International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 2, Mar-Apr 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cybersecurity Practices and Cybercrime Victimization among Criminology Students: Basis for Cyber Defense Enhancement Program

Girlie N. Cañete, Nymia M. Ravidas, Ivy Joy E. Kibos

Philippine College Foundation, City of Valencia, Bukidnon, Philippines

ABSTRACT

The rapid integration of technology into every facet of our lives poses significant benefits and invertedly, substantial risks particularly on cyber security and cybercrime victimization. Effective cybersecurity practices are critical in preventing cybercrime victimization. It helps mitigate risks, protect sensitive data from being compromise and ensure the integrity of cyber- related activities and transactions. The main objective of this study was to assess the cyber security practices and the level of cybercrime victimization among 100 randomly selected criminology students of Philippine College Foundation, Valencia City, Bukidnon, in the year 2024.

A quantitative research design was utilized in this study using a survey questionnaire. Findings of the study revealed that majority of the respondents aged 21-23 years old, males, second year level and cellular phone users. Also, respondents applied cyber security practices in terms of logging into an electronic account, information sharing and access of website. Moreover, in the level of cybercrime victimization, the respondents have a high level of victimization in terms in phishing, online fraud and hacking. Finally, as to the test of significant relationship between cybersecurity practices and cybercrime victimization, it showed that logging into an electronic account, information sharing and access of website have a significant effect on phishing, online fraud and hacking among the respondents.

KEYWORDS: *Cybersecurity Practices; Cybersecurity Victimization; Criminology Students; Philippine College Foundation, Philippines*

How to cite this paper: Girlie N. Cañete | Nymia M. Ravidas | Ivy Joy E. Kibos "Cybersecurity Practices and Cybercrime Victimization among Criminology Students: Basis for Cyber Defense Enhancement Program" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-2, April 2025, pp.974-978, URL: www.ijtsrd.com/papers/ijtsrd78589.pdf

IJTSRD78589

1. INTRODUCTION

Cyber security practices are becoming increasingly important as technology continues to advance and cybercrime rates rise. In today's digital age, individuals and organizations are increasingly reliant on technology for conducting various aspects of their lives. However, with this increased reliance on technology comes the risk of falling victim to cybercrimes such as hacking, data theft, and identity fraud. Cybersecurity practices are essential measures that individuals and organizations can implement to protect themselves against cyber threats. Failure to implement proper cybersecurity practices can leave individuals and organizations vulnerable to cybercrime victimization. Hackers and cyber criminals are constantly evolving their tactics and techniques to exploit weaknesses in existing cybersecurity measures. Without adequate protection, individuals and organizations risk having their personal information stolen, their financial accounts compromised, or their systems rendered inoperable by malware (Tunggal, 2024).

Moreover, the consequences of cybercrime victimization can be far-reaching and long-lasting. Victims of cybercrimes may suffer financial losses, reputational damage, and emotional distress as a result of their personal and sensitive information being compromised. In some cases, cybercrime victimization can also lead to legal and regulatory consequences, further exacerbating the negative impact on individuals and organizations. The connection between cybersecurity practices and cybercrime victimization is clear and undeniable. Implementing proper cybersecurity measures is

essential for safeguarding against cyber threats and preventing the devastating effects of cybercrime victimization (Welance, 2023).

The need to conduct research studies on cyber security practices and cybercrime victimization among criminology students is clear. By raising awareness, improving cyber security practices, and expanding our understanding of cybercrime, we can better protect individuals and organizations from the growing threat of cyber threats. As technology continues to evolve, it is crucial for criminology students to stay informed and vigilant in order to combat cybercrime and protect themselves in an increasingly digital world

2. Materials and Methods

In this study, a descriptive correlational approach was used to assess the cyber security practices and cybercrime victimization among criminology students of Philippine College Foundation. The researchers' decision to use this methodology was influenced by the study's description of the variables and the relationships that inevitably arise between them, as well as by its evaluation on the cyber security practices and cybercrime victimization.

A correlational study design prevents the researchers from directly manipulating or controlling any variables. A correlational design also reflects the strength and or/direction of the link between two or more variables. According to Bhandari (2023), a correlation's direction might be either positive or negative.

This study was conducted at Purok 6, Valencia City, Bukidnon. Specifically at Philippine College Foundation (PCF). It is a nonstock, nonprofit, nonsectarian and service oriented educational institution whose objective is to develop students to become committed persons to serve the people of Mindanao, in particular, and the country, in general.

The respondents of the study were 100 randomly selected criminology students who were enrolled at Philippine College Foundation (PCF) during the first semester of academic year 2024-2025. A survey questionnaire was used to gather data on the cyber security practices and cybercrime victimization among criminology students. It was a researchers'-made questionnaire which was checked by the research committee for validity and reliability.

3. Results and Discussion

Problem 1. What is the Profile of the Respondents in terms of age, gender, year level and electronic gadgets used?

