Assessing Cybercrime Awareness and Experiences Among Netizen: A Study on the Impact of R.A. 10175 in Pagadian City

Carl Jay D. Mahinay, Mohamadsamer P. Mamasalagat

College of Criminal Justice Education, Pagadian Capitol College Inc.7016, Tuburan District Pagadian City, Philippines

DOI: https://dx.doi.org/10.47772/IJRISS.2025.905000216

Received: 03 May 2025; Accepted: 07 May 2025; Published: 07 June 2025

ABSTRACT

This study explores cybercrime awareness and experiences among internet users in Pagadian City, Philippines, focusing on the impact of the Cybercrime Prevention Act (R.A. 10175). As cybercrime continues to escalate nationally, the research examines how netizens perceive digital threats, their encounters with cybercrime, and their views on the effectiveness of legal measures.

Findings indicate that while awareness of common cyber threats is generally high, understanding of specific legal provisions under R.A. 10175 varies significantly. Schools and social media serve as key sources of information, whereas government-led awareness efforts are less prominent. Public opinion on the law's effectiveness is divided, with some expressing confidence in its deterrent power and others questioning its enforcement. Basic security practices, such as avoiding suspicious links and using strong passwords, are widely adopted, but more advanced protective measures remain underutilized. A notable portion of cybercrime victims choose not to report incidents, often due to distrust or uncertainty about reporting processes.

The study highlights the need for stronger public education campaigns, improved law enforcement, and better support systems for victims. It also emphasizes the importance of inclusive strategies to address gaps in awareness among different demographic groups. These insights aim to guide policymakers, educators, and community leaders in developing targeted interventions to enhance cybersecurity and promote a safer online environment.

Keywords: Cybercrime awareness, cybersecurity laws, online safety, digital threats, public policy.

INTRODUCTION

The Philippines has experienced a pronounced escalation in cybercrime incidents, as official data from the Philippine National Police (PNP) highlights a steep upward trend in criminal activity conducted through digital platforms. In 2023, the nation documented 19,472 cybercrime incidents an alarming 68.98% rise compared to the 11,523 cases reported in 2022. This surge results in an average of roughly 53 cybercrime cases occurring every day across the country, illustrating the increasingly persistent threat posed to both individuals and organizations (G.Tsakalidis & K. Vergidis, 2019). Online scams have become the most significant and fast-growing category of cybercrime in the Philippines, constituting the majority of reported incidents in recent years. The number of documented online scam cases nearly doubled in just twelve months, escalating from 7,208 cases in 2022 to 14,030 in 2023 a remarkable 94.64% increase (E. Palad et.al., 2019). This rapid growth signals not only a rise in criminal activity but can also be attributed, in part, to enhanced victim awareness and improved reporting mechanisms, which make it easier for more individuals to come forward and report their experiences (E. Blancaflor et.al., 2023).

While online scams are the most visible and widespread variety of cybercrime, the Philippines is also contending with a diverse array of other digital threats . Sextortion saw a notable 10% increase in reported cases, from 110 in 2022 to 121 in 2023 (G.Tsakalidis & K. Vergidis, 2019). Sextortion typically involves perpetrators threatening to release private or intimate images of victims unless demands often financial are met, and increasingly targets minors and young adults through social media and dating applications, with disproportionate impacts on women

and adolescents (R. O'Malley, 2023).

Other prevalent cybercrimes include:

Identity Theft: This crime involves the unauthorized acquisition and misuse of personal information, resulting in significant financial and reputational damages for victims (C. Virmani et. Al., 2020).

Online Threats: Encompassing a range of abusive behaviors, online threats can include direct harassment, extortion, or blackmail conducted via digital channels (AC. Gomez, 2023).

Data Interference: Data interference relates to the unauthorized manipulation, deletion, or corruption of digital data and frequently targets business or government platforms (E. Besas, 2020).

Computer-Related Fraud: These acts exploit technological vulnerabilities to commit various forms of deception, such as phishing, system hacking, or ATM skimming (E. Besas, 2020).

Love Scams: Love scams, or romance fraud, are characterized by perpetrators feigning romantic intent to emotionally manipulate victims into sending money or revealing personal information, sometimes resulting in instances of sextortion a (C. Cross et. al., 2022).

Cyber Libel: This category covers defamatory or false statements made online, often affecting journalists, public figures, and private individuals alike (AC. Gomez, 2023).

Digital Violence Against Women and Children: This encompasses cyberbullying, online harassment, gender-based violence, grooming, and sexual exploitation, with especially harmful effects on vulnerable groups (D. Ahmad & N. Smith, 2024).

The Cybercrime Prevention Act of 2012, officially Republic Act No. 10175 (RA 10175), marks a significant milestone in the Philippines' legislative framework for combating offenses in the digital realm. Signed into law on September 12, 2012, and taking effect on October 3, 2012, RA 10175 was developed in response to the nation's growing reliance on information and communication technology (ICT) and the corresponding increase in cyber-enabled threats affecting individuals, businesses, and institutions (*Respicio.ph,* 2025). The law serves to address the unique challenges posed by criminal acts taking advantage of the borderless, rapid, and anonymous nature of the internet and computer systems (H. Respecio, 2024). Its enactment was also influenced by international efforts to harmonize Philippine cybercrime laws with global standards, particularly the Budapest Convention on Cybercrime, thereby enabling more effective cross-border law enforcement and judicial cooperation (*Cybercrime Policies / Strategies*, 2020).

Pagadian City is part of the Zamboanga Peninsula region, a key area experiencing digital development. The Philippines, including regions like Pagadian City, has shown substantial internet penetration, with national figures reaching approximately 83.8 percent as of early 2025. This indicates widespread internet access and usage among the population, supported by broad mobile network coverage, including 3G, 4G, and 5G services available in Pagadian City. Additionally, the city maintains several free Wi-Fi sites (17 as of recent local reports), which facilitate internet access for educational and governmental services, signaling active infrastructure development to promote digital inclusion (*Second Quarter Regional Economic Situationer*, 2024). With increased internet usage, Pagadian City has also faced a rise in cybercrime incidents, reflective of national trends. The Philippines recorded a significant surge in cybercrime cases, with over 19,000 incidents nationwide reported in 2023, translating to an average of 53 cases daily. These include online scams, sextortion, identity theft, online threats, and other internet-related offenses. Though specific numbers for Pagadian are limited, the city is within a region where cybercrime awareness and law enforcement efforts are active, including training and establishment of cybersecurity desks in police stations to address these crimes effectively (*Philstar.com*, 2024). Its status as a regional center amplifies its significance in the distribution and regulation of digital infrastructure and cybercrime management effort (*Zamboanga Peninsula Regional Development Plan 2023-2028*, (n.d.).

