P-ISSN: 0119-3058
E-ISSN: 2945-4093

The Vector: International Journal of Emerging Science, Technology and Management
Volume 34, Issue 1, January - December 2025

Sectoral Awareness of the Cybercrime Prevention Act Of 2012 (Ra 10175) in Bangued, Abra

Nydiel G. Tadeja[1] Arlan G. Reburon[2]
[1] Criminology Department, Data Center, Bangued, Philippines
[2] College of Criminal Justice Education, University of Northern Philippines, Philippines
[1] ntadeja14@gmail.com
[2] agreburon@unp.edu.ph

ABSTRACT

The tremendous growth in global web usage has significantly increased digital connectedness and the community's vulnerability to online fraud, cyberattacks, and other forms of online exploitation. Public awareness, grassroots comprehension, and frontline staff's ability to successfully enforce regulations continue to be severely lacking. This study evaluated the knowledge of Bangued inhabitants regarding the Cybercrime Prevention Act of 2012, also known as RA 10175, with an emphasis on sociodemographic, information sources, online platform usage, ownership of ICT devices, and understanding of its provisions, punishable acts, and punishments. It also examined the relationship between profiles and levels of awareness, as well as their differences across areas. A mixed-methods Explanatory Sequential design was used to quantitatively collect data from 394 respondents: 123 from schools, 48 from the business sector, and 223 residents, selected through stratified random sampling using Slovin's formula. The qualitative part involved nine participants purposely selected to explain emerging patterns from which data was used to triangulate the initial quantitative findings. Results revealed that respondents were generally aware of the provisions of the law and the punishable acts; however, the respondents had a low understanding of the penalties, with residents consistently demonstrating the lowest awareness, and there was a significant relationship between educational attainment, age of the community respondents, and their level of awareness of RA 10175. It is recommended that this study provide localized, sector-specific evidence on awareness gaps in cybercrime legislation, which may inform community-based and sector-targeted cybercrime education initiatives, curriculum integration, and business compliance training to address identified gaps in awareness of the Cybercrime Prevention Act of 2012 and to support evidence-based awareness initiatives in Bangued, Abra.

***Keywords**: Cybercrime Awareness, Digital Literacy, Community-Based Prevention*

INTRODUCTION

The internet, or the World Wide Web, is like a double-edged sword; it has its advantages and disadvantages, and it has transformed humans to rely on these technologies. It has been deemed as one of the fastest-growing threats to individuals, organizations, and governments, with incidents of ransomware, phishing, and data breaches escalating in frequency and sophistication each year. Records demonstrate an increasingly serious threat to businesses, vital

P-ISSN: 0119-3058
E-ISSN: 2945-4093

infrastructure, and internet users worldwide, underscoring the critical need for comprehensive knowledge and preventive measures.

Rapid digital development in the ASEAN area has increased cybercriminals' attack surface. According to studies, 3% of the region's documented web-based threats—millions of harmful attempts are found annually—came from Philippine companies. These figures confirm that nations and populations are vulnerable to abuse when digital expansion occurs without equivalent cybersecurity readiness (CEDTyClea, 2024).

In the meantime, there are growing cyberthreats, as recorded cybercrime events in the Philippines increased by almost 69% in 2023 to 19,472 cases, or an average of 53 cybercrimes per day, from 11,523 in 2022. Records show that over half of Filipino internet users experienced technology-facilitated incidents in 2024, highlighting persistent vulnerabilities stemming from limited awareness, insufficient reporting mechanisms, and skill gaps. Online scams are the most common incidents, nearly doubling in number within a single year despite expanded reporting and enforcement efforts by all coordinated law enforcement authorities. In addition, the Philippines has seen a notable rise in hacked internet accounts and data breaches, placing it among nations where cybersecurity issues are becoming more pressing as digital adoption rises (Tupas, 2024).