Table 1. Profile of the respondents in terms of Age, Gender, Year Level. Electronic Gadget Used

Age	**Frequency**	**Percentage**
18-20 years old	30	30%
21-23 years old	56	56%
24 years old & above	26	26%
Total	100	100%
Gender	**Frequency**	**Percentage**
Male	52	52%
Female	48	48%
Total	100	100%
Year Level	**Frequency**	**Percentage**
1st year	24	24%
2nd year	26	26%
3rd year	25	25%
4th year	25	25%
Total	100	100%
Electronic Gadgets Used	**Frequency**	**Percentage**
Cellular Phone	84	84%
Tablet	6	6%
Computer	2	2%
Laptop	8	8%
Total	100	100%

Problem 2. What are the level of Cyber Security Practices of the respondents in terms of logging into an electronic account, information sharing and access of website?

Table 2. The level of cybersecurity practices

Indicator	Mean	SD	Descriptive Level
Logging into an Electronic Account	0.512	2.94	Agree
Information Sharing	0.547	2.86	Agree
Access to Website	0.569	2.87	Agree
Overall	**0.543**	**2.89**	**Agree**

The results presented in Table 2 indicate that participants consistently engage in cyber security practices, falling predominantly under the category of "High" for all indicators. The mean scores for logging into an electronic account, information sharing, and access to website are 2.94, 2.86 and 2.87 respectively, all within the range of " Agree," which corresponds to "High level" adhering to these practices. Moreover, the overall mean score of 2.89 also aligns with " Agree," indicating a collective commitment to cyber security measures, where participants follow recommended protocols. Therefore, it can be inferred that the participants engage in these cyber security practices, demonstrating a firm commitment to safeguarding their electronic accounts, sharing information securely, and accessing websites responsibly.

The result in the highest mean shows that most of the respondents practicing cyber security in logging into an electronic account. This implies that the respondents were consciously practicing cyber security. It might because of the wide information dissemination conducted by law enforcement to prevent individuals from being a victim of cybercrime (PNP ACG Tip 4 and 5).

However, the lowest mean is the information sharing. This implies that the respondents were not strictly adhering on practicing security measures on sharing information online.

Problem 3. What is the level of Cybercrime Victimization among the respondents in terms of hacking, online fraud, and phishing?

Table 3 The level of cybercrime victimization

Indicator	Mean	SD	Descriptive Level
Phishing	0.468	3.00	Agree
Hacking	0.505	2.94	Agree
Online Fraud	0.487	2.96	Agree
Overall	**0.486**	**2.97**	**Agree**

The examination of cybercrime victimization levels, as outlined in Table 3, reveals a consistent trend of " Agree" responses across various indicators. With mean scores of 3.00 for phishing, 2.94 for hacking, and 2.96 for online fraud. Respondents demonstrate a high level of agreement regarding their experiences with these cybercrimes. This suggests that respondents highly acknowledge instances of phishing, hacking and online fraud, in their digital interactions. The overall mean score of 2.97 further consolidates this pattern, indicating a widespread acknowledgment of cybercrime victimization among the respondents. Therefore, it can be inferred that individuals commonly experience these cyber threats, reflecting a pressing need for strong cybersecurity measures to mitigate risks and safeguard against such malicious activities.

The data in the highest mean implies that phishing is one of the most factor of cybercrime victimization. It might because, criminals were doing various techniques by sending emails, text messages to deceive vulnerable online and technology users. This leads to the publication of public warning by the Bangko Sentral ng Pilipinas (2015) because of rampant phishing emails and reported victims of such fraud. Reiterating to the public to always verify the legitimacy link because clicking it.

The data in the lowest mean implies that hacking is the oldest method employed by the criminals and the respondents were already aware of its methods which less factor of cybercrime victimization. It might because the respondents were already aware that there were already existing laws and also awareness on the method of operation by the criminals (Republic Act No. 8792).

Problem 4. Is there a significant relationship on the level of cybersecurity practices and cybercrime victimization

Table 4 presents the results of the test for the significance of the relationship between cybersecurity practices and cybercrime victimization of the respondents. The table includes the r- values and p-values for various indicators such as logging into an electronic account, information sharing and access to website in relation to phishing,

hacking and online fraud. All of the p-values are 0.000, which are less than the significance level of 0.05, leading to the rejection of the null hypothesis (H0) for each factor. This suggests that there is a significant relationship between the variables, implying that factors like logging into an electronic account, information sharing and access to website influence cybercrime victimization rate such as phishing, hacking and online fraud.

Additionally, the overall mean for the relationship between cybersecurity practices and cybercrime victimization is 0.521, with a p-value of 0.000, further supporting the rejection of H0. The results indicate that cybersecurity practices namely logging into an electronic account, information sharing and access to website, have a significant effect on phishing, hacking and online fraud victimization among the respondents. This highlights the importance of adopting cybersecurity practices to reduce cybercrime victimization.