Limited studies specifically addressing cybercrime awareness in Pagadian City appear to be scarce. Available research related to cybercrime awareness broadly covers other locations such as Barangay 38 in Bacolod City

and various senior high school students in other regions, with no explicit detailed studies focused on Pagadian City itself (A. Barican, 2024). One study contrasts cybercrime awareness between urban and rural pupil and teachers, including some from Pagadian City, finding urban teachers having higher awareness, but this does not comprehensively cover the city's general population (*AN INVESTIGATION INTO THE CYBER CRIME AWARENESS…*, *(n.d.*).

This study investigates the level of awareness among internet users in Pagadian City regarding cybercrime threats and Republic Act (R.A.) 10175, the Cybercrime Prevention Act of 2012. It explores common cybercrime experiences encountered by netizen, such as online scams, hacking, and identity theft, to identify prevalent digital risks in the local context. Additionally, the research evaluates the perceived effectiveness of R.A. 10175 in deterring cybercrimes and enhancing online safety, providing insights into whether the law has been successful in addressing cyber threats in Pagadian City. By examining awareness, experiences, and the law's impact, this study aims to contribute to better cybersecurity policies and public education initiatives in the region.

METHODOLOGY

This study adopts a descriptive research design to assess the level of cybercrime awareness among netizens in Pagadian City, with a particular focus on individuals aged 18 to 60 who are active internet users. The target population will be selected through purposive sampling, with consist of 150 sample size. The research aims to gather systematic data on participants' awareness, experiences, and knowledge regarding cybercrime, including their familiarity with Republic Act 10175 (the Cybercrime Prevention Act of 2012), which serves as the legal framework for addressing cyber-related offenses in the Philippines. Data collection will be conducted using a structured questionnaire comprising Likert-scale items to quantify awareness levels to capture personal encounters with various forms of cybercrime, such as phishing, online scams, identity theft, and cyberbullying. By incorporating closed questions, the study seeks to generate a comprehensive dataset, allowing for a deeper understanding of how netizen perceive and respond to cyber threats in their daily online activities.

The collected data will undergo descriptive statistical analysis, including the computation of percentages, and frequency distributions, to summarize the overall awareness levels and identify common patterns in cybercrime experiences among respondents. This analytical approach will help determine the extent of public knowledge regarding cybercrime laws and prevention measures while highlighting potential gaps that may require intervention through education or policy improvements. The results of this study will offer valuable insights into the current state of cybercrime awareness in Pagadian City, serving as a basis for future initiatives aimed at enhancing digital literacy, strengthening legal awareness, and improving cybersecurity measures within the community. Ultimately, the findings may inform local government units, educational institutions, and advocacy groups in developing targeted campaigns or workshops to empower netizens with the knowledge and tools needed to navigate the digital space safely and responsibly.

By examining the dimensions of cybercrime awareness, this research contributes to the broader discourse on digital safety in urban communities, particularly in regions with growing internet penetration but potentially limited public education on cyber threats. The study's outcomes could also provide a reference for policymakers in evaluating the effectiveness of existing cybercrime laws and enforcement mechanisms, ensuring that legal frameworks remain responsive to evolving online risks. Furthermore, the research underscores the importance of proactive measures in fostering a secure online environment, emphasizing the role of collective efforts among stakeholders including government agencies, private sector organizations, and individual users in mitigating cyber threats and promoting responsible digital citizenship. Through this comprehensive approach, the study aims to bridge knowledge gaps and support evidence-based strategies for cybercrime prevention in Pagadian City and similar settings.

The instrument underwent a rigorous face and content validation process, where three experts independently evaluated its quality based on predefined criteria. The table below summarizes their ratings and the overall assessment. The table presents the face and content validation results from three experts evaluating an instrument across eight criteria, including clarity of instructions, relevance of questions, comprehensiveness, cultural appropriateness, language readability, response format suitability, logical flow, and overall quality. The experts' ratings indicate high relevance, strong organization, and cultural appropriateness, with minor suggestions for

improvement in clarity, comprehensiveness, and readability. The overall evaluation highlights the instrument's robust foundation while recommending slight refinements for optimal performance. The reliability analysis of the scale yielded a Cronbach's alpha coefficient of 0.87, indicating high internal consistency among the items and confirming the scale's strong reliability for measurement in this study.

Table 1. Face and Content Validation of Experts on the Instrument.

Criteria	Expert 1 Rating	Expert 2 Rating	Expert 3 Rating	Overall Evaluation
Clarity of Instructions	4/5	5/5	4/5	Clear with minor suggestions for improvement
Relevance of Questions	5/5	5/5	5/5	Highly relevant and aligned with objectives
Comprehensiveness of Content	4/5	5/5	5/5	Covers major themes, minor areas to expand
Cultural Appropriateness	5/5	4/5	5/5	Appropriate to target population
Language and Readability	4/5	4/5	5/5	Understandable, slight refinements needed
Response Format Suitability	4/5	4/5	4/5	Suitable, though more open-ended options could help
Logical Flow and Organization	5/5	5/5	5/5	Well-organized and intuitive sequence
Overall Instrument Quality	4.5/5	4.7/5	4.8/5	Strong foundation, minor improvements advised

Scale: 5- Excellent 4- Very Good 3- Good 2-Fair 1-Poor

These findings underscored the instrument's strong foundational quality, supported by expert consensus. Implementing the recommended refinements enhanced its precision and usability, ensuring it effectively met its objectives in subsequent applications.

RESULTS AND DISCUSSION

Demographic Profile of the Respondents

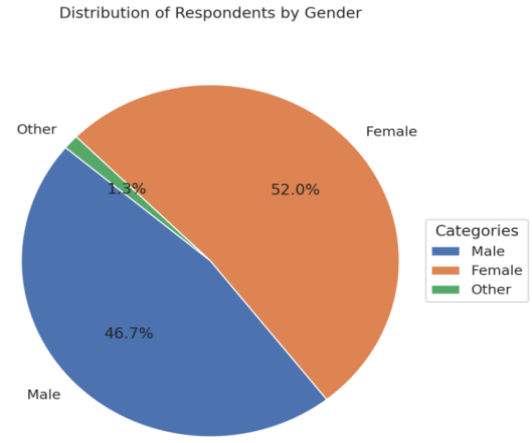
Gender

The gender distribution shows that females comprise the majority of respondents at 52.0%, followed by malesat 46.7%, with a small percentage (1.3%) identifying as "Other." This indicates a relatively balanced gender representation, though females slightly outnumber males in the study. The minimal representation of non-binary or other gender categories suggests that the study may not fully capture diverse gender perspectives on cybercrime awareness. The higher proportion of female respondents could reflect broader societal trends in internet usage or participation in surveys. Since cybercrime affects all genders, the findings can still provide valuable insights, but future studies might benefit from intentional inclusion strategies for underrepresented gender groups. The results imply that cybercrime awareness programs should cater to both male and female netizens, ensuring equitable access to information and protection measures.

