ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691|| ISI Value: 1.188

AWARENESS OF CYBERCRIME PREVENTION ACT (RA 10175) AMONG CRIMINOLOGY STUDENTS: BASIS FOR CYBER ENRICHMENT PROGRAM

Girlie N. Cañete[a*], Hermogenes P. Malagamba[b], Ladie Mae J. Bayocot[c]
Philippine College Foundation, City of Valencia, Bukidnon, 8709, Philippines

ABSTRACT

The purpose of this study is to evaluate criminology students' knowledge of the Cybercrime Prevention Act. This study aims to determine areas for improvement in criminology students' education and training by examining their awareness and comprehension of RA 10175. A quantitative research design was used to gather the data from the randomly selected criminology students of Philippine College Foundation.

Results revealed that majority of the respondents aged 21- 23, male and single. A high level of awareness in terms of content related offenses, computer related offenses, and offense against confidentiality was seen. T- test was used to examine the significant difference on the responses of the respondents when they are grouped according to their profile. The result is in conformity to the problem.

KEYWORDS: *Cybercrime; computer related offenses; offense against confidentiality; content related offenses criminology students; Philippine College Foundation, Philippines*

1. INTRODUCTION

While there are many advantages to the quick development of technology, there are also new avenues for criminal activities. With hackers, identity thieves, and other bad actors posing a threat to people, businesses, and governments, cybercrime in particular has grown in importance on a global scale. The Philippine government passed the Cybercrime Prevention Act of 2012, also known as Republic Act No. 10175, in response to this escalating menace. Computer-related crimes like hacking, cybersquatting, and computer fraud, as well as content-related crimes like cybersex and online libel, are all intended to be prevented and suppressed by this law. It is anticipated that criminology students would be essential in stopping and looking into cybercrime as future law enforcement officers. However, their legal expertise and comprehension determine how successful law enforcement operations are. Thus, the purpose of this study is to evaluate criminology students' knowledge of the Cybercrime Prevention Act. This study aims to determine areas for improvement in criminology students' education and training by examining their awareness and comprehension of RA 10175. This would ultimately help the Philippines and nearby countries prevent and investigate cybercrime more effectively.

2. MATERIALS AND METHODS

This study utilized a descriptive- quantitative research design. A researchers' made survey instrument was the primary tool in gathering the data from the research respondents. This tool was validated by three research experts to see to it that every indicator contained therein fitted to the research issue.

The locale of this study is 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. Twenty- five respondents were taken from each year level resulting to a total of 100 respondents. This sampling was chosen so that all of the year levels will have an equal representation.

3. RESULTS

Profile of the respondents in terms of Age

Table 1.1 presents the age distribution of the respondents. The largest group is within the 21-23 age range, comprising 56 individuals or 56% of the total sample. This is followed by the 18-20 age group with 25 individuals, representing 25% of the respondents. The 24-26 age group accounts for 12 respondents, or 12%, while the smallest group is aged 27 and above, with 7 individuals, making up 7% of the total. The data suggests that the majority of the respondents are in the early stages of adulthood, between 21 and 23 years old.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691|| ISI Value: 1.188

Table 1.1 Profile of the respondents in terms of Age

Age	Frequency	Percentage
18-20	25	25%
21-23	56	56%
24-26	12	12%
27 and above	7	7%
Total	**100**	**100%**

Profile of the respondents in terms of Gender

Table 1.2 shows the gender distribution of the respondents, with 51 males (51%) and 46 females (46%) participating in the study. This indicates a relatively balanced representation of both genders, with a slight majority of male respondents. The data suggests that the gender distribution among the participants is nearly equal.

Table 1.2 Profile of the respondents in terms of Gender

Gender	Frequency	Percentage
Male	51	51%
Female	46	46%
Total	**100**	**100%**

Profile of the respondents in terms of Civil Status

Table 1.3 presents the civil status of the respondents. The majority are single, representing 86% of the total population, followed by common law at 10%. A smaller portion of the respondents are married comprising 4%. The presence of respondents from various civil status categories also suggests a diverse demographic, potentially enriching the perspectives represented in the study.

Table 1.3 Profile of the respondents in terms of Civil Status

Civil Status	Frequency	Percentage
Single	86	86%
Married	4	4%
Common Law	10	10%
Total	**100**	**100%**

Level of awareness on the selected provisions of Republic Act 10175 also known as "Cybercrime Prevention Act of 2012"

Table 2 presents the respondents' level of awareness regarding the selected provisions of Republic Act 10175, also known as the "Cybercrime Prevention Act of 2012." The data shows that all indicators—offenses against confidentiality, computer-related offenses, and content-related offenses—received mean scores ranging from 3.30 to 3.50, all of which fall under the "Strongly Agree" category with an interpretation of "Highly Aware". The highest mean score was observed for content-related offenses, with a mean of 3.50, suggesting that respondents are most aware of this aspect of the law. The overall mean of 3.42 further confirms a high level of awareness among respondents regarding the provisions of the Cybercrime Prevention Act of 2012.