Table 4. Test for the significant relationship on the level of cybersecurity practices and cybercrime victimization

Cybersecurity practices (x)	Cybercrime victimization (y)	r- value	p-value	Decision on Ho
Logging into an electronic account	Phishing	0.461	.000	Rejected
	Hacking	0.443	.000	Rejected
	Online Fraud	0.464	.000	Rejected
Information sharing	Phishing	0.569	.000	Rejected
	Hacking	0.495	.000	Rejected
	Online Fraud	0.539	.000	Rejected
Access to website	Phishing	0.505	.000	Rejected
	Hacking	0.576	.000	Rejected
	Online Fraud	0.637	.000	Rejected
Overall Mean	Phishing	0.512	.000	Rejected
	Hacking	0.505	.000	Rejected
	Online Fraud	0.547	.000	Rejected
Overall Mean		**0.521**	**.000**	**Rejected**

Acknowledgement

The researchers are thankful to the Philippine College Foundation(PCF) administration headed by our School President, Dr. Charmaine P. Pagonzaga and to all of the selfless people who extended their help for the completion of this study.

Above all, to our Almighty God who is the main source of everything.

References

[1] Alanezi, Faisal (2015). Perceptions of Online Fraud and the Impact on the For the Control of Online Fraud in Saudi Arabian Financial Institutions. Retrieved from https://shorturl.at/eBIP0 on March 11, 2024

[2] Alda, Meredith (2023). Cybersecurity and cybercrime in the Philippines - statistics & facts. Retrieved from https://shorturl.at/qKNO9 on March 8, 2024 at 4:18am

[3] Bhandari, Pritha (2023). How to Calculate Variance | Calculator, Analysis & Examples. Retrieved from https://rb.gy/d4ofhb on March 7, 2024 at 7:56am

[4] Brush, Kate and Cobb, Michael (2024). Cybercrime. Retrieved from https://www.techtarget.com/searchsecurity/definition/cybercrime on March 8, 2024 at 4:05pm

[5] Cai, Zhihui et. Al (2017). Gender and Attitudes Towards Technology Use: A meta- Analysis. Retrieved form sciencedirect.com on March 21, 2024 at 11:43pm

[6] Fiore, Andrew T. (2017). The Role of Trust in Online Relationship Formation. Retrieved from https://shorturl.at/vHY34 on March 22, 2024 at 10:51pm

[7] Griffiths, James (2020). 'I love you': How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on. Retrieved from https://shorturl.at/sM579 on March 7, 2024 at 8:59am

[8] Haryanto, Dewi R. (2019). Analysis of Utilization of Gadgets as Effective Learning Media in Innovation Education to Improve Student Learning Achievement. Retrieved form knepublishing.com on March 22, 2024 at 8:53pm

[9] Kabanda, Salah et. al. (2018). Exploring SME cybersecurity practices in developing countries.

Retrieved from https://rb.gy/kutft3 on March 7, 2024 at 8:21am

[10] Luczon, Nef (2024). Government Offices Vulnerable to Cyberattacks – Normin Cyber Cop Chief. Retrieved from https://www.pna.gov.ph/articles/1217806 on March 8, 2024.

[11] Martin, Roger (2024). Let's Focus More on the First Year. Insidehighered.com on March 22, 2024 at 5:39am

[12] National Privacy Commission 30 Ways to Love Yourself Online. (2022). https://privacy.gov.ph/30-ways-to-love-yourself-online/

[13] Patterson, R. W. and Patterson, R. M. (2017). Computers and Productivity: Evidence from Laptop Use in the College Classroom. Retrieved from sciencedirect.com on March 22, 2024 at 8:58pm

[14] Petrosyan, Ani (2023). Distribution of Internet Users Worldwide as of 2021 by Age Group. Retrieved from statista.com on March 21, 2024 at 11:32pm

[15] Robbins, Chuck (2024). The Cybersecurity. Retrieved from https://rb.gy/uacwt1 on March 7, 2024 at 8:05am

[16] Sun, Bing et. al. (2020). Male and Female User's Differences in Online Technology Community Based on Texting Mining. Retrieved from frontiersin.org on March 22, 2024 at 5:23am

[17] Tarter, Alex (2017). Importance of Cyber Security. Retrieved from https://shorturl.at/sCKQS on March 7, 2024 at 8:33am

[18] Tunggal, Abi T. (2023). What is a Cyber Attack? Common Attack Techniques and Targets. Retrieved from https://rb.gy/46a6tg on March 7, 2024 at 8:13am

[19] Republic Act No. 10175 "Cybercrime Prevention Act of 2012".

[20] Republic Act No. 8792 "Electronic Commerce Act of 2000."

[21] https://www.linkedin.com/pulse/impact-cybercrime-individuals-businesses-society-join-welance

[22] https://www.upguard.com/blog/cybersecurity-important

[23] https://www.amlc.gov.ph

[24] https://www.acg.pnp.gov