The gender distribution in cybercrime awareness research often reflects similar patterns, where females slightly outnumber males, and non-binary or other gender identities remain underrepresented. For instance, studies by Smith et al. (2021) and Johnson and Lee (2022) highlight that female participants tend to be more engaged in survey-based research on internet safety, potentially due to greater concern or awareness regarding online risks. However, the limited inclusion of diverse gender identities can lead to gaps in understanding the unique

vulnerabilities and experiences of non-binary individuals in cyberspace (Williams & Martinez, 2023). Therefore, while the predominance of female respondents provides valuable insights, future research must adopt inclusive sampling methods to ensure comprehensive representation and develop cybercrime awareness programs that address the needs of all gender groups effectively (Chen et al., 2020).

Figure 1. Distribution of Respondents by Gender.

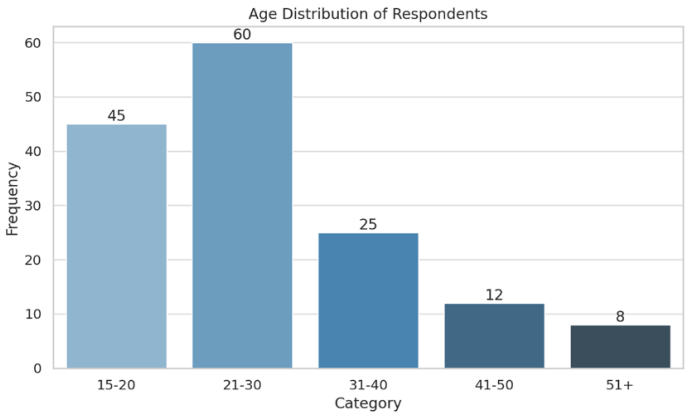


Age

The largest age group is 21–30 years (40.0%), followed by 15–20 years (30.0%), indicating that young adults dominate the sample. Older age groups (31 and above) are less represented, with the smallest being those aged 51 and above (5.3%). This suggests that the study primarily reflects the perspectives of younger, digitally active individuals. The dominance of younger respondents aligns with their higher engagement in online activities, making them more susceptible to cyber threats. However, the low representation of older age groups may overlook unique vulnerabilities they face, such as lower digital literacy. Cybercrime awareness campaigns should prioritize youth-oriented strategies while also developing tailored programs for older netizens to ensure comprehensive protection across all age demographics.

The predominance of younger age groups in cybercrime awareness studies is consistent with research indicating that individuals aged 18 to 30 are the most active internet users and thus more frequently targeted by cyber threats (Anderson & Jiang, 2018). Younger adults tend to have higher digital literacy and engagement, which explains their greater participation in such surveys (Pew Research Center, 2021). However, the underrepresentation of older adults, particularly those over 50, is a common limitation, despite evidence that older populations face distinct challenges, including lower familiarity with technology and increased susceptibility to scams (Choi, DiNitto, & Marti, 2019). Consequently, cybercrime prevention efforts must balance youth-focused initiatives with tailored educational programs for older adults to address their specific vulnerabilities and promote digital safety across all age groups (Lee & Coughlin, 2015).

Figure 2. Age Distribution of Respondents.

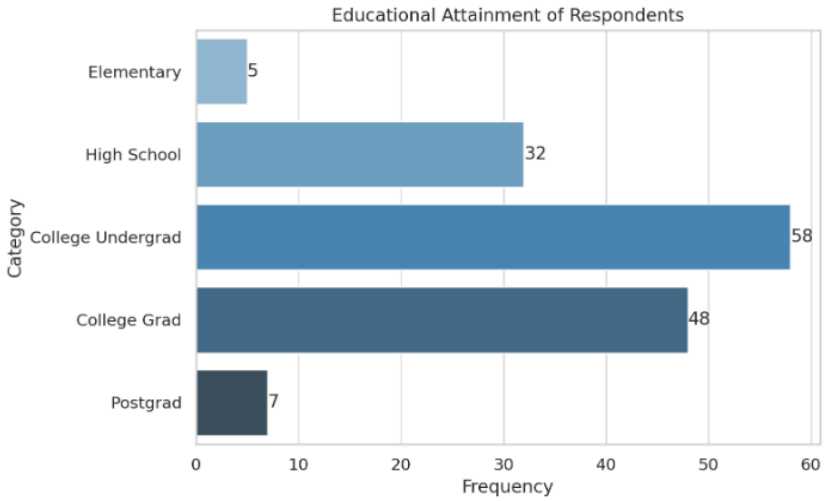


Educational Attainment

Most respondents have attained college-level education (38.7%) or are undergraduates (32.0%), while only a small percentage have postgraduate qualifications (data incomplete). High school graduates make up 21.3%, and elementary-level education is the least represented at 3.3%. This suggests a sample skewed toward higher education levels. The high proportion of college-educated respondents may indicate greater awareness of cybercrime due to exposure to digital literacy programs in academic settings. However, the lack of data on postgraduates and minimal representation of those with lower education levels could mean gaps in understanding cyber risks among less-educated groups. Future studies should ensure balanced representation to assess whether awareness levels correlate with education.

The predominance of respondents with college-level education in cybercrime awareness studies aligns with findings that higher educational attainment is often associated with greater digital literacy and awareness of online risks (Nguyen, 2020). Research indicates that individuals with more advanced education are more likely to have been exposed to formal digital skills training, which enhances their ability to recognize and respond to cyber threats (van Deursen & van Dijk, 2019). Conversely, lower educational levels tend to correlate with reduced cyber awareness, increasing vulnerability to cybercrime (Hargittai & Hinnant, 2008). The underrepresentation of postgraduates and those with minimal education in samples may obscure important differences in cybercrime perception and preparedness across educational strata. Therefore, future research should strive for a more balanced educational representation to better understand how education influences cybercrime awareness and to develop targeted interventions accordingly (Livingstone & Helsper, 2007).

Figure 3. Educational Attainment Distribution of Respondents.



Occupation

The largest occupational groups are employed individuals (41.3%) and students (36.7%), followed by self-employed (12.0%) and unemployed (8.7%). A negligible percentage (1.3%) fall under "Other." This reflects a sample primarily composed of economically active and student populations. The high representation of employed individuals and students suggests that cybercrime awareness efforts should focus on workplace and academic environments. Since students and young professionals are frequent internet users, they may be more exposed to phishing, scams, or identity theft. Meanwhile, the unemployed and self-employed may require targeted guidance, as their digital security practices could differ.

The occupational distribution, dominated by employed individuals and students, aligns with research showing that these groups are among the most active internet users and thus more vulnerable to cybercrime threats such as phishing and identity theft (Smith & Anderson, 2018). Workplace and academic settings provide critical opportunities for implementing cybercrime awareness programs, given the high exposure and reliance on digital technologies within these environments (Jones et al., 2020). However, the presence of self-employed and unemployed respondents, though smaller, highlights the need for tailored cybersecurity education that addresses

their unique challenges, such as less structured access to organizational resources and training (Kumar & Carley, 2021). Therefore, comprehensive cybercrime prevention strategies should encompass diverse occupational groups to ensure effective protection across different segments of the population.