Even though the Philippines has legislation that defines and punishes cybercrime to bring domestic laws into compliance with international norms, its application is nevertheless hampered by low public awareness, poor digital literacy, and a lack of capability among frontline staff. There is clear empirical evidence about locals' knowledge of cybercrime laws, safe online conduct, and the wider ramifications of cybercrime at the local level, particularly in the communities. The dearth of localized documentation and analysis hampers efforts to develop focused, culturally relevant, and community-responsive cybersecurity initiatives. Since this study gap stems from the unique demands, behaviors, and vulnerabilities of local communities, it is crucial to examine it. By analyzing Bangued residents' knowledge of the Cybercrime Prevention Act of 2012, profiling respondents to identify sociodemographic correlates of awareness, and identifying specific awareness deficiencies—particularly among all internet users and the so-called protectors—this study fills the identified gaps. In keeping with Pasinhon and Donato's (2024) findings, the study emphasizes that frontline staff frequently experience training gaps and a lack of technological tools, which limit their ability to conduct investigations and take preventative measures. Additionally, in line with Garcia and Bongo's (2022) findings, which showed that teachers' and students' differing levels of cybersecurity awareness during the transition to online learning highlight the critical need for frequent, community-based awareness programs to foster resilience and digital responsibility.

P-ISSN: 0119-3058
E-ISSN: 2945-4093

The Vector: International Journal of Emerging Science, Technology and Management
Volume 34, Issue 1, January - December 2025

Despite the enactment of the Cybercrime Prevention Act of 2012, limited empirical studies have examined how different community sectors understand its provisions, punishable acts, and penalties at the local level. In particular, there is a lack of sector-specific evidence from provincial communities such as Bangued, Abra.

The study's findings are intended to help law enforcement agencies, educational institutions, and local government organizations develop more effective, inclusive, and durable cybersecurity initiatives. In the end, by encouraging safer, better-informed, and digitally empowered communities, this research supports ongoing initiatives in line with the United Nations Sustainable Development Goals, particularly Quality Education (SDG 4), Decent Work and Economic Growth (SDG 8), Industry, Innovation and Infrastructure (SDG 9), Sustainable Cities and Communities (SDG 11), Peace, Justice and Strong Institutions (SDG 16), and Partnerships for the Goals (SDG 17).

Ultimately, this study focuses on assessing awareness levels and associated factors, rather than evaluating enforcement effectiveness or actual compliance with the law.

Objectives of the Study

This study aimed to determine the level of awareness of the Cybercrime Prevention Act of 2012 (RA 10175) among selected sectors in Bangued, Abra. Specifically, it sought to: (1) Describe the profile of the respondents in terms of socio-demographic characteristics, sources of information, online platforms used, and ICT devices owned; (2) Assess the level of awareness of the respondents regarding the provisions, punishable acts, and penalties of RA 10175; (3) Determine the relationship between selected profile variables and the level of awareness of RA 10175; (4) Identify significant differences in awareness levels among schools, the business sector, and residents; and (5) Propose an action plan to address identified gaps in awareness of RA 10175.

METHODOLOGY

This section outlines the research design, participants, instruments, procedures, ethical considerations, and statistical tools used in this study.

Research Design. A mixed-methods explanatory sequential design was used, with a quantitative phase to gauge the understanding of the Cybercrime Prevention Act of 2012 among Bangued, Abra inhabitants and a qualitative phase to investigate the underlying causes of the results. As an explanatory sequential mixed-methods study, this research examines patterns and relationships in awareness levels but does not establish causal effects. This two-phase approach provided a thorough and in-depth analysis of public awareness (Ivankova et al., 2006).

P-ISSN: 0119-3058
E-ISSN: 2945-4093

Participants of the study. The study focused on three groups: schools, businesses, and residents of Bangued, Abra. Slovin's Formula and stratified random sampling were used to select 394 participants—123 from schools, 48 from business sectors, and 223 from localities. Additionally, nine respondents were picked especially for qualitative interviews.

