TECHNIUM
SOCIAL SCIENCES JOURNAL

www.techniumscience.com

Vol. 71/2025

A New Decade for Social Changes

PLUS COMMUNICATION
International Communication & PR

Technium Social Sciences Journal
Vol. 71, 215-232, May, 2025
ISSN: 2668-7798
www.techniumscience.com

Cybersecurity Awareness and Practices Among Criminal Justice Students in One Higher Educational Institution in Cordillera

Claire D. Rufino[1], Warren G. Moyao[2]

[1]Faculty Member, Pangasinan State University – Binmaley Campus Binmaley, Pangasinan, Philippines, [2]Program Chair, Bachelor of Forensic Science, University of Baguio, Baguio City, Philippines

clairerufino214@gmail.com, warren.moyao@e.ubaguio.edu

Abstract. Cybersecurity has emerged as an essential component of contemporary living in the digital realm, where practically all transactions, including those of students, occur online. The study attempts to determine the present degree of student awareness to potentially identify cybersecurity vulnerabilities in their operations. A survey employing Likert-scale questions was conducted among college students pursuing criminal justice degrees to assess their cybersecurity understanding, experiences, and practices. The acquired data were analyzed via descriptive statistics. Students exhibit a considerable understanding of established cybersecurity issues; yet they continue to engage in minor problematic behaviors, particularly with social networking, which remains susceptible to exploitation by cyber offenders. Consequently, additional efforts are encouraged not only to promote awareness but also to translate awareness of cybersecurity issues into tangible behaviors.

Keywords. cybersecurity, social networking, cybercrimes, collegiate cybersecurity awareness

1. Introduction

The world is home to seven billion people, one-third of which are using the Internet. 45% of the world's Internet users are below the age of 25 [1].The United Nations Office on Drugs and Crime reports that in less than two decades the Internet has evolved from a curiosity to a need for millions of people [2]. Like other spheres of globalization, its fast development has exceeded regulatory capacity, permitting several rounds of misuse. To compound the problem, the Internet was developed on a military framework to avoid intervention and outside rules.

Cybercrime covers hacking, phishing, content, and copyright violations [3]. The hostile one-upmanship of cyber-vandals has rapidly developed into a range of profit-making illicit businesses. Like everyone else, criminals use the Internet for information gathering and communication, which has supported various kinds of coordinated crime activity. Our reliance on the Internet and its increasing relevance have created many fresh criminal opportunities.

More than one-third of the world's population, 2.3 billion people, had internet access in 2011 [1]. Of the internet users, 45% are under 25 while over 60% are in developing nations.

Technium Social Sciences Journal
Vol. 71, 215-232, May, 2025
ISSN: 2668-7798
www.techniumscience.com

By 2017, about seventy percent of people on the planet will have mobile broadband. By 2020, the "Internet of Things" will surpass individuals six to one, redefining our perspective of the Internet.

United Nations research on cybercrime found that worldwide connectivity has increased as the economy and population have changed [4]. Income inequality is expanding, private sector spending is falling, and money is scarce. The study's law enforcement participants believe cybercrime is rising worldwide. Because individuals and organized criminal groups are taking advantage of new criminal opportunities to gain money and improve their lives. Up to 80% of cybercrime begins with organized activity. Cybercrime underground economies involve developing malware, infecting computers, operating botnets, gathering, and selling personal and financial data, and "cashing out" financial information. Cybercriminals no longer need complex skills or strategies. Some developing country youth commit computer-related financial fraud.

1.1. Literature Review

According to Internet World Stats, sixty million Filipinos used the Internet in January 2017 [5]. The Philippines has the fastest Internet penetration growth, exhibiting no signs of slowing. This rise has enabled the government to launch and extend its online operations, affecting business, academics, and health. Online banking, credit card transactions, and electronic data interchange are expected to rise. However, this development and accessibility of usage have generated security problems in the Philippines. Online platforms and local news outlets have reported cybercrime, including identity theft, online fraud, and financial institution cyberattacks. In August 2016, the Department of Health (DOH) website was hacked to steal BPI cardholder data. The Philippine central bank, Bangko Sentral ng Pilipinas (BSP), disclosed a cyberattack in April 2016. The BSP governor claims the attack only affected its website and not its financial system. Cyber-attacks are rampant, according to reports.

Anonymous Philippines breached the Philippine Voters' Database server in March 2016, exposing at least 54 million sensitive data records, including 1.3 million passport numbers of Filipino expatriates. SQL injection breached the system. Hacking, defacement, and DDoS attacks hit at least sixty-eight government websites that year [6]. The Philippines has faced cyber espionage. In 2016, a Finnish security firm found malware targeting government and private data. Remote Access Trojans (RATs) are viruses that masquerade as harmless files. When executed, it infiltrates the victim's machine and sends intelligence to the attacker [7].

Though computing has been around since the beginning, awareness of data security and sanctity did not take off until the internet's explosive growth, which gave hackers a playground to bring down websites, steal data, and commit fraud. Viruses and malware precede this. Cybercrime is the current term. Hardware, software, policy, and people work together to prevent or mitigate cybercrimes. This involves cybersecurity [8].

Cybersecurity encompasses a variety of techniques aimed at protecting the cyber environment of individuals and organizations. It is concerned with maintaining the integrity of networks, programs, and data against unauthorized access and includes a range of technologies and processes. The significance of cybersecurity is escalating due to the increasing dependence on computer systems [9].

Cyber threats have grown increasingly intricate and varied, leading to situations where Internet users lacking proper cybersecurity awareness may unknowingly fall victim to attacks or even become perpetrators themselves. As a result, the rise of the Internet and mobile technology has led to greater use of computers, smartphones, and other devices for transactions,

Technium Social Sciences Journal
Vol. 71, 215-232, May, 2025
ISSN: 2668-7798
www.techniumscience.com

processing, transmission, and storage of information. It is crucial for public awareness and understanding of cybersecurity to extend to enough users [10].

