ICT) statistics. <https://psa.gov.ph/statistics/ict>
- [29] Alabab, M. C., Dizon, N. R., & Garcia, L. P. (2023). Cybersecurity awareness of college students in a private higher education institution in Nueva Ecija, Philippines. *International Journal of Computing Sciences Research*, 7, 1123-1135.
- [30] Dela Cruz, J. M., & Santos, K. A. (2025). Cybersecurity awareness among college students: Implications for data privacy and online behavior. *Asian Journal of Education and Social Studies*, 10(1), 45-56.
- [31] Bautista, A. L., & Mendoza, R. S. (2022). Cybersecurity awareness and practices among students in Davao City. *Eurasian Journal of Applied Sciences, Engineering and Technology*, 5(3), 78-85.
- [32] Cabaltica, R. B., & Calibjo, M. A. (2019). Cybersecurity awareness among selected educational institutions in Butuan City, Philippines. *International Journal of Advanced Trends in Computer Science and Engineering*, 8(1), 135-140.
- [33] De Leon, M. J., & Diaz, P. R. (2024). Cybersecurity awareness among senior high school students in Tanza, Cavite: Basis for a cybersecurity education program. *International Journal of Research in Education and Science*, 10(2), 210-225.
- [34] Marcial, D. E. (2020). Internet security awareness of Filipinos: A survey paper. *International Journal of Computing Sciences Research*, 4(2), 250-266.

- [35] Dela Rosa, A. P. M. (2025). Assessing Data Privacy Attitudes of Information Technology Students: Basis for Awareness Enhancement. *International Journal of Multidisciplinary: Applied Business and Education Research*, 6(10), 4952-4962.
- [36] Zwillling, M., Klien, G., Lesjak, D., Wiechetek, M., Cetin, F., & Basim, N. (2020). Cybersecurity awareness, knowledge and behavior: A comparative study. *ScienceDirect*.
- [37] Escobar, D. T. C. (2022). Cybersecurity knowledge of the Cagayan State University academic community: Basis for cybersecurity policy. *Journal of Positive School Psychology*, 6(5), 4839-4850.
- [38] Santelices, R. B. (2025). A students' perspective on cybersecurity awareness and education. *International Journal of Research and Innovation in Social Science*. <https://doi.org/10.47772/IJRISS.2025.903SEDU0597>