Data Collection Procedure. Permissions were obtained from school administrators and local government offices. Respondents were guaranteed confidentiality and provided informed consent. Following the collection of quantitative data, structured interviews with a subset of respondents were conducted during the qualitative phase to delve deeper into their perspectives. A suggested action plan to raise awareness of cybercrime was developed using data from both phases.

Data Gathering Instrument. The validated questionnaire ensured that the measured awareness levels reflected respondents' perceived understanding of RA 10175 rather than actual legal compliance. Expert validation ensured content clarity, appropriateness, and reliability with a score of 4.56. A four-point Likert scale was used:

Scale	Range	Descriptive Rating
4	3.26-4.00	**Proficient (P)**
3	2.51-3.25	**Aware**
2	1.76-2.50	**Familiar (F)**
1	1.00-1.75	**Unaware (U)**

Data Analysis. The data gathered in his study were examined using Frequency counting and Percentages for demographic profiles, Weighted Mean for the level of awareness, Bivariate Correlation for profile-awareness relationships, and One-way ANOVA for group differences.

RESULTS AND DISCUSSION

This section presents, analyses, and interprets the findings, which were corroborated by previous studies.

1. Profile of the Respondents

Socio-demographic. The majority of responders are young adults, aged from late teens to mid-twenties. Individuals in their late twenties and early thirties exhibit smaller proportions, whilst those in the later age groups are noticeably smaller. Female respondents are the most numerous, followed by males, and very few identified as LGBTQ+. This shows that the most predominant participants in the study are female. By level of education, most respondents pursue college, followed

by those who have completed their undergraduate studies. The least number have completed or are still studying at the high school level, and only a very few have finished or are still in elementary school. Few are currently pursuing or have finished graduate school. It may be deduced that the bulk of the participants have also attained or are still pursuing higher education.

Source of Information. In terms of information sources, social media is the primary channel through which most respondents receive news and updates. Many others, such as radio, television, the internet, and printed material, are not as frequently used, especially printed media. That shows the dominance of social media in how information is presented to respondents.

Online platform. Examining online platforms, Facebook is the most prevalent, followed by YouTube, Instagram, and TikTok. Other online platforms, including 9gag and Twitter, are used by only a fraction of respondents; this means the listed platforms essentially account for most participants' online activity.

ICT Device ownership. Regarding ownership of ICT devices, mobile phones are the most common, with widespread ownership of computers and laptops. Still, a small number of respondents have less common devices, such as tablets or e-readers. Thus, this implies that mobile phones, together with standard ICT tools, are almost universally available among the respondents. The response group is predominantly young, female, and well-educated, relying heavily on social media, especially Facebook, for information and online engagement. Their near-universal ownership of mobile phones and other ICT devices marks this group as digitally connected, but it also exposes them to vulnerabilities related to cybercrime. The predominance of young, digitally connected respondents highlights both increased exposure to online risks and the importance of targeted cybercrime education for this demographic.

2. On the level of awareness

The comparison of the respondents' awareness regarding the three main domains of the Cybercrime Prevention Act of 2012-that, that is, Provisions, Punishable Acts, and Penalties, revealed that the Business Sector, Schools, and Residents respondents demonstrated a general but uneven awareness of RA 10175, with notable gaps in understanding its penalties but at dissimilar levels.

P-ISSN: 0119-3058
E-ISSN: 2945-4093

Table 1

Summary of the level of awareness on the Cybercrime Prevention Act of 2012 (RA 10175)

Indicator	Resident		Business Sector		Schools		As a Whole	
	x	DR	x	DR	x	DR	x	DR
PROVISION	2.63	Aware	2.90	Aware	2.90	Aware	**2.75**	Aware
PUNISHABLE ACTS	2.69	Aware	2.99	Aware	2.97	Aware	**2.81**	Aware
PENALTY	2.53	Aware	2.79	Aware	2.81	Aware	**2.65**	Aware
Overall	**2.62**	Aware	**2.89**	Aware	**2.89**	Aware	**2.74**	Aware