In 2016, the Philippine Congress passed Republic Act No. 10844, The Creation of the Department of Information and Communications Technology, to adapt to the changing information and communications technologies, the Internet, and cyberspace. R.A. 10844 created a National Agency to address ICT concerns. Republic Act No. 10175, or the Cybercrime Prevention Act of 2012 formed the Cybercrime Investigation and Coordinating Center (CICC)and the National Privacy Commission (NPC), which was created under the Data Privacy Act of 2012. The NTC, CICC, and NPC were affiliated to the DICT.

The Philippine government's strategic objectives focus on technical, administrative, and procedural measures, according to the Department of Information and Communication Technology's National Cybersecurity Plan 2022. The strategy includes three programs: (a) strengthening government, public, and military networks to withstand sophisticated attacks; (b) promoting cybersecurity among individuals and businesses; and (c) growing the cybersecurity expert pool.

Global cybersecurity has been affected by the coronavirus outbreak. Phishing and contact-tracing scams use uncertainty and fear. Economic aid and unemployment benefits are targeted by fraudsters. Healthcare and other critical infrastructure ransomware attacks are riskier than ever. Businesses face new and increased risks due to remote work [11].

To ensure learning continuity during the COVID-19 pandemic, schools across are closing, restricting travel, and adopting remote or distance learning approaches. Cybersecurity and privacy must be considered before using technology to teach. Students and instructors face security and privacy hazards if cybersecurity and privacy are ignored until the end of planning and implementation.

Higher education students are aware of smartphone security issues, but not all hazards and best practices [12]. Training and awareness campaigns after finding vulnerabilities in industrial control systems due to poor password management, unpatched software, and outdated anti-virus and malware protection. These studies show that cybersecurity attitudes, knowledge, and behavior may differ [13].

When security methods are too complicated, users may try to bypass controls, undermining past and existing awareness attempts. For positive behavior and attitude change, information transfer, awareness, and influencing tactics are needed [14]. Cybersecurity training requires a baseline of cybersecurity perceptions, attitudes, knowledge, and abilities and their interrelationships [15].

The consensus that emerged from these pieces of literature is that education and training are essential actions that should be undertaken to raise awareness and improve behaviors that are not satisfactory in terms of internet security. The research also implies that knowledge, self-perception of skills, actual skills and behaviors, and attitudes are all essential in assessing cybersecurity awareness. Furthermore, the studies suggest that knowledge alone is often insufficient to ensure that knowledge is often a weak variable.

1.2. Theoretical Framework

The study will employ a modified theory of planned behavior (TPB) framework like Figure 1. The TPB framework, proposed by Icek Ajzen, was suitable because it has been used to study people's ethical behavior and decisions regarding computer security, including adoption and compliance. Since the TPB framework does not explicitly incorporate cybercrime awareness, Chandarman and Niekerk's () customized version will be employed. Their variables and connections were based on cybercrime awareness research. Accordingly, the adapted

Technium Social Sciences Journal
Vol. 71, 215-232, May, 2025
ISSN: 2668-7798
www.techniumscience.com

version of the TPB framework investigated CSA via a focus on relationships among four core variables: (1) knowledge, (2) self-perception of skills, (3) actual skills and behavior, and (4) attitudes.

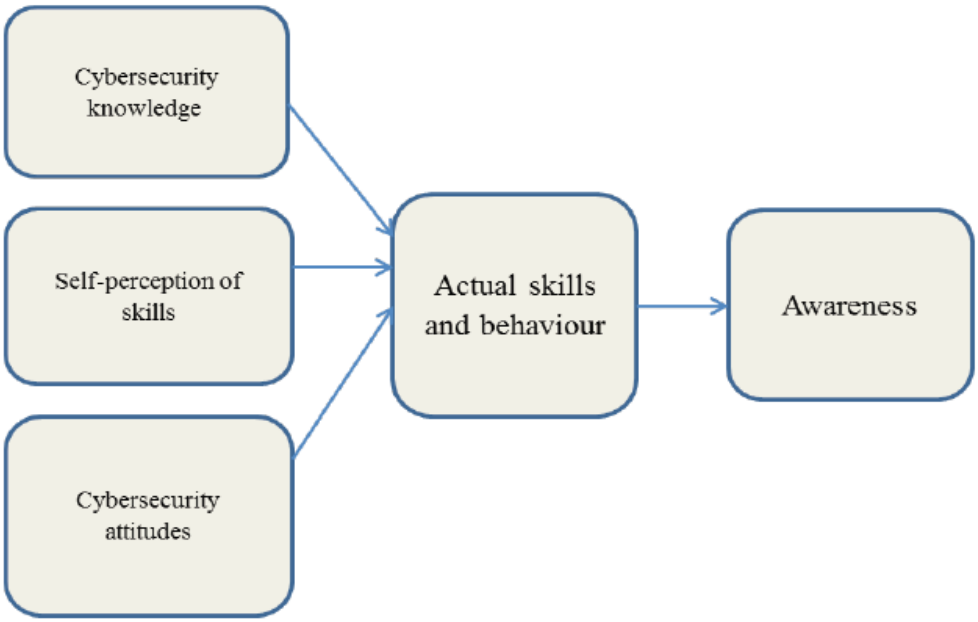

Figure 1. Adapted TBP Framework for Cybersecurity Awareness

In the Philippines, the legal framework for cybersecurity is primarily Republic Act 10175 or the Cybercrime Prevention Act of 2012 which was signed into law by President Aquino on Sept. 12, 2012. It aims to protect and safeguard the confidentiality, integrity, and availability of data, computer and communications systems, networks, and databases and adopt mechanisms to effectively prevent and combat cyber offenses by facilitating their detection, investigation, and prosecution, at both the domestic and international levels.

Under the law, the acts punishable are classified into offenses against the confidentiality, integrity, and accessibility of computer data and systems or CIA offenses, computer-related offenses, and content-related offenses. CIA offenses include illegal access, illegal interception, data interference, system interference, and misuse of devices. Computer-related offenses involve acts that are originally punishable but were facilitated using computer devices including computer-related forgery, computer-related fraud, and computer-related identity theft. Lastly, content-related offenses include cybersex, child pornography, and cyber libel because of the illicit or immoral nature of its contents.