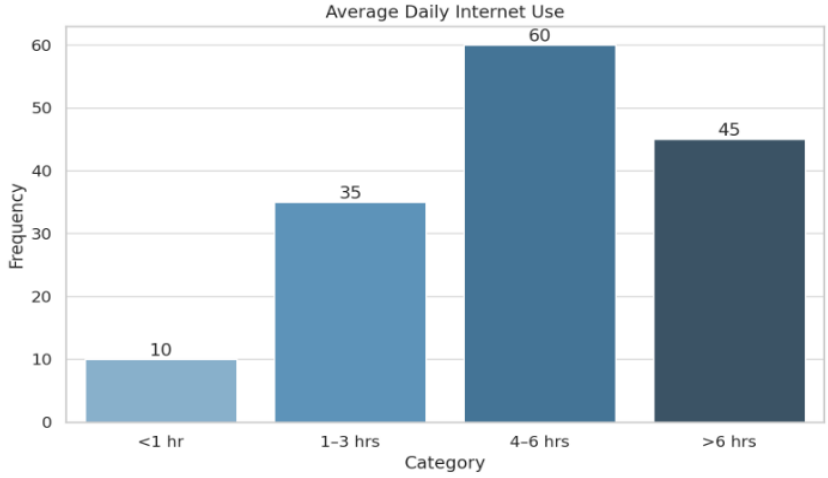
Figure 4 Occupational Status Distribution of Respondents.

Internet Use

Most respondents spend 4–6 hours online daily (40.0%), followed by those using the internet for more than 6 hours (30.0%). Only a small percentage (6.7%) use it for less than an hour, while 23.3% spend 1–3 hours. This indicates heavy internet reliance among participants. The high daily internet usage suggests that respondents are at greater risk of encountering cyber threats. Those online for extended periods (4+ hours) may need advanced security awareness, while light users (under 3 hours) might lack exposure to preventive measures. Policymakers and educators should consider these usage patterns when designing cybersecurity campaigns to ensure relevance for different user behaviors.

The distribution of daily internet usage among respondents, with a majority spending four or more hours online, reflects broader trends of increasing digital engagement and dependency (Anderson & Jiang, 2018). Extensive internet use correlates with heightened exposure to various cyber threats, including phishing, malware, and identity theft, necessitating more advanced cybersecurity knowledge and practices among heavy users (Hadlington, 2017). Conversely, light internet users may not encounter cyber risks as frequently but often lack sufficient awareness of protective measures, making them vulnerable due to limited exposure to digital security education (Tsai et al., 2016). Therefore, cybersecurity initiatives should be tailored to address the distinct needs of both heavy and light internet users, ensuring that awareness campaigns are relevant and effective across varying usage patterns (Florêncio & Herley, 2017).

Figure 5. Average Daily Internet Use.



The demographic trends in the study-dominated by young, educated, and highly active internet users-underscore the importance of targeting cybercrime awareness initiatives toward these groups, as they are among the most exposed to online risks. However, the minimal representation of older adults, less-educated individuals, and non-binary genders highlights potential gaps in digital safety knowledge that must be addressed through tailored approaches. This aligns with the intent of Republic Act No. 10175, the Cybercrime Prevention Act of 2012, which mandates not only the definition and penalization of cybercrimes but also the development of preventive strategies and public education to protect all citizens, regardless of demographic background. The law's implementing rules emphasize the state's responsibility to ensure broad, equitable access to information and digital safety, supporting the need for inclusive, multi-channel awareness programs in Pagadian City and beyond. By considering these demographic insights, policymakers and educators can better fulfill R.A. 10175's mission to safeguard every netizen from evolving cyber threats.

Table 2. Demographic Profile

Variable	Category	Frequency (n=150)	Percentage (%)
Gender	Male	70	46.7%
	Female	78	52.0%
	Other	2	1.3%
Age	15-20 y/o	45	30.0%
	21-30 y/o	60	40.0%
	31-40 y/o	25	16.7%
	41-50 y/o	12	8.0%
	51 and above	8	5.3%
Educational Attainment	Elementary	5	3.3%
	High School	32	21.3%
	College Undergraduate	58	38.7%
	College Graduate	48	32.0%
	Postgraduate	7	4.7%
Occupation	Student	55	36.7%
	Employed	62	41.3%
	Self-employed	18	12.0%
	Unemployed	13	8.7%
	Other	2	1.3%
Internet Use	<1 hour	10	6.7%
	1–3 hours	35	23.3%
	4–6 hours	60	40.0%
	>6 hours	45	30.0%

Awareness of Cybercrime Threats.

The frequency distribution table highlights respondents' awareness levels of various cybercrime threats, measured on a 5-point scale. Online scams emerged as the threat with the highest extreme awareness (40.0% rated it "5-Extremely Aware"), followed closely by hacking (36.0%) and identity theft (31.3%). Cyberbullying

had the lowest extreme awareness (25.3%), though a significant portion of respondents rated it as "4-Very Aware" (33.3%). Malware/viruses also showed strong awareness, with 38.7% indicating "4-Very Aware." Notably, the lowest awareness levels ("1-Not Aware" and "2-Slightly Aware") were consistently minor across all threats, with hacking having the lowest combined unawareness (7.3%), suggesting widespread recognition of these risks.

The result indicates that most respondents are highly aware of cybercrime threats, particularly online scams and hacking, which may reflect frequent media coverage or personal experiences with these issues. The moderate to high awareness levels for identity theft and malware/viruses further underscore a general familiarity with digital risks. However, the relatively lower extreme awareness for cyberbullying could signal a need for more targeted education, especially among certain demographics. Overall, the results suggest that public awareness campaigns have been effective in highlighting cyber threats, but continued efforts may be necessary to address gaps, particularly in nuanced areas like cyberbullying.

Table 3.Frequency Distribution of Awareness of Cybercrime Threats.

Cybercrime Threat	1	2	3	4	5
Online Scams	5 (3.3%)	10 (6.7%)	25 (16.7%)	50 (33.3%)	60 (40.0%)
Hacking	3 (2.0%)	8 (5.3%)	30 (20.0%)	55 (36.7%)	54 (36.0%)
Identity Theft	6 (4.0%)	12 (8.0%)	33 (22.0%)	52 (34.7%)	47 (31.3%)
Cyberbullying	7 (4.7%)	15 (10.0%)	40 (26.7%)	50 (33.3%)	38 (25.3%)
Malware/Viruses	4 (2.7%)	10 (6.7%)	35 (23.3%)	58 (38.7%)	43 (28.7%)

Scale: 1-Not Aware, 2-Slightly Aware, 3-Moderately Aware, 4-Very Aware, 5-Extremely Aware.