Legend:

Scale	Range	Descriptive Rating
4	3.26-4.00	Fully Aware
3	2.51-3.25	Aware
2	1.76-2.50	Not Aware
1	1.00-1.75	Fully not aware

Participants from the Business Sector and Schools showed the greatest comprehension of the legal foundation and structure of the Act. Despite being somewhat less knowledgeable, residents also demonstrated a reasonable comprehension of the scope and relevance of its laws. This implies that, generally speaking, all groups comprehend the essential components of the act to a sufficient degree. The Abdajabar & Md Yunus (2023) study supports your findings by demonstrating that awareness and system preparedness—rather than just the presence of laws—are crucial in preventing cybercrime.

There was far greater awareness of punitive activities. Again, the Business Sector and School groups had a strong understanding, especially regarding crimes such as fraud, hacking, and unauthorized access. Although relatively limited, the inhabitants' awareness of the types of acts that might be classified as cybercrime was nonetheless rather high. Some organizations did not fully grasp certain nuances, such as disputes over domain names or device abuse.

While most respondents knew something about cybercrime, they knew very little about the penalties and legal ramifications under RA 10175. Participants in schools seemed to be more aware, followed by those in the business sector, while members of the community showed the least awareness. This is consistent with the findings of Bele et al. (2014), who noted that if awareness is to be translated into actual prevention, educational interventions—such as organized, stakeholder-

involved programs and integrated learning modules—are essential. The limited grasp of fines thus highlights the need for targeted teaching initiatives that go beyond raising awareness to improve comprehension of how the law is implemented through its repercussions, thereby developing responsible digital behavior.

Similarly, the study by Tamayo et al. (2024) discovered that resilience is the ability to remain proactive and unyielding in the face of stressful and high-risk circumstances, as demonstrated by the lived experiences of OFW nurses during the COVID-19 epidemic. The ability to identify, respond to, and recover from cyberthreats, including malware, phishing, and online fraud, is known as digital resilience, or cyber awareness. Users in digital contexts benefit from developing perseverance, self-efficacy, and problem-solving skills to address evolving cybersecurity challenges, just as nurses demonstrated courage and tenacity in addressing unknown health hazards. To lessen the emotional and mental strain caused by online threats, it is important to promote ongoing learning, implement proactive security measures, and remain composed when dealing with cyber incidents.

Further, Agup's (2024) study shows that despite participants' moderate to high level of RA 10175 awareness, barriers such as limited digital literacy, inadequate training, and a lack of institutional support preclude full compliance. Consistent with studies in healthcare data privacy, knowledge, organizational support, and continuous education are necessary to effectively mitigate cybercrime concerns. According to Colubong et al. (2024), increased awareness alone does not ensure proper practice. Discovered that university students' knowledge of e-cigarettes did not always result in safe conduct, underscoring the necessity of reinforcement through instruction, peer pressure, and direction.

Furthermore, these trends are explained by qualitative comments. According to business respondents, legal briefings and seminars focus on actions that are illegal but seldom discuss precise punishments, leaving a knowledge vacuum about the entire ramifications of the law. The Cybercrime Prevention Act, particularly its punitive measures, is rarely covered in formal education, according to students, and as a result, they have only rudimentary or fragmented knowledge from unofficial sources. Residents emphasized that the law is rarely discussed at the community level and that clear, culturally relevant information is not easily accessible. To make the law comprehensible and applicable, they advocated for specialized educational initiatives, including communication in regional dialects. In conclusion, every industry showed a general understanding of the Cybercrime Prevention Act of 2012. Nonetheless, awareness tends to be weak regarding penalties but strong regarding regulations and activities that are punished. The consistently lower awareness of penalties indicates that knowledge of cybercrime

P-ISSN: 0119-3058
E-ISSN: 2945-4093

laws remains largely procedural rather than consequence-oriented. Systemic issues, such as a lack of localized information transmission, a lack of attention in seminars, and an absence from the formal curriculum, are revealed by the awareness gap. These findings further underscore the need for comprehensive, multi-sectoral educational efforts that must transcend mere awareness to fully convey the legal consequences of committing cyber offenses, thereby enhancing the populace's preparedness to recognize and act properly on cybercrime.