1.1. Research Paradigm

Figure 2 presents the study's paradigm and shows its process. The research aims to determine students' cybersecurity awareness by measuring their cybersecurity knowledge, perception of their cybersecurity skills, actual cybersecurity skills and behavior, and attitude. Furthermore, it aims to discover whether these factors correlate with each other.

Technium Social Sciences Journal
Vol. 71, 215-232, May, 2025
ISSN: 2668-7798
www.techniumscience.com

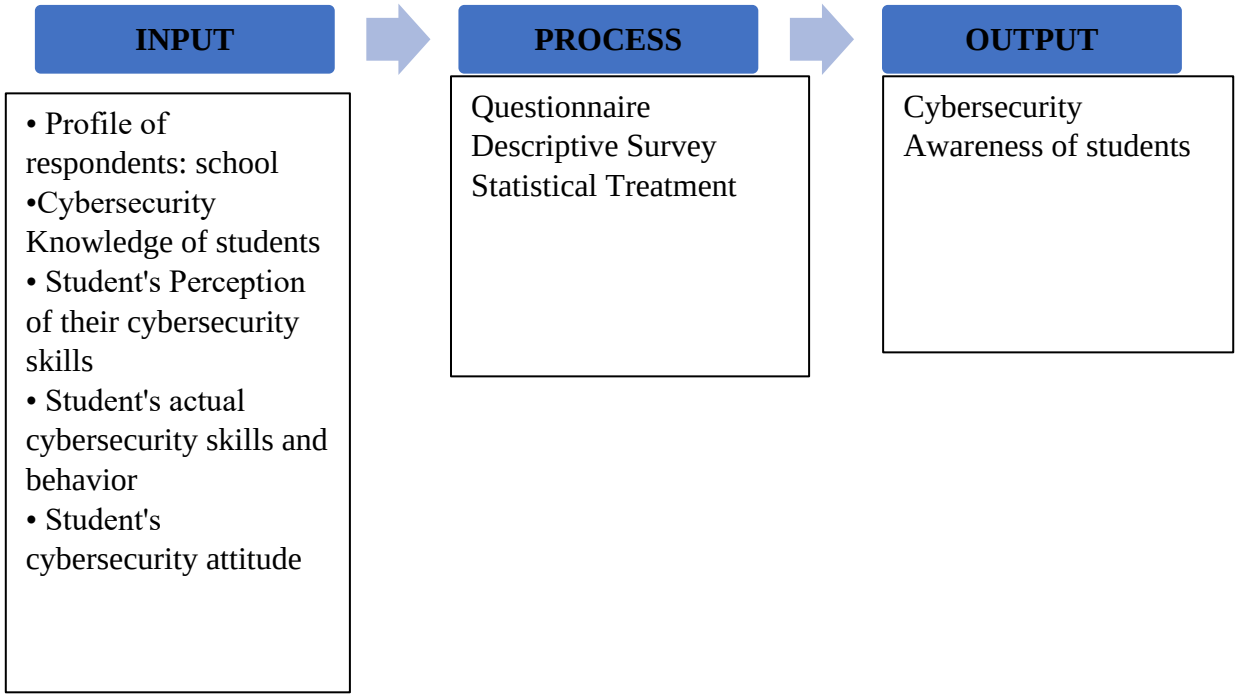

Figure 2. Paradigm of the study

1.3. Significance of the Study

Today's world is becoming increasingly dependent on technology, which has resulted in protecting sensitive information becoming an even more important issue than it was in the past. Cyber threats have the potential to disrupt organizations and influence individuals all over the world using personal data and financial activities. In addition, students are an essential component of the infrastructure of the cybersecurity scene. Students can become both targets and defenders against cyber dangers because of their activities on digital platforms. It is therefore essential to measure their knowledge in the campaign for promoting cybersecurity since it is necessary to recognize the gap between the awareness of students and the actual practice of cybersecurity. The findings may be useful in the development of more efficient educational programs covering cybersecurity.

1.4. Objectives of the Study

The use of computers, cell phones, and devices connected to the internet constantly rises in the educational sector because of online classes. At the same time, the trend of cybercrimes and cybersecurity breaches is also constantly on the rise. As students and educators use cyberspace now more than ever, this study aims for the following:

- To determine the level of awareness about cybersecurity threats of criminal justice students in a higher educational institution in the Cordillera
- To determine the level of cybersecurity practice of criminal justice students in a higher educational institution in the Cordillera

2. METHODOLOGY

2.1. Study Design

The study will employ the descriptive-survey research method. It will present the general computer-related activities of students, and awareness of the identified top cybersecurity concerns namely password security, browser security, email security, and social

Technium Social Sciences Journal
Vol. 71, 215-232, May, 2025
ISSN: 2668-7798
www.techniumscience.com

networking security. Through a survey, the self-perceived assessment of the above-enumerated cybersecurity concerns will be measured as well as their actual behavior.

2.2. Sample/Population of the Study

The study will be conducted among criminology and forensic science students for the summer term of the academic year 2023-2024. These students are actively engaged in the use of ICT considering that classes have been delivered to them virtually and are more exposed to social media and the internet. Furthermore, cybersecurity will be one of the concerns of these students as future professionals in the field of criminal justice especially investigation and forensic science. The study will use total enumeration in which all enrolled students will be asked to participate. Willing students will comprise the respondents of the study.

2.3. Data Gathering Tools

Data will be gathered through a survey questionnaire which will be administered online. A researcher-made questionnaire based on identified top cybersecurity concerns will be used.

The tool consists of four sections, each section measuring a piece of specific information necessary for analysis. Section 1 consists of the student's profile, specifically their school and overall computer or internet usage. Section 2 includes questions measuring the student's self-perceived level of cybersecurity awareness. Section 3 assesses the students' behavior and experience. Section 4 assesses the students' cybersecurity attitudes. These sections cover the top security concerns including password security, browser security, email security, and social networking security.