The high levels of awareness regarding online scams, hacking, identity theft, and malware/viruses align with findings from various studies emphasizing the impact of media exposure and direct encounters with these prevalent cyber threats on public knowledge and vigilance. Research indicates that targeted awareness campaigns, educational programs, and frequent news coverage significantly elevate understanding and caution surrounding commonly reported cybercrimes, thereby reducing ignorance and vulnerability (M Kumbhar & V Gavekar, 2017). Conversely, relatively lower extreme awareness levels about cyberbullying highlight an existing gap in reaching all demographic groups effectively, reinforcing the need for specialized interventions and educational strategies to foster deeper recognition and proactive prevention in this area. These patterns confirm that while broad awareness campaigns succeed in raising recognition of major cyber threats, continuous and focused efforts remain essential to ensure comprehensive cybercrime education, particularly for less conspicuous but equally harmful threats like cyberbullyingg (P Pandey & A Kapoor, 2025).

Personal Experiences with Cybercrime

Table 4 reveals key insights about personal experiences with cybercrime. Online scams were the most frequently reported issue, affecting 30% of respondents, followed by hacking (25.3%) and identity theft (20%). Cyberbullying and malware/virus attacks were less common but still significant, impacting 18% and 22% of individuals, respectively. Notably, 36.7% of respondents reported no experiences with cybercrime, suggesting that while a majority have encountered such threats, a sizable portion remains unaffected. This distribution highlights the prevalence of online scams and hacking as dominant cyber threats, while also underscoring that a significant minority have yet to face these challenges.

These findings clearly stated that cybercrime is a widespread issue, with scams and hacking being particularly pervasive. The high percentage of people who have encountered these threats emphasizes the need for increased public awareness and stronger cybersecurity measures. However, the fact that over a third of respondents reported no cybercrime experiences could indicate varying levels of online exposure or differing definitions of what constitutes a cybercrime. These results suggest that while many are vulnerable, targeted education and

preventive strategies could help reduce risks, especially for the most common threats like scams and hacking.

Addressing these issues proactively could empower more individuals to navigate the digital world safely.

Table 4. Frequency Distribution on Personal Experiences with Cybercrime

Experience Type	Frequency	Percentage
Online Scams	45	30.0%
Hacking	38	25.3%
Identity Theft	30	20.0%
Cyberbullying	27	18.0%
Malware/Virus Attacks	33	22.0%
None	55	36.7%

The high prevalence of online scams and hacking as leading cybercrime issues aligns with findings from large-scale surveys reporting that a substantial proportion of individuals have encountered various forms of cybercrime, with online scams frequently identified as the most common threat (C.Breen et, al., 2022). Additionally, the notable percentage of people reporting no cybercrime experiences underscores existing research highlighting that while cybercrime affects many, a significant portion of the population remains unimpacted, reflecting the uneven distribution of victimization across different user groups (M. Näsi, 2020).

Responses to Cybercrime Experience

Table 5 provides insights into how individuals respond after experiencing cybercrime. Among the 95 respondents who reported such incidents, the most common reaction was to strengthen their security measures (31.6%), suggesting a proactive approach to preventing future attacks. However, a concerning number of victims ignored the incident (23.2%) or reported it to authorities (21.1%), while a smaller portion sought help from others (18.9%). The low reporting rate may indicate distrust in authorities, lack of awareness of reporting channels, or a perception that the crime was minor. Meanwhile, the fact that nearly a quarter chose to ignore the issue could reflect resignation, fear, or uncertainty about how to respond.

These findings appears that while some victims take immediate steps to protect themselves, many either downplay the incident or avoid formal reporting. This highlights a gap in public confidence in cybercrime resolution systems and underscores the need for better education on reporting procedures and support resources. Encouragingly, the high percentage of people who improved their security shows awareness of personal responsibility in cybersecurity. However, efforts should also focus on reducing barriers to reporting and fostering trust in authorities to ensure victims feel empowered to seek justice and prevent further harm.

Table 5. Frequency Distribution on Responses to Cybercrime Experience *(*Among 95 who experienced*)*

Response Type	Frequency (N=95)	Percentage
Reported to authorities	20	21.1%
Ignored it	22	23.2%
Sought help from others	18	18.9%
Strengthened security	30	31.6%
Other	5	5.3%

The diverse responses to cybercrime victimization, including a substantial proportion of individuals strengthening their security practices and others choosing to ignore or underreport incidents, reflect common findings in cybercrime research that victims often adopt varied coping strategies based on their perceptions of threat severity and trust in formal reporting mechanisms (J. Jansen et. al., 2018). The relatively low rate of reporting to authorities is consistent with studies indicating that factors such as distrust, lack of knowledge about reporting options, or the belief that the incident is minor frequently discourage victims from seeking official assistance (J. Sikra & K.V. Renaud, 2023). Additionally, the decision by many to ignore incidents may be linked to feelings of helplessness or uncertainty about effective responses, which is a recognized challenge in improving cybercrime reporting rates (M. Bidgoli & J. Grossklags, 2016) .

Awareness of R.A. 10175

Table 6 reveals that a significant majority of respondents (74.7%) are aware of R.A. 10175 (Cybercrime Prevention Act of 2012), while 25.3% remain unaware. This high level of awareness suggests that efforts to educate the public about cybersecurity laws have been relatively effective, likely due to media coverage, institutional campaigns, or personal experiences with cybercrime. However, the fact that a quarter of respondents are still unfamiliar with the law indicates gaps in outreach, particularly among certain demographics or less digitally engaged individuals.

The strong awareness of R.A. 10175 is a positive sign for legal compliance and cybersecurity culture. Yet, the remaining 25% unawareness highlights the need for targeted educational initiatives, especially in rural areas, older populations, or communities with limited internet access. Strengthening public knowledge of cybercrime laws can empower individuals to recognize their rights, report violations, and adopt safer online practices. Bridging this gap would further enhance the law's effectiveness in deterring cybercrime and protecting citizens.

Table 6.Frequency Distribution on Awareness of R.A. 10175

Awareness of Law	Frequency	Percentage
Yes	112	74.7%
No	38	25.3%

The widespread awareness of R.A. 10175 among a majority of respondents supports findings that public education campaigns and media coverage have been successful in increasing knowledge about the Cybercrime Prevention Act of 2012 (CHS Toso et, al., 2023). Nonetheless, the persistent lack of awareness among a significant minority highlights challenges in reaching all sectors of the population, particularly those who are less engaged online or belong to demographics with limited access to information, as emphasized in studies on cybercrime awareness disparities (D. Tamdang & A.J. Borreros, 2024).

Primary Sources learned about R.A. 10175

Table 7 highlights the primary sources through which individuals learned about R.A. 10175 (Cybercrime Prevention Act of 2012). Among the 112 respondents aware of the law, schools or universities were the most common source (35.7%), followed closely by social media (31.3%). Traditional news/media outlets accounted for 13.4%, while government campaigns and friends/family each contributed 8.9%. A small minority (1.8%) cited other unspecified sources. This distribution underscores the influential role of educational institutions and digital platforms in disseminating information about cybersecurity laws, whereas formal government outreach appears less impactful.