Table 2 level of awareness on the selected provisions of Republic Act 10175 also known as "Cybercrime Prevention Act of 2012

Indicator	Mean	SD	Descriptive Level
Offense against confidentiality	0.783	3.30	Strongly Agree
Computer Related offenses	0.677	3.44	Strongly Agree
Content Related offenses	0.659	3.50	Strongly Agree
Overall	**0.706**	**3.42**	**Strongly Agree**

Significant difference on the responses of the respondents when they are grouped according to their profile

The table below shows the significant differences in the responses of respondents regarding their awareness of the selected provisions of Republic Act 10175, grouped according to their profile. For all three categories—offense against confidentiality, computer-related offenses, and content-related offenses—the t-values for age, gender, civil status, and program are all highly significant, with p-values less than 0.05. This leads to the rejection of the null hypothesis (H0) in each case, indicating that these demographic factors influence the respondents' awareness of cybercrime provisions under the law.

In other words, the respondents' awareness levels differ significantly based on their age, gender and civil status, highlighting that these factors may play a role in how individuals perceive and understand cybercrime offenses. The consistent rejection of H0 across all profile categories suggests that the profile variables have a significant impact on the level of awareness about cybercrime, reinforcing the importance of

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 4| April 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691|| ISI Value: 1.188

considering these demographic factors when evaluating public awareness of the provisions of Republic Act 10175.

Table 3 significant difference on the responses of the respondents when they are grouped according to their profile

Profile	*Awareness on the selected provisions of Republic Act 10175 also known as "Cybercrime Prevention Act of 2012*								
	Offense against confidentiality			*Computer Related offenses*			*Content Related offenses*		
	T-value	**P-Value**	**Decision on H0**	**T-value**	**P-Value**	**Decision on H0**	**T-value**	**P-Value**	**Decision on H0**
Age	52.320	0.000	reject	56.020	0.000	reject	51.942	0.000	reject
Gender	54.565	0.000	reject	55.114	0.000	reject	53.010	0.000	reject
Civil Status	55.521	0.000	reject	55.383	0.000	reject	52.296	0.000	reject
Significant if P-value is <0.05									
Legend: H0 is rejected if Significant *H0 is accepted if Not Significant*									

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. *Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by the international law and cyber convention. Multidisciplinary Reviews, 8(1), 2025024-2025024.*
2. *Dalpini, N. (2021). Cybercrime Protection in E-Commerce During the COVID-19 Pandemic. Utica College.*
3. *Dupont, B. (2019). Enhancing the effectiveness of cybercrime prevention through policy monitoring. Journal of Crime and Justice, 42(5), 500-515.*
4. *Khan, S., Saleh, T., Dorasamy, M., Khan, N., Leng, O. T. S., & Vergara, R. G. (2022). A systematic literature review on cybercrime legislation. F1000Research, 11, 971.*
5. *Li, J. (2021). Cybercrime in the Philippines: A case study of national security. Turkish Journal of Computer and Mathematics Education, 12(11), 4224-4231.*
6. *Serzo, A. L. O. (2021). Philippine Regulations for Cross-Border Digital Platforms: Impact and Reform Considerations. Research Paper Series (Philippine Institute for Development Studies), (8), I-41.*
7. *Siregar, G., & Sinaga, S. (2021). The law globalization in cybercrime prevention. International Journal of Law Reconstruction, 5(2), 211-227.*
8. *Sviatun, O. V., Goncharuk, O. V., Roman, C., Kuzmenko, O., & Kozych, I. V. (2021). Combating cybercrime: economic and legal aspects. WSEAS Transactions on Business and Economics, 18, 751-762.*
9. *Tamdang, D., Borreros, A. J., & Forca, A. (2024). Raising Awareness of IT Regulations and Compliance through Symposium on Philippine Public High Schools in Buenavista, Guimaras. JPMI (Jurnal Pengabdian Masyarakat Inovatif), 2(2), 49-56.*
10. *Trajkovska, E., Del Becaro, T., & Mijalkov, B. (2024, September). PREVENTION OF CYBERCRIME IN THE AGE OF ARTIFICIAL INTELLIGENCE (AI) WITHIN THE EUROPEAN UNION. In Proceedings of the International Scientific Conference" Social Changes in the Global World" (Vol. 11, No. 11, pp. 177-189).*
11. *https://cybercrime.doj.gov.ph/republic-act-no-10175-cybercrime-prevention-act-of-2012/*