The questionnaire will undergo content validity by a tool validator before being administered.

2.4. Data Gathering Procedures

Considering the current virtual meetings for schools today, the survey questionnaire will be converted to an electronic copy using Google Forms. After seeking the permission of the Deans of each school in the University of Baguio, the researcher will ask for assistance from faculty members of each school in the distribution of the survey link to their respective students.

The respondents will be asked to complete the survey questionnaire. The questionnaire will comprise several sections, each having a purpose of its own. The preliminary section would be a message to the respondent explaining the nature of the research and requesting their voluntary participation by answering each item truthfully. Furthermore, it will explain to the respondents that data gathered from the questionnaire will be kept confidential and will be strictly used for research purposes only.

2.5. Treatment of Data

The raw data will be generated in a tabular form using Google Sheets and will be analyzed using Microsoft Excel. Descriptive statistics will be utilized to assess individual topics and variables. Both problems will undergo univariate analysis. For problem number one which is the awareness of students asked using the Likert scale, frequency count, mean and mode will be derived. In determining the level of cybersecurity practice, frequency and percentage will be used and presented in graphs.

2.6. Ethical Considerations

The study carefully followed the ethics of research from obtaining the permissions of the school deans and the respondents themselves before proceeding with the data gathering. No unnecessary information will be gathered other than what is required for the problems of the research. The respondents will be provided an informed consent form explaining that their participation is completely voluntary and that they may withdraw at any time of the study.

Technium Social Sciences Journal
Vol. 71, 215-232, May, 2025
ISSN: 2668-7798
www.techniumscience.com

Furthermore, the date they have submitted will be used exclusively for the study, and anonymity in the presentation of the results will be earnestly observed. After the completion of the survey, the respondents will be informed that they will expect the research paper, specifically the findings of the study, to be available at the library upon completion.

3. Results and discussion

This chapter presents the collected data along with the corresponding findings, analysis, and interpretation for each. The data collected from the retrieved questionnaires forms the foundation of the analysis and provides valuable insights into cybersecurity awareness and practices among criminal justice students in one higher educational institution in the Cordillera.

Out of 137 responses, almost half of the respondents' internet usage lasts from five to eight hours daily. A significant percentage also noted that their frequency of using the internet goes beyond eight hours. The widely used channel to access the internet is via the smartphone which is handy making it easier to have access anytime anywhere. Moreover, a laptop, tablet or iPad, and desktop computer are also among the top-used devices to access the internet. Additionally, the respondents' top purpose of accessing the internet is for academic purposes followed by the purpose of signing into social media. There is also quite a significant percentage of those who use it for gaming, and a few use the internet for work and other purposes.

3.1. Level of Awareness

Cybersecurity awareness is crucial since it helps people and companies to minimize data loss risks using appropriate information, therefore enabling their identification and handling of cyber threats.

Table 1
Awareness of Identified Cybersecurity Concerns

CYBERSECURITY CONCERNS	MEAN	INTERPRETATION
1. Securing and updating my devices regularly.	3.38406	Totally Aware
2. Ensuring my browser is secured.	3.32609	Totally Aware
3. Protecting my devices from malicious software (viruses, worms, spyware, etc.).	3.5	Totally Aware
4. Identifying scams or phishing attacks in emails and text messages.	3.52899	Totally Aware
5. Distinguishing between authentic and pirated software.	3.27536	Totally Aware
6. Using strong, unique passwords across different sites.	3.52174	Totally Aware
7. Reporting online harassment or bullying.	3.22464	Aware

Table 1 shows the responses of students on their awareness of the identified common cybersecurity concerns. For purposes of comparing the general awareness of students across

Technium Social Sciences Journal
Vol. 71, 215-232, May, 2025
ISSN: 2668-7798
www.techniumscience.com

these cybersecurity concerns, mean scores for each concern were also generated and presented in the figure.

Survey results show that the level of awareness of students regarding all the identified cybersecurity concerns is high. This is the most specific on identifying phishing and scam attacks and the use of strong passwords across different sites, both having mean scores of with the mean score of 3.55. Although still relatively high, students recorded the lowest level of awareness on reporting online harassment and bullying (3.25) and distinguishing between authentic and pirated software (3.30).

These results indicate that as students' exposure to the internet increases, so does their awareness of cybersecurity threats. This is evident as an average of only 6% of the respondents leaned towards 2 (Unaware) and 1 (Totally Unaware) across the different cybersecurity concerns. A high degree of awareness means responders may know how to avoid phishing and social engineering. There is a strong association between poor cybersecurity awareness and higher cybercrime rates, emphasizing the importance of awareness in cyber prevention [16].

Students acknowledged the need for privacy and social media cybersecurity. Additionally, this survey identified considerable disparities in students' privacy and security knowledge across age groups and educational levels. Higher-educated and older social media users are more cognizant of privacy and cybersecurity [17]. Password security, browser safety, and social media use affect students' cybersecurity awareness. In general, pupils understand the need for cybersecurity [18].

Respondents may know Internet security software well, but implementation is limited [19]. Most respondents' Internet security perception is derivative: they practice online measures without comprehending the aim. Filipinos are vulnerable to cyberattacks, especially phishing and malware.

Many students have strong cybersecurity knowledge, phishing awareness, safe online practices, cybersecurity behaviors and attitudes, and incident response awareness. Cybersecurity knowledge and application may affect passing marks. The findings suggest that the academic curriculum should include comprehensive cybersecurity instruction to prepare pupils for the digital world. The research found that respondents' cybersecurity awareness is adequate, but continual improvement and specific interventions are needed. Future studies with better gender representation may clarify the link between cybersecurity awareness and academic achievement across populations. Because students have different networking and cybersecurity backgrounds, specialized instructional methodologies are needed to teach them. Educational institutions can improve academic performance and digital security by emphasizing these areas to prepare students for digital cybersecurity concerns [20].

3.2.Cybersecurity Practice

This section examines the actual practice of students as awareness does not necessarily equate to actual practice. The practices examined include password security, browser security, email security, and social networks.