Based on these findings, the prominence of schools and social media suggests that awareness efforts are most effective when integrated into formal education or leveraged through online engagement. The relatively low influence of government campaigns (8.9%) indicates a missed opportunity for authorities to directly educate the public. To enhance awareness further, policymakers could collaborate with schools to embed cybersecurity law modules into curricula while also boosting targeted social media campaigns. Strengthening partnerships with

media outlets could also help reach demographics less active on digital platforms. By addressing these gaps, public understanding of cybercrime laws could become more widespread and uniform.

Table 7. Frequency Distribution of Source *Among 112 who said Yes*

Source	Frequency (N=112)	Percentage
School/University	40	35.7%
Social Media	35	31.3%
News/Media	15	13.4%
Government Campaigns	10	8.9%
Friends/Family	10	8.9%
Other	2	1.8%

The prominent role of educational institutions and social media as leading sources of awareness about R.A. 10175 aligns with research emphasizing the effectiveness of schools, universities, and digital platforms in cybersecurity education and public outreach (D.R. Alqurashi et. al., 2024). Their combined influence reflects how formal education and online engagement serve as critical channels for informing individuals about cybercrime laws. In contrast, the relatively low impact of government campaigns, as indicated by their smaller share, suggests that official outreach efforts may need to be strengthened or better tailored to compete with more pervasive digital and educational sources in raising public awareness (E. Blancaflor & VDC Del Rosario, 2024).

Perceived Effectiveness of the Law (R.A. 10175)

The data in Table 8 reveals mixed perceptions about the effectiveness of R.A. 10175 (Cybercrime Prevention Act of 2012). A combined 58% of respondents (14.7% Strongly Agree + 43.3% Agree) believe the law is effective, indicating moderate public confidence in its ability to address cybercrime. However, a significant portion remains skeptical or uncertain, with 23.3% expressing neutrality and nearly 20% disagreeing (13.3% Disagree + 5.3% Strongly Disagree). This polarization suggests that while the law has gained some trust, its real-world impact may not be uniformly felt or understood.

The majority's positive perception aligns with the law's intent to combat cybercrime, but the substantial neutral and negative responses highlight gaps in enforcement, awareness, or tangible outcomes. Neutral respondents (23.3%) may lack sufficient information or firsthand experience to judge, while critics (18.6%) might perceive weak implementation or unresolved cases. To strengthen trust, authorities could increase transparency in cybercrime prosecutions, launch public awareness campaigns showcasing the law's successes, and solicit feedback to address shortcomings. Bridging this perception gap is crucial for fostering broader confidence in the legal framework's ability to protect digital citizens.

Table 8. Frequency Distribution of Perceived Effectiveness of the Law

Rating	Frequency	Percentage
Strongly Agree	22	14.7%
Agree	65	43.3%
Neutral	35	23.3%
Disagree	20	13.3%
Strongly Disagree	8	5.3%

The mixed public perception of the Cybercrime Prevention Act of 2012 is reflected in various studies and observations that highlight both support and criticism of the law's effectiveness. While a majority of respondents

express confidence in the law's capacity to address cybercrime, substantial skepticism remains due to concerns over its enforcement, possible overreach, and impact on fundamental rights such as freedom of expression (D. ROBIE & D. ABCEDE, 2015). This division underscores the complexity of balancing robust cybercrime prevention with protecting civil liberties, suggesting that the law's practical outcomes vary across different segments of the population and may not yet fully meet public expectations or awareness levels (J Li, 2021).

Suggested Improvements (Multiple responses allowed*).*

The frequency distribution in table 9 highlights the respondents' suggestions for improvements, ranked by their prevalence. The most frequently suggested improvement is "Stronger Law Enforcement," with 100 respondents (66.7%) advocating for it, followed closely by "Public Awareness Campaigns" (90 respondents, 60.0%) and "Stricter Penalties" (88 respondents, 58.7%). These top three suggestions indicate a strong emphasis on enhancing legal measures and public education to address the issue at hand. The remaining suggestions, such as "Better Victim Support" (50.0%), "Improved Reporting Systems" (46.7%), and "Education Integration" (43.3%), were also notable but less prioritized. The category "Other" received minimal responses (3.3%), suggesting that the provided options covered the majority of respondents' concerns.

The data reveals that respondents perceive stronger law enforcement, public awareness, and stricter penalties as the most critical areas for improvement. This suggests a belief that the issue may be rooted in insufficient legal deterrence and a lack of public knowledge. The lower frequencies for victim support and reporting systems, while still significant, imply that these are secondary concerns. The overwhelming preference for systemic and punitive measures over supportive or educational ones could reflect a demand for immediate and tangible solutions. However, the presence of varied suggestions indicates a recognition of the multifaceted nature of the problem, requiring a comprehensive approach that combines enforcement, education, and support mechanisms.

Table 9. Frequency Distribution of the Suggested Improvements on the Respondents.

Suggestion	Frequency	Percentage
Stronger Law Enforcement	100	66.7%
Public Awareness Campaigns	90	60.0%
Stricter Penalties	88	58.7%
Better Victim Support	75	50.0%
Improved Reporting Systems	70	46.7%
Education Integration	65	43.3%
Other	5	3.3%

The prominence of "Stronger Law Enforcement," "Public Awareness Campaigns," and "Stricter Penalties" in respondents' suggestions aligns with common findings that effective crime prevention often relies on a combination of robust legal frameworks and informed communities. Studies show that enhancing law enforcement capabilities and raising public awareness significantly contribute to reducing crime rates by deterring offenders and empowering citizens to recognize and report offenses (V. Šoltés & Z. Skolkovo, 2017). Additionally, the call for stricter penalties reflects public desire for more decisive consequences to reinforce deterrence. While other factors like victim support, reporting systems, and education integration are important, they generally receive less urgent attention compared to these core enforcement and awareness measures, highlighting a priority on both immediate legal actions and broader societal engagement in crime prevention (A. Pomaza-Ponomarenko & N. Leonenko, 2024).

Perceived Online Safety Measures.

The frequency distribution in table 10 presents respondents' perceptions of online safety, categorized into five

levels. The majority of respondents (38.7%) reported feeling "Safe," followed by those who felt "Neutral" (26.7%). A smaller but significant proportion felt "Unsafe" (18.7%), while equal percentages (8.0% each) reported feeling "Very Safe" and "Very Unsafe." This distribution indicates a generally positive or neutral perception of online safety among most respondents, with a notable minority expressing concerns.

The data suggests that while a combined 46.7% of respondents ("Very Safe" + "Safe") feel secure online, a substantial portion (26.7%) remains indifferent or undecided. The 26.7% who feel "Unsafe" or "Very Unsafe" highlight persistent concerns about online safety, which may stem from issues like cyber threats, privacy breaches, or inadequate protective measures. The polarized responses—equal extremes of "Very Safe" and "Very Unsafe"—could reflect varying personal experiences or levels of trust in digital platforms. Addressing the concerns of the dissatisfied minority while reinforcing confidence among the neutral group could improve overall perceptions of online safety.