3. Significant correlation between respondents' awareness of RA 10175 and their profile.

Table 2
Correlational coefficient showing the relationship between the Profile of Respondents and their Level of Awareness

Profile	Awareness of RA 10175			
	Provision	Punishable Acts	Penalties	As a Whole
Gender	-0.061	-0.024	-0.030	-0.040
Age	-0.080	-0.097	-.106*	-.103*
Educational Attainment	.169**	.154**	.169**	.178**
Sources of Information	0.040	0.011	0.007	0.020
Online Platform used	0.045	0.087	0.022	0.055
ICT devices owned	0.063	0.048	0.041	0.054

***. Correlation is significant at the 0.01 level (2-tailed).*

**. Correlation is significant at the 0.05 level (2-tailed).*

The table shows the analysis of respondent profiles and their awareness of RA 10175, or the Cybercrime Prevention Act of 2012, presents nuanced patterns. In general, the results indicate that age and educational attainment are significantly associated with awareness of RA 10175, while other profile variables show no meaningful relationships. The educational attainment level turned out to be the most significant factor, positively correlating with all measures of awareness: provisions of the Act, punishable acts, and penalties, and with overall understanding of the Act. In other words, respondents with higher levels of education generally had a slightly better understanding of the law. Age also showed a significant relationship: the younger the respondent, the more aware they were likely to be.

On the other hand, other characteristics, such as gender, preferred sources of information, online platforms used, and the number of ICT devices owned,

P-ISSN: 0119-3058
E-ISSN: 2945-4093

The Vector: International Journal of Emerging Science, Technology and Management
Volume 34, Issue 1, January - December 2025

showed little or no observable relationship with the respondents' awareness of the Act. These variables did not seem to affect participants' level of understanding of the law either way. These findings suggest that formal education plays a more critical role in shaping legal awareness than access to digital platforms alone. Rather, this implies a call for further research on other personal, social, or contextual factors that may account for awareness in cybercrime legislation and would support more specific educational or awareness drives.

4. Significant Difference between the Assessment of the three groups of respondents on the level of awareness of RA 10175.

Table 3

Analysis of variants showing the Difference between the assessment of the three groups of respondents on their level of awareness

Sources of Variation		Sum of Squares	df	Mean Square	f	Sig.
PROVISION	Between Groups	7.080	2	3.540	7.931	0.000
	Within Groups	174.503	391	0.446		
	Total	**181.582**	**393**			
PUNISHABLE ACTS	Between Groups	7.887	2	3.944	7.583	0.001
	Within Groups	**203.361**	**391**	**0.520**		
	Total	**211.249**	**393**			
PENALTY	Between Groups	7.195	2	3.597	5.213	0.006
	Within Groups	269.839	391	0.690		
	Total	**277.034**	**393**			
Overall	Between Groups	7.375	2	3.687	7.994	0.000
	Within Groups	180.355	391	0.461		
	Total	**187.730**	**393**			

Note: sig @ 0.05 is significant

The analysis of variance of awareness levels among the three groups of respondents regarding RA 10175, the Cybercrime Prevention Act of 2012, indicates a significant difference among the groups. On average, the significantly lower

P-ISSN: 0119-3058
E-ISSN: 2945-4093

awareness among residents underscores the need for community-level and non-institution-based awareness initiatives that go beyond schools and formal organizations.

In particular, there were significant differences among responses from the Business Sector, Schools, and Residents on all items of the Act, including its provisions, punishable acts, penalties, and general awareness. These disparities show inequalities in exposure, access to information, or use of legal and educational resources, suggesting that certain groups may have a better grasp of particular aspects of the law than others.