3.2.1. Password Security. Password security is the practice of using strong passwords and other methods to protect your accounts and devices. Having strong passwords is particularly important. They protect your personal information by keeping unauthorized people from getting into your electronic accounts and gadgets. The more difficult the password, the safer data will be from hackers and other computer threats.

Technium Social Sciences Journal
Vol. 71, 215-232, May, 2025
ISSN: 2668-7798
www.techniumscience.com

Table 2.
Password Security Practice

Password Security Practice	Mean	Verbal Interpretation
1. Do all your passwords include at least 12 characters, a mix of upper- and lowercase letters, numbers, and symbols?]	0.82	YES
2. Do you use the same strong password across different websites and accounts?]	0.68	YES
3. Do you reuse previously used passwords?	1.00	YES
4. When you change your password, do you base the new password on your old one (for example, changing 'password2007' to 'password2008')?	0.45	NO
5. Do you use two-factor authentication for any of your accounts?	0.85	YES
6. Do you write your passwords down?	0.65	YES
7. Do you use software to manage your passwords (e.g., password managers like LastPass or browser-based options like those in Internet Explorer or Firefox)?	0.42	NO
8. Do you share your password(s) with other people?	0.21	NO
9. Do you change your passwords regularly?	0.48	YES

Data gathered shows the insight of the respondents on password security practices based on their self-reported behaviors. The data reveal both strengths and weaknesses in how individuals manage their passwords, with certain security practices being followed while others indicate potential vulnerabilities.

The data showed that the respondents displayed high awareness of strong password creation with a mean of 0.82 however this awareness contradicts their practices as it was evident by the mean under items that asked about their usage of the same passwords across different platforms and reusing old or previous passwords. Password reuse compromises the security of all systems accessible to a user, thereby amplifying the risks [21-23]. Cognitive limitations lead many users to select easily memorable passwords, often derived from meaningful combinations of names and/or numbers.

The gathered data showed a good mean of (0.45) from the respondents of not base their new password on their old one. This is further strengthened by a good outcome that most of the respondents use a 2-way factor authentication which adds up to the security measures done to secure one's account or important file. Two-way factor authentication requires you to present both "something you know" and "something you have" or "something you are" [24]. Biometrics like fingerprints, retinas, DNA, etc. are "something you are" [25]. Although these authentication systems' technical designs are flawed [26], adding layers of authentication reduces risk.

However, a significant mean of 0.65 has been derived from the data from the respondents who wrote down their passwords. Users and their alphabetic passwords are the "weakest link" in the "security chain" [27]. Poor password security practices including reuse, documentation, and sharing, as well as misunderstandings about secure password requirements, are the key issues. For almost 35 years, computer password management has remained unchanged. Password systems are vulnerable because users and their passwords are easily guessed, such as words, names, and birthdates [27].

Technium Social Sciences Journal
Vol. 71, 215-232, May, 2025
ISSN: 2668-7798
www.techniumscience.com

The data gathered showed a positive attitude of the respondents towards not sharing their passwords with anyone else. Also, the good thing is that there is still a high mean of those who changed their password regularly which indicates good security measures. However, from the data gathered it is seen that only a few percent of the respondents use the software in managing their passwords which is an opportunity to increase their guard against any cyber threats.

3.2.2. Browser Security Practice. Browser security is the field of technology, tools, platforms, and methods that turn browsers into safe surroundings. While safeguarding the systems and data of the company, these solutions allow web access to apps and websites.

Table 3.
Browser security practices

Browser Security Practice	Mean	Interpretation
1. Is the software on your computer (e.g., operating systems like Windows, browsers like Internet Explorer, and applications like Microsoft Office) regularly updated or upgraded?	0.81	YES
2. Do you regularly check your browser history for suspicious activities?	0.66	YES
3. Do you read and understand the terms and conditions before downloading applications?	0.69	YES
4. Do you install browser extensions from third-party websites?	0.38	NO
5. Do you use peer-to-peer file-sharing software/programs (such as BitTorrent, Direct Connect, eDonkey, eMule, Napster, Kazaa, etc.)?	0.30	NO
6. Does your device have an anti-virus program installed?	0.78	YES

Based on the data gathered, the respondents displayed an in-depth level of understanding of cybersecurity since there is a positive trend in terms of user awareness and behavior regarding browser and device security.

The high mean in regular software updates indicates that the respondents are proactive in keeping their system up to date which is one of the basic aspects of cybersecurity. However, there is a significant difference when it comes to regularly checking their browser history whereas this is also important as to guard the complete system from any hidden suspicious activities and potential threats.

Cybersecurity awareness is positively correlated with web browser security. Students who practice greater online browser security so typically have more cybersecurity awareness [29].

Technium Social Sciences Journal
Vol. 71, 215-232, May, 2025
ISSN: 2668-7798
www.techniumscience.com

3.2.3. Email Security Practices. Email is the most often used communication medium among cyber-attackers and criminals; it is used to propagate malware and viruses, pilfer sensitive data, run ransomware and phishing campaigns, and drive users into revealing confidential information. Solutions for email security are meant to guard against the always-changing range of email-borne attack paths.

Email security is intentionally gathering technologies and strategies to protect email-based communications, ensuring message availability, confidentiality, and integrity. Email security protects essential data, identifies, and filters harmful content, and prevents unauthorized access, making it suitable for all types of businesses.

Table 4
Email Security Practices

Email Security	Mean	Interpretation
1. Does your Email program have an Email spam filter.	0.77	YES
2. Do you open Emails if you do not know who the sender is?	0.42	NO
3. Do you open Email attachments if you do not know who the sender is?	0.30	NO
4. Do you use encryption when sending Email?	0.43	NO

The data gathered shows that there is a high awareness of basic email security practices from the respondents however the data also presents that there is a significant low mean from the respondents who use encryption when sending emails. Email encryption is a security measure that encodes an email message so that only the intended recipients can read it. Email encryption protects against cybercriminals, particularly identity thieves, from obtaining vital information for financial gain. Email encryption can protect the privacy of those who have shared sensitive information with you and reduce cybercrime. This suggests respondents may need further email encryption knowledge or exploration to improve email security.