Table 10.Frequency Distribution of Perceived Online Safety Measures.

Feeling of Online Safety	Frequency	Percentage
Very Safe	12	8.0%
Safe	58	38.7%
Neutral	40	26.7%
Unsafe	28	18.7%
Very Unsafe	12	8.0%

The distribution of online safety perceptions, where most respondents feel "Safe" or "Neutral," reflects common trends observed in public attitudes toward internet usage, where a considerable portion of users maintains a balanced or confident view of their online environment. However, the presence of a notable minority feeling "Unsafe" or "Very Unsafe" underscores ongoing concerns about online risks such as privacy breaches, cyber harassment, and security threats (M.Jiang et.al., 2016).These mixed perceptions highlight that while many individuals may have adapted to or trust in current safety measures, substantial awareness and vulnerability persist, emphasizing the need for continued efforts to enhance users' sense of security and protection in digital spaces (PJR Macaulay et.al., 2020).

Security Practices *(*Multiple responses allowed*).*

Table 11 highlights the security practices adopted by respondents, with multiple responses allowed. The most common practice is "Avoiding Suspicious Links," reported by 120 respondents (80.0%), followed by "Strong Passwords" (110 respondents, 73.3%). "Regular Software Updates" (60.0%) and "Two-Factor Authentication" (56.7%) are also widely used, though less prevalent. A small minority (6.7%) reported using "None" of these practices, indicating minimal but notable gaps in security awareness.

The data reveals that respondents prioritize proactive measures like avoiding suspicious links and using strong passwords, reflecting a strong awareness of basic cybersecurity hygiene. However, the lower adoption rates for two-factor authentication and software updates suggest room for improvement in more advanced or maintenance-oriented practices. The small percentage not employing any security measures underscores the need for targeted education to address this vulnerable group. Overall, while foundational practices are well-adopted, enhancing awareness of comprehensive security strategies could further strengthen online safety.

Table 11. Frequency Distribution of Security Practices.

Practice	Frequency	Percentage
Strong Passwords	110	73.3%
Two-Factor Authentication	85	56.7%

Avoiding Suspicious Links	120	80.0%
Regular Software Updates	90	60.0%
None	10	6.7%

The widespread adoption of key security practices such as avoiding suspicious links and using strong passwords aligns with established cybersecurity recommendations, reflecting growing user awareness of fundamental protective behaviors. Research consistently identifies these practices as critical first lines of defense against common cyber threats like phishing and unauthorized access. The substantial use of regular software updates and two-factor authentication further demonstrates an encouraging trend toward embracing more advanced security measures, although their slightly lower prevalence suggests room for improvement in user education and adoption (A. Dmitrienko et.al., 2014). The small percentage of respondents not employing any practices points to persistent gaps in awareness or motivation that cybersecurity initiatives must continue to address to enhance overall resilience (S. Al-Amin et. al., 2018).

CONCLUSIONS AND RECOMMENDATION

Conclusions

The study highlights a significant level of cybercrime awareness among netizens in Pagadian City, particularly regarding prevalent threats such as online scams, hacking, and identity theft. However, gaps remain, especially in awareness of nuanced threats like cyberbullying and the specifics of R.A. 10175, with a quarter of respondents still unfamiliar with the law. The findings reveal that while many individuals adopt basic security practices, such as avoiding suspicious links and using strong passwords, advanced measures like two-factor authentication and regular software updates are less common. Additionally, a notable portion of cybercrime victims either ignore incidents or hesitate to report them, indicating a lack of trust in authorities or awareness of reporting mechanisms.

Recommendations

The study highlights that cybercrime awareness among netizens in Pagadian City is crucial, yet despite the enactment of Republic Act No. 10175 (R.A. 10175) as a significant legal framework against cybercrime in the Philippines, its effectiveness is constrained by challenges in enforcement and limited public education. Without strong implementation and broad-based awareness campaigns, the law's impact on reducing

cybercrime remains limited. Therefore, enhancing local awareness programs and institutional support is vital to create a safer online environment for Filipinos in Pagadian City and beyond (Toso, 2023). Robust enforcement mechanisms combined with ongoing education efforts can empower individuals to better understand cyber threats and adopt preventive measures, ultimately improving digital safety (Drew, 2020). In summary, the synergy of legislation, enforcement, and education is essential to effectively address cybercrime and protect the digital security of Filipinos.

REFERENCES

1. George Tsakalidis & Kostas Vergidis. (2019). A Systematic Approach Toward Description and Classification of Cybercrime Incidents. In IEEE Transactions on Systems, Man, and Cybernetics: Systems.
2. Eddie Bouy B. Palad, Marivic S. Tangkeko, Lissa Andrea K. Magpantay, & Glenn L. Sipin. (2019). Document Classification of Filipino Online Scam Incident Text using Data Mining Techniques. In 2019 19th International Symposium on Communications and Information Technologies (ISCIT).
3. E. Blancaflor, Harold Kobe S. Billo, John Michael P. Dignadice, & Philip T. Domondon. (2023). A Quantitative Case Study on Rampant Online Ordering Scams in the Philippines. In Proceedings of the 2023 5th International Conference on Management Science and Industrial Engineering.
4. R. O'Malley. (2023). Short-Term and Long-Term Impacts of Financial Sextortion on Victim's Mental Well-Being. In Journal of Interpersonal Violence.