It follows that different groups of respondents in Bangued, Abra, perceive different levels of awareness regarding RA 10175. The results have highlighted the need for customized educational interventions and awareness campaigns for various groups to help them understand and comply with the Cybercrime Prevention Act.

Summary of the Scheffe

The Cybercrime Prevention Act 2012 (RA 10175) is interpreted differently by the different respondent types in Bangued, Abra. Given their continually low evaluations on the Act's provisions, punishable acts, punishments, and overall awareness, these results support the notion that residents are less familiar with the legislation and its principles than the Business Sector and School groups.

The business sector and schools, however, don't really differ from one another. Therefore, it seems they share similar views on the Cybercrime Prevention Act; in this regard, both groups have reached the same level of awareness due to equal exposure to information, training, or educational resources. This implies that, despite awareness of the Cybercrime Prevention Act, RA 10175, both business sectors and educational institutions exhibit a similar inadequate understanding of the legal framework and its enforcement, perhaps due to comparable exposure to information and training. Chang (2020) cited the Budapest Convention's framework for harmonizing cybercrime laws as evidence for this. Therefore, to improve comprehension and compliance, the research advocates greater awareness-raising efforts that connect local law to worldwide cybersecurity norms.

Overall, the Business Sector and School participants tend to show similar levels of awareness, whereas the residents show a much lower level of understanding. To close the awareness gap and ensure that every member of the community has a thorough understanding of the Cybercrime Prevention Act, our findings emphasize the need for targeted awareness creation among residents.

P-ISSN: 0119-3058
E-ISSN: 2945-4093

The Vector: International Journal of Emerging Science, Technology and Management
Volume 34, Issue 1, January - December 2025

5. The Proposed Action Plan

The proposed action plan was formulated directly from the identified awareness gaps, particularly the low understanding of penalties and the consistently lower awareness among residents.

Table 4
The Proposed Action Plan

Concern	Component Program	Specific Objectives	Implementation Strategies	Respon-sible Agencies/ Stake-holders	Time Frame	Expected Outcome
Low public knowledge of punishable cyber offenses	Public Cybercrime Awareness Campaign	Increase public knowledge and understanding of punishable cybercrimes	Conduct localized seminars and webinars; distribute infographics and flyers (in Filipino and local dialects); showcase real-life examples of cybercrime cases	DICT, DOJ, DepEd, LGUs, NBI	6–12 months	Improved public recognition of different types of punishable cyber offenses
Lack of awareness of the legal consequences of cybercrime	Penalty-Focused Legal Literacy Program	Educate citizens on the legal consequences of committing cyber offenses	Launch penalty-focused campaigns via community chats; integrate penalties into educational modules and youth programs; invite legal	DOJ, NBI, DepEd, CHED, Barangay Councils	6–12 months	Improved deterrent effect through awareness of sanctions

Concern	Component Program	Specific Objectives	Implementation Strategies	Respon-sible Agencies/ Stake-holders	Time Frame	Expected Outcome
			experts for community.			
Gaps in Cyber Law knowledge in the business sector	Compliance Training for Private Enterprises	Better compliance and reduced cyber offenses in business sectors	Partner with local chambers of commerce; conduct workshops; encourage adoption of internal reporting and protection systems	DILG, DICT, Business Groups, Tech Firms	6–12 months	Higher compliance and reduced business-related cyber offenses
Incomplete coverage in the education curriculum	Cybercrime Education Integration Program	Improve student knowledge of cybercrime laws, punishable acts, and penalties.	Integrate RA 10175 topics in Araling Panlipunan, Edukasyong Pantahanan, and ICT; organize student forums and competitions; collaborate with CHED for college-level modules.	DepEd, CHED, School Administrators, LGUs	12-24 months	Improved knowledge of cyber laws and preventive behaviors among students

P-ISSN: 0119-3058
E-ISSN: 2945-4093

The Vector: International Journal of Emerging Science, Technology and Management
Volume 34, Issue 1, January - December 2025