Students' email security behaviors depend on self-efficacy and perceived rewards [30].Email security boosts cybersecurity awareness [18]. Understanding email security can boost cybersecurity awareness by 31.3%. This study's students are aware of email security and already avoid unknown senders and accounts that request personal information.

3.2.4. Social Network Practices. Social networking services enable users to create an open profile and connect with others who share their interests and hobbies. Social networking has become a pervasive part of human interaction and is changing the society rules in the modern world at a tremendous pace" (millions of people use it) [31]. Cybersecurity risks increase with social media use. Recent security events prompt academics and security professionals to examine connected cyberattacks on social media.

This section examines whether student’s social network practices indicate loopholes that can be exploited.

Technium Social Sciences Journal
Vol. 71, 215-232, May, 2025
ISSN: 2668-7798
www.techniumscience.com

Table 5

Social Network Practices

SOCIAL NETWORK PRACTICE	MEAN	INTERPRETATION
Are you a member of any social or professional networking sites (e.g., Facebook, Instagram, LinkedIn)?	0.72	YES
Does your website, webpage, or blog contain personal information such as your email address or telephone number?	0.51	YES
Do you post personal pictures on social media?	0.70	YES
Do you accept friend requests from strangers on social media?	0.19	NO
Do you share your current location on social media?	0.20	NO
Do you know how to report any threat of suspicious activity on social media?	0.83	YES

The data gathered evaluated the respondents' social networking practices and their online behaviors, awareness of security threats, and their experiences in cybersecurity incidents. The results showed positive indicators though some areas need a little reinforcement of the importance of safe social networking practices as a means of prevention for any potential cyber threats.

Most respondents use social or professional networking sites, and a mean of 0.51 said their personal information is displayed there. The findings also showed a high mean of 0.70 for responders publishing photos online. Social media makes it easy to share ideas, opinions, and experiences with individuals around the world [32]. Social media use and spread pose various concerns. Due to fake news, misinformation, security problems, etc., these platforms' information exchanges may be unreliable [33].

Furthermore, the respondents demonstrated caution when it comes to their engagement with unknown individuals online through the resulting mean of 0.19 and 0.20 on accepting friend requests from strangers and sharing their location online, respectively.

3.3. Experience On Cybersecurity Risk

This section examines the actual cybersecurity threats experienced by students.

Table 6

Experience Of Cybersecurity Risks

EXPERIENCE ON CYBERSECURITY RISKS	MEAN	INTERPRETATION
Have you ever had a virus on your device?]	0.42	NO
Had you lost personal files in your device because of malwares? (corrupted/missing files)]	0.42	NO

Technium Social Sciences Journal
Vol. 71, 215-232, May, 2025
ISSN: 2668-7798
www.techniumscience.com

Have you ever had your identity stolen online? (Someone pretended to be you)]	0.21	NO
Have you experienced losing cash on online banking or any other wallet applications (GCASH, Maya, Etc)?]	0.17	NO
Have you experienced having your account or device hacked?]	0.33	NO
Have you been a victim of scam while purchasing online?]	0.30	NO
Have you experienced bullying online (harassment, intimidation, or humiliation, etc.)?]	0.33	NO

Preliminary results showed no correlation between internet security and privacy awareness and behavior and any of the tested characteristics. Most respondents first used the internet as older teens or young adults and primarily use cell phones for that access [34].

Based on the data, it can be deduced that most respondents did not experience any cybersecurity incidents firsthand. Whilst the figures are low, it is still significant to note that some of the respondents experienced these incidents themselves which just signifies the importance of continuous awareness and actions to do some preventive measures against any cyber threats.

The data showed a mean from the respondents that 0.42 had ever experienced malware-related issues equaled those who lost their personal files in their device due to malware. Whilst this is not many of the respondents it still imposes those threats can happen. These malware threats are related to password security practices. One possibility is that malware infections harvest newly changed passwords, or that they were deceived by a phishing attack after their initial recovery [35].

Identity theft is obtaining and fraudulently using another's identity. Cyber-identity theft involves hacking, phishing, pharming, traffic redirections, keyloggers, and password theft [36]. There is a significantly low level of counts from the respondents who experienced online identity theft and those who experienced losing their money through online platforms indicating that they were able to effectively manage their personal and financial information on the internet. The respondents' data showed that there were low cases of hacking, online fraud, and harassment that they have experienced but it is not zero indicating a few portions of the population experienced these cyber incidents.

3.4. Attitudes Toward Cybersecurity

The table below shows the data gathered from the respondents on their perceptions and attitudes toward cybersecurity, including their confidence in protecting their devices, awareness of potential threats, and trust in online security practices.

Table 7

Attitudes Toward Cybersecurity

Statement	Mean	Interpretation
1. I can protect my computer from harm (hackers, phishers, etc.) by taking good care of computer security (regularly changing passwords, using firewalls, encryption, etc.).	3.35	Strongly Agree

Technium Social Sciences Journal
Vol. 71, 215-232, May, 2025
ISSN: 2668-7798
www.techniumscience.com

2. Updating my security software and operating system (Windows/Apple) is manageable and does not excessively consume bandwidth/data.	3.33	Strongly Agree
3. The information I keep on my computer could potentially interest someone attempting unauthorized access.	3.17	Agree
4. I only download software from secure sites and ensure that it is not free downloads that could be insecure.	3.34	Strongly Agree
5. Taking proactive security measures can significantly reduce the risk of hacking into my computer and our network.]	3.46	Strongly Agree
6. It is important to pay attention to cybersecurity without overreacting.]	3.54	Strongly Agree
7. I am comfortable using the Internet for financial transactions.]	2.99	Agree
8. Cybersecurity concerns me.]	3.38	Strongly Agree
9. I trust that my friends would not send me malicious content or scams through email.]	3.28	Strongly Agree
10. Changing passwords regularly is worthwhile to enhance security, even though risks still exist.]	3.43	Strongly Agree

Respondents with a mean of 3.35 confidently agreed that they can protect their computers from harm through some computer security measures. Correspondingly, the respondents strongly agree that they can manage to update their security software and operating system. Additionally, the respondents are very much aware that taking initiative-taking security measures can reduce the threats and other risks related to cyber incidents or crimes with a supporting mean of 3.46. The key to overcoming cyber security difficulties is to remain ahead of the game by adopting initiative-taking measures before adversaries exploit the system [37]. Furthermore, respondents recognize the importance of cybersecurity without overreacting with a mean of 3.54 suggesting a balanced approach to online security. Their strong agreement for a mean of 3.38, that cybersecurity concerns them indicates a general awareness of potential threats.