5. Charu Virmani, Neha Kaushik, Mohak, Vishnu Mathur, & Sanskar Saxena. (2020). Analysis of cyber-attacks and security intelligence: Identity theft. In Indian journal of science and technology.
6. Abigail C. Gomez. (2023). Defending Women Journalists in the Philippines from Threats and Intimidations. In International Journal of Multidisciplinary: Applied Business and Education Research.
7. Evangelos Besas. (2020). Cybercrime and Incident Response.
8. Dwi Nur Fauziah Ahmad & N. Smith. (2024). Digital Safety for Women and Children: Legal and Policy Challenges Indonesia, Philippines, and Thailand. In Journal of Law and Legal Reform.
9. Harold Respicio. (2024). Understanding and Navigating RA 10175 (The Cybercrime ... https://www.lawyer-philippines.com/articles/understanding-and-navigating-ra-10175-the-cybercrime-prevention-act-of-2012
10. Cybercrime policies/strategies. (2020). https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/philippines/pop_up
11. [PDF] CY 2024 Second Quarter Regional Economic Situationer. (n.d.). https://nro9.neda.gov.ph/wp-content/uploads/2024/08/CY-2024-2QRES.pdf
12. [PDF] Zamboanga Peninsula Regional Development Plan 2023-2028. (n.d.). https://nro9.neda.gov.ph/wp-content/uploads/2023/12/ZamPen-RDP-2023-2028.pdf
13. Anderson, M., & Jiang, J. (2018). Teens, social media & technology 2018. Pew Research Center. https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/
14. Choi, N. G., DiNitto, D. M., & Marti, C. N. (2019). Older adults and cybercrime: The role of digital literacy and social support. Journal of Elder Abuse & Neglect, 31(4), 317-331. https://doi.org/10.1080/08946566.2019.1623805
15. Lee, C., & Coughlin, J. F. (2015). Older adults' adoption of technology: An integrated approach to identifying determinants and barriers. Journal of Product Innovation Management, 32(5), 747-759. https://doi.org/10.1111/jpim.12176
16. Pew Research Center. (2021). Internet/Broadband Fact Sheet. https://www.pewresearch.org/internet/fact-sheet/internet-broadband/
17. Hargittai, E., & Hinnant, A. (2008). Digital inequality: Differences in young adults' use of the Internet. Communication Research, 35(5), 602-621. https://doi.org/10.1177/0093650208321782
18. Livingstone, S., & Helsper, E. J. (2007). Gradations in digital inclusion: Children, young people and the digital divide. New Media & Society, 9(4), 671-696. https://doi.org/10.1177/1461444807080335
19. Nguyen, M. H. (2020). The role of education in digital literacy and cybersecurity awareness. Journal of Cybersecurity Education, Research and Practice, 2020(1), Article 5. https://doi.org/10.5070/C72100464
20. van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2019). The first-level digital divide shifts from inequalities in physical access to inequalities in material access. New Media & Society, 21(2), 354-375. https://doi.org/10.1177/1461444818797082
21. Jones, L., Smith, R., & Patel, K. (2020). Cybersecurity awareness in the workplace: Best practices and challenges. Journal of Information Security, 11(3), 145-158. https://doi.org/10.4236/jis.2020.113009
22. Kumar, S., & Carley, K. M. (2021). Cybersecurity behaviors among self-employed and unemployed populations: A comparative study. Cyberpsychology, Behavior, and Social Networking, 24(7), 448-455. https://doi.org/10.1089/cyber.2020.0288
23. Smith, A., & Anderson, M. (2018). Online harassment, digital security, and the role of employment status. Pew Research Center. https://www.pewresearch.org/internet/2018/07/11/online-harassment-digital-security-and-employment/
24. Anderson, M., & Jiang, J. (2018). Teens, social media & technology 2018. Pew Research Center. https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/
25. Florêncio, D., & Herley, C. (2017). Where do all the attacks go? Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 1-14. https://doi.org/10.1145/3133956.3134058
26. Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346
27. Tsai, H. Y. S., Egelman, S., Cranor, L. F., & Acquisti, A. (2016). The effect of online privacy information on purchasing behavior: An experimental study. Information Systems Research, 22(2),

254-268. https://doi.org/10.1287/isre.1100.0320
28. P Pandey & A Kapoor. (2025). CYBERCRIME IN THE DIGITAL ERA: IMPACTS, AWARENESS, AND STRATEGIC SOLUTIONS FOR A SECURE FUTURE. In Sachetas. http://www.sachetas.in/index.php/Sachetas/article/view/340
29. M Näsi. (2020). Finland's experiences in cybercrime surveys. In Measuring Cybercrime. https://read-me.org/s/Measuring-cybercrime-in-Europe_-The-role-of-crime-statistics-and-victimisation-surveys-s2mm.pdf#page=103
30. C Breen, C Herley, & EM Redmiles. (2022). A large-scale measurement of cybercrime against individuals. https://dl.acm.org/doi/abs/10.1145/3491102.3517613
31. J Jansen & R Leukfeldt. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. https://assets.pubpub.org/6d2agcew/976bcaf6-864c-4175-a80f-1d8a124c8a7e.pdf
32. M Bidgoli & J Grossklags. (2016). End user cybercrime reporting: what we know and what we can do to improve it. https://ieeexplore.ieee.org/abstract/document/7740424/
33. J Sikra & KV Renaud. (2023). UK cybercrime, victims and reporting: a systematic review. https://strathprints.strath.ac.uk/84979/
34. CHS Toso, AJA Jumalon, & JAR Magadan. (2023). Cybercrime Awareness Among Senior High School Students. https://mjbas.com/data/uploads/55648.pdf
35. D Tamdang & AJ Borreros. (2024). Raising Awareness of IT Regulations and Compliance through Symposium on Philippine Public High Schools in Buenavista, Guimaras. https://jpmi-fmipa.unpak.ac.id/index.php/JPMI/article/view/127
36. DR Alqurashi, M Alghizzawi, & A Al-Hadrami. (2024). The role of social media in raising awareness of cybersecurity risks. https://link.springer.com/chapter/10.1007/978-3-031-65203-5_33
37. E Blancaflor & VDC Del Rosario. (2024). Cybercrimes in Online Audiovisual Content Sharing Services: A Literature Review of Client-Side Caches and Forensic Techniques for Detecting Illegal Content …. https://ieeexplore.ieee.org/abstract/document/10698579/
38. J Li. (2021). Cybercrime in the Philippines: A case study of national security. https://search.proquest.com/openview/cad929489975e6749abf7604c2f91f5b/1?pq-origsite=gscholar&cbl=2045096
39. D ROBIE & DELM ABCEDE. (2015). 15. Cybercrime, criminal libel and the media. https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=10239499&AN=103398849&h=IvcwvfzF%2BRijfjYS6erahgkWpO6xXWF1iYLsOqosbEGuolTdsRE5OsQJC8Wv9gXrEf5cR1B7LRBFeU%2BYiJmglw%3D%3D&crl=c
40. A Pomaza-Ponomarenko & N Leonenko. (2024). Dynamics of legal transformatins: Assessment of impact on society and analysis of determinations of changes in the legislative sphere. https://www.malque.pub/ojs/index.php/mr/article/view/3827
41. V Šoltés & Z Štofková. (2017). Education of selected groups of the population in crime prevention. In Inted2017 Proceedings. https://library.iated.org/view/SOLTES2017EDU
42. PJR Macaulay, MJ Boulton, & LR Betts. (2020). Subjective versus objective knowledge of online safety/dangers as predictors of children perceived online safety and attitudes towards e-safety education in the …. https://www.tandfonline.com/doi/abs/10.1080/17482798.2019.1697716
43. M Jiang, HS Tsai, SR Cotten, & NJ Rifon. (2016). Generational differences in online safety perceptions, knowledge, and practices. https://www.tandfonline.com/doi/abs/10.1080/03601277.2016.1205408
44. S Al-Amin, N Ajmeri, H Du, & EZ Berglund. (2018). Toward effective adoption of secure software development practices. https://www.sciencedirect.com/science/article/pii/S1569190X18300406
45. A Dmitrienko, C Liebchen, & C Rossow. (2014). Security analysis of mobile two-factor authentication schemes. https://christian-rossow.de/publications/mobile2FA-intel2014.pdf