Concern	Component Program	Specific Objectives	Implementation Strategies	Respon-sible Agencies/ Stake-holders	Time Frame	Expected Outcome
Lack of localized, comprehensible materials	Community-Based Information Dissemination Initiative	Increase localized understanding of punishable acts and penalties	Translate and simplify RA 10175 into accessible pamphlets; use local dialects; involve barangay officials and youth volunteers in education efforts	LGUs, Barangay Units, NGOs, PNP-ACG	6-12 months	Increased grassroots-level awareness and community engagement in cybercrime prevention

The strategy suggests a Public Cybercrime Awareness Campaign to raise residents' awareness of cybercrimes and alleviate poor public awareness of chargeable cyber violations. Localized webinars and seminars, leaflets and infographics in Filipino and regional dialects, and real-world instances of cybercrime incidents are all part of this campaign. Over the course of six to twelve months, the DICT, DOJ, DepEd, LGUs, and NBI will carry out the program, which is anticipated to raise public awareness and comprehension of criminal internet violations.

A Penalty-Focused Legal Literacy Program aims to educate people about the legal penalties for cybercrime to address ignorance of those penalties. The implementation strategies of the Penalty-Focused Campaign include the use of penalties in educational modules and at youth events, and the hosting of community meetings moderated by lawyers and law enforcement officers. The project will run and be overseen by members of the DOJ, NBI, DepEd, CHED, and the Barangay Councils over six to twelve months, expected to improve the deterrent effects and awareness of the penalties under the laws.

Compliance Training for Private Enterprises is recommended to help address knowledge gaps in cyber law among members of the private sector. Coordination with local chambers of commerce, conduct of cybercrime protection seminars, and creation of reporting and protection systems within the company are part of this program. The implementation shall be monitored by the DILG, DICT, chambers of commerce, and IT firms for six to twelve months to improve compliance and reduce cybercrime in the private sector.

P-ISSN: 0119-3058
E-ISSN: 2945-4093

The Cybercrime Education Integration Program will improve students' understanding of cyber laws, punishable activities, and sanctions to fill gaps in the curriculum. Techniques include creating forums and competitions, creating college-level modules in partnership with CHED, and incorporating RA 10175 issues into Araling Panlipunan, Edukasyong Pantahanan, and ICT courses. The program, which is carried out over 12 to 24 months by DepEd, CHED, school administrators, and local government units, aims to increase students' awareness and preventive practices.

Lastly, the Community-Based Information Dissemination Initiative would translate and simplify RA 10175 into easily readable pamphlets in regional languages and actively involve young volunteers and barangay officials to address the dearth of localized, understandable materials. Within six to twelve months, LGUs, barangay units, NGOs, and PNP-ACG will carry out this initiative, which aims to raise community involvement and understanding of cybercrime prevention.

CONCLUSIONS

According to the survey, a higher proportion of respondents in Bangued, Abra, are young, female, educated, and own mobile phones and other ICT devices. They also extensively rely on social media, particularly Facebook, for information. The Cybercrime Prevention Act of 2012 (RA 10175) is generally understood by the Business Sector, Schools, and Residents, especially regarding its provisions and punishable acts. However, residents have the least awareness of the penalties when compared to the other two groups. Furthermore, overall, the findings reveal that awareness of RA 10175 in Bangued, Abra, is uneven across sectors, with knowledge concentrated on provisions and punishable acts but limited understanding of penalties. These results highlight the need for localized, sector-specific approaches to cybercrime awareness that emphasize legal consequences and practical application.

RECOMMENDATIONS

It is recommended that concerned government agencies, educational institutions, and local stakeholders adopt the proposed action plan to address sector-specific awareness gaps on RA 10175. Priority should be given to resident-focused and penalty-oriented awareness initiatives. Integration of cybercrime law education into school curricula and business compliance programs is likewise encouraged. Future studies may examine behavioral compliance and reporting practices related to cybercrime legislation.