The result of the data shows that the respondents are aware that the information they keep on their computer could potentially interest someone attempting unauthorized access with a mean of 3.17. This awareness highlights an understanding that cyber threats are not limited to high-profile targets but can affect ordinary users as well. Similarly, the respondents posited a favorable mean of 3.34 for downloading software from secure sites and ensuring that it is not free downloads that could be a cybersecurity threat. Interestingly, a mean of 3.28 of the respondents' answers which strongly agreed that they trust their friends that they would not send them malicious content or scams through email which could create exposure to threats such as phishing or other cyber-attacks.

The data gathered showed that the respondents are comfortable using the Internet for their financial transactions. On the other hand, the respondents with a mean of 3.43 strongly agree that changing passwords regularly is worthwhile to enhance security, even though risks still exist.

Tech users prefer digital payments over checks or cash. As everyone knows, e-transactions give consumers many benefits, including instant payments, faster purchases, and simpler transactions [38]. Safe websites employ strong passwords, VPNs, SSL certificates, and hardware-level security. Antivirus, antimalware, and antispyware are used. Intruders still brute force passwords, PINs, and other protections. Single-level encryption is insufficient for online shopping security. Multilevel encryption is needed so customers may conclude online transactions even if one is broken.

The data results also revealed that many of the respondents know how to report any threats of suspicious activity on social media indicating a satisfactory level of awareness regarding online safety. Half of the population also obtained computer and information security training to better grasp their organization's policy and its importance. Cyber risks and attacks can take numerous forms, and users may not realize they are being attacked [39]. To promote cyber-safety, users, especially youngsters, must be educated and empowered to use online resources and platforms responsibly.

4. Conclusion and recommendations

Most students possess a commendable understanding of prevalent security dangers, encompassing password security, browser security, email security, and social media security. This suggests that with the rise in internet usage, there is a corresponding increase in cybercrimes and awareness. Nonetheless, it is crucial to acknowledge that certain students remain susceptible to violations, given their real conduct. They remain insufficiently cautious. This is particularly applicable to their practices on social media and in conducting financial transactions online. It is crucial to recognize that awareness does not invariably convert into action. Moreover, the elevated awareness among the respondents in this survey may not accurately reflect that of other schools, particularly those with limited financial means for awareness training and seminars, as well as those with younger children. Consequently, it is advisable to enhance students' cybersecurity awareness via an information campaign conducted by the Philippine National Police—Anti-Cybercrime Group. Educators are advised to emphasize the necessity of exercising utmost caution in the utilization of cyberspaces to their students. Moreover, further research should concentrate on other demographics, particularly middle-aged and elderly individuals, who may still be subjected to more sophisticated forms of victimization.

References:

[1] ITU World Telecommunication/ICT Indicators database & Wireless Intelligence : *The World in 2011 ICT facts and figures*. https://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf (2011)

[2] UNODC (2010): *The globalization of crime: a transnational organized crime threat assessment*. Retrieved from https://www.unodc.org/res/cld/bibliography/the globalization-of-crime-a-transnational-organized-crime-threat assessment_html/TOCTA_Report_2010_low_res.pdf

[3] S. GORDON, R. FORD: On the Definition and Classification of Cybercrime,' *Journal in Computer Virology*, Vol. 2, No. 1, 2006, page 13-20.

[4] UNITED NATIONS OFFICE ON DRUGS AND CRIME : *Comprehensive study on cybercrime.* Retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (2011)

[5] MINIWATTS MARKETING GROUP: Internet World Stats: Usage and Population Statistics. Retrieved from https://www.internetworldstats.com/stats.htm (2017)

[6] *J. MATEO (2016, July 16) 68 gov't websites attacked*. The Philippine Star : Retrieved from https://www.philstar.com/headlines/2016/07/16/1603250/68-govt-websites-attacked

[7] *M. MOAJE (2024, June 21). NBI nabs Manila Bulletin data officer, 2 others for "hacking."* Philippine News Agency. https://www.pna.gov.ph/articles/1227438

[8] AUSTRALIAN COMPUTER SOCIETY: *Cybersecurity threats challenges opportunities*. Retrieved from http://www.acs.org.au›content›dam›acs›acs-publications (2016)

[9] P. SEEMMA, S. NANDHINI, AND M. SOWMIYA : Overview of Cyber Security. *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 7, Issue 11 (2018)

[10] *DICT: National Cybersecurity Plan 2022*. Retrieved from https://dict.gov.ph/wpcontent/uploads/2019/07/NCSP2022-rev01Jul2019.pdf *(2022).*

[11] L. NEWMAN : *Schools already struggled with cybersecurity then came COVID-19*. Retrieved from https://www.wired.com/story/schools-already-struggled-cybersecurity-then-came-covid-19/. (2020)

[12] D. PRAMOD, & R. RAMAN : A study on the user perception and awareness of smartphone security. *International Journal of Applied Engineering Research* (2014).

[13] B. PRETORIUS & B. VAN NIEKERK : Cyber-security and governance for ICS/SCADA in South Africa. In J. Zaaiman, & L. Leenen (Eds.), *Proceedings of the 10th International Conference on Cyber Warfare and Security* (pp. 241-251). (2015).

[14] M. BADA & A. SASSE : *Cyber security awareness campaigns. Why do they fail to change behaviour?* Global Cyber Security Capacity Centre. Retrieved from http://discovery.ucl.ac.uk/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf (2014).