ETHICAL STATEMENT

The study has formal approval from the Ethical Review Committee of the University of Northern Philippines (Approval No. A-2025-032). To conform to

Republic Act No. 10173, also known as the Data Privacy Act of 2012, it strives to promote voluntary response, privacy, and confidentiality while adhering closely to ethical research practices. To ensure that the study was beneficial to the participants and the community at large, the principle of beneficence has been observed, and all sources are appropriately acknowledged in accordance with the APA 7th edition guidelines.

ACKNOWLEDGMENT

The researchers would like to thank Dr. Edmar M. Paguirigan, Dr. Edelyn A. Cadorna, the University Research and Development Office Personnel & Staff, and Dr. Erwin F. Cadorna, President of UNP, for their support, encouragement, and faith in the researchers' ability to succeed. Above all, the researchers would like to express their sincere gratitude to Almighty God, whose health, power, and wisdom have sustained them. This achievement would not have been possible without your love, support, and trust.

REFERENCES

Brauer, K. & Proyer, R. (2017). Are impostors playful? Testing the association of adult playfulness with the impostor phenomenon. *Personality and Individual Differences, 116*, 57–62. https://doi.org/10.3389/fpsyg.2018.01440

Abdajabar, A., & Md Yunus, N. A. (2023). A review of the impact of cybersecurity crimes in financial institutions during the time of COVID-19. *Acta Informatica Malaysia, 7*(1), 19–23. https://doi.org/10.26480/aim.01.2023.19.23

Agup, R. M. (2024). Data Privacy Act: Awareness, compliance, and challenges of nurses of government hospitals in Northern Philippines. *South Eastern European Journal of Public Health, 25*. https://doi.org/10.XXXX/seejph2024

Bele, J.-L., et al. (2014). *Raising awareness of cybercrime: The use of education as a means of prevention and protection*. International Association for the Development of the Information Society. https://eric.ed.gov/?id=ED557216

Colubong, M. R. T., Cabudol, H. M. L. S., Pagay, J. B., Belizar, R. R. D., Gabutan, J. M. F. S., Pula, P. A., Friala, B. P. J. F., & Cabides, J. T. (2024). E-cigarette: Exploring awareness and understanding of students in a state university in the Philippines. *South Eastern European Journal of Public Health*, 2065–2074. https://doi.org/10.70135/seejph.vi.2819

Chang, L. Y. C. (2020). Legislative frameworks against cybercrime: The Budapest Convention and Asia. In T. J. Holt & A. M. Bossler (Eds.), *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 327–343). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3_6

CEDTyClea. (2024, December 3). 3% of cyber threats in region target PHL firms—Study. *BusinessWorld Online*.

https://www.bworldonline.com/corporate/2024/12/04/639136/3-of-cyber-threats-in-region-target-phl-firms-study/

Garcia, A. B., & Bongo, S. M. C. (2022). A cybersecurity cognizance among college teachers and students in embracing online education. In *Proceedings of the IEEE International Conference on Information Management (ICIM)*. IEEE. https://doi.org/10.1109/ICIM56520.2022.00028

Pasinhon, L., & Donato, L. M. (2024). Capability of the regional anti-cybercrime unit–Cordillera (RACU-COR) in handling cybercrime cases. *Asia Pacific Journal of Advanced Education and Technology, 2*(3). https://doi.org/10.54476/apjaet/06740

Tamayo, R., Tamayo, E., Darisan, L., Rodillas, F., Cabangbang, I., & Gerona, I. (2024). Journey to heroism: Lived experiences of overseas Filipino worker (OFW) nurses working in hospitals during the COVID-19 pandemic. *South Eastern European Journal of Public Health, 25*. https://doi.org/10.XXXX/seejph2024

Tupas, E. (2024, February 11). PNP: 19,000 cybercrimes recorded last year. *Philstar.com*. https://www.philstar.com/headlines/2024/02/11/2332462/pnp-19000-cybercrimes-recorded-last-year/