[15] T.R. PELTIER : Implementing an information security awareness program. Inf. Secur. J. A Glob. *Perspect*., 14(2), 37-49 (2005).

[16] F.K. MUPILA, H. GUPTA, AND A. BHARDWAJ : An empirical study on cyber crimes and cybersecurity awareness. Available at Research Square https://doi.org/10.21203/rs.3.rs-3037289/v1 (09 June 2023)

[17] J.N. SALES, R. TIONGCO, S. LU, M. J. RUIZ, J. CRUZ, & M. PRUDENTE : PERSONAL Privacy and Cyber Security: Student Attitudes, Awareness, and Perception on the Use of Social Media: Student Attitudes, Awareness, and Perception on the Use of Social Media. *International Journal of Curriculum and Instruction*, *16*(1), 175-190. (2024).

[18] M.A. ALQAHTANI: Cybersecurity Awareness Based on Software and E-mail Security with Statistical Analysis. *Computational Intelligence and Neuroscience*, *2022*(1), 6775980. (2022).

[19] C.D. OMOROG, & R.P. MEDINA : Internet security awareness of Filipinos: A survey paper. *arXiv preprint arXiv:2012.03669*. (2020).

[20] R.A.G. TORRES, &C.N.P. OLIPAS : Analyzing Student Academic Performance and Cybersecurity Awareness Levels: Basis for Enhancing Instruction. (2024).

[21a] M. BISHOP, & D.V. KLEIN : Improving system security via proactive password checking. *Computers & Security*, *14*(3), 233–249. https://doi.org/10.1016/0167-4048(95)00003-q (1995).

[22] A.S. BROWN, E. BRACKEN, S. ZOCCOLI, & K. DOUGLAS : Generating and remembering passwords. *Applied Cognitive Psychology: The Official Journal of the Society for Applied Research in Memory and Cognition*, *18*(6), 641-651. (2004).

[23] K. BRYANT & J. CAMPBELL : User Behaviours Associated with Password Security and Management. *AJIS. Australasian Journal of Information Systems/AJIS. Australian Journal of Information Systems/Australian Journal of Information Systems*, *14*(1). https://doi.org/10.3127/ajis.v14i1.9 (2006).

[24] A. OMETOV, S. BEZZATEEV, N. MÄKITALO, S. ANDREEV, T. MIKKONEN, & Y. KOUCHERYAVY : Multi-factor authentication: A survey. *Cryptography*, *2*(1), 1. (2018).

[25] O. BACHURINA, & P.A. WATTERS : Multi fingerprint biometric verification using XML Web Services: A funds transfer case study. In *International Conference on Recent Advances in Soft Computing (6th: 2006)* (pp. 441-448). University of Kent. (2006).

[26] S. YOUNG : Contemplating corporate disclosure obligations arising from cybersecurity breaches. *J. Corp. L.*, *38*, 659. (2012).

[27] V. TANESKI, M. HERIČKO, & B. BRUMEN : Systematic overview of password security problems. *Acta Polytechnica Hungarica*, *16*(3), 143-165. (2019).

[28] V. TANESKI, M. HERIČKO, & B. BRUMEN : Password security—No change in 35 years? In *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1360-1365). IEEE. (2014, May).

[29] Z. BINTI MOHAMAD : Web browser security and its correlation with cybersecurity awareness among Malaysian university students. *Jurnal Al-Sirat*, *24*(2), 84-88. (2024).

[30] G. SCHYMIK & J. DU : Student intentions and behaviors related to email security: an application of the health belief model. *J Inf Syst Appl Res*, *11*, 14-24. (2018).

[31] N. SAINI, G. SANGWAN, M. VERMA, A. KOHLI, M. KAUR, & P.V.M. LAKSHMI : Effect of Social Networking Sites on the Quality of Life of College Students: A Cross-Sectional Study from a City in North India. *The Scientific World JOURNAL*, *2020*, 1–8. https://doi.org/10.1155/2020/8576023 (2020).

[32] N. MILADI : Social media and social change. *Digest of Middle East Studies* 25.1 (2016): 36-51.

[33] P. DIZIKES : Why social media has changed the world — and how to fix it. *MIT News | Massachusetts Institute of Technology*. https://news.mit.edu/2020/hype-machine-book-aral-0924 (2020, September 24).

[34] J. ALVES-FOSS & B.G. LLEGO : Internet Security and Privacy Awareness Among College Students in the Philippines. In *2024 IEEE Cyber Science and Technology Congress (CyberSciTech)* (pp. 132-137). IEEE. (2024, November).

[35] K. THOMAS, F. LI, A. ZAND, J. BARRETT, J. RANIERI, L. INVERNIZZI, Y. MARKOV, O. COMANESCU, V. ERANTI, A. MOSCICKI, D. MARGOLIS, V. PAXSON & E. BURSZTEIN : Data breaches, phishing, or malware? *Proceedings of*

the 2022 ACM SIGSAC Conference on Computer and Communications Security. https://doi.org/10.1145/3133956.3134067 (2017).

[36] K.O. ASANTE-OFFEI, & W. YAOKUMAH: Cyber-Identity theft and fintech services. *Journal of Information Technology Research*, *14*(3), 1–19. https://doi.org/10.4018/jitr.2021070101 (2021).

[37] D. PERWEJ, S.Q. ABBAS, J.P. DIXIT, N. AKHTAR, & A.K. JAISWAL : A Systematic Literature review on the Cyber Security. *International Journal of Scientific Research and Management (IJSRM)*, *9*(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04 (2021).

[38] M.S. HUSAIN, & M. HAROON : A Review of Information Security from Consumer's Perspective Especially in Online Transactions. *International Journal of Engineering and Management Research*, *10*(4), 11–14. https://doi.org/10.31033/ijemr.10.4.2 (2020).

[39] N.A.A. RAHMAN, I.H. SAIRI, N.A.M. ZIZI & F. KHALID : The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378-382. (2020).