

Impact of Campaigns of the Quezon City Police District Anti-Cybercrime Team Against Scams and Frauds

PSSg Fitz Patrick R. Bueno, RCrim

Master of Science in Criminology, PHINMA-St. Jude College Quezon City Inc., Murphy, Quezon City, Philippines

Publication history: Received: April 24, 2026; Revised: April 30, 2026; Accepted: May 7, 2026

Email of Corresponding Author: fira.bueno.rc@phinmaed.com

Abstract

This study evaluated the impact of the Quezon City Police District Anti-Cybercrime Team's campaigns against scams and fraud within the jurisdiction of Quezon City. Anchored on the conceptual link between social media awareness campaigns, public awareness, behavioral change, and cybercrime reduction, the study was further guided by Protection Motivation Theory and Empowerment Theory. A qualitative research design was used, supported by face-to-face interviews, documentary analysis, immersion, and thematic analysis. The respondents consisted of sixteen subjects identified from QCPD blotter records, including cases involving unjust vexation, cyber libel, online threats, middleman scams, Facebook hacking, identity theft, investment scams, vishing, phishing, text scams, online scams, recruitment scams, and employment scams. Findings revealed that cybercrime victimization was influenced by excessive social media use, limited digital literacy, blind trust in online information, age-related difficulty in using technology, and economic need. The QCPD Anti-Cybercrime Team's programs, including hotlines, Facebook-based updates, barangay visits, seminars, information campaigns, digital forensic support, volunteers, and inter-agency collaboration, were perceived as helpful in improving awareness, reporting, and public confidence. Records also showed a nearly 34 percent decrease in cybercrime cases, from 159 to 105 incidents, with a high case-resolution rate. However, challenges remained, including limited awareness, weak digital literacy, resistance to change, insufficient infrastructure, delayed response, data privacy concerns, and the need for stronger cooperation. The study concluded that cybercrime may be prevented, reduced, and controlled through sustained awareness, institutional capacity, public trust, and community participation. The study supports SDG 4, SDG 9, SDG 11, SDG 16, and SDG 17 by promoting digital education, safer communities, stronger institutions, and collaborative cybercrime prevention. Its sustainability impact lies in strengthening institutional, governance, digital, and community-based responses to online scams and fraud.

Keywords: Anti-Cybercrime Campaigns, Community Engagement, Cybercrime Prevention, Digital Literacy, Quezon City Police District, Scams and Fraud, Social Media Awareness

1. Introduction

The rapid expansion of digital technology and social media has transformed communication, education, governance, and public interaction. However, the same technological advancement has also created opportunities for cybercriminals to commit scams, fraud, identity theft, phishing, hacking, online threats, and other technology-assisted offenses. This study focuses on the impact of the Quezon City Police District Anti-Cybercrime Team's campaigns against scams and fraud, particularly in terms of public awareness, behavioral change, and the enhancement of strategies for cybercrime prevention within Quezon City.

Technology has become deeply embedded in Filipino society, influencing communication, information access, education, and public service delivery. Carreiro, S (2020) claims that technology begets sophistication, and this is reflected in the growing dependence of Filipinos on electronic devices, mobile communication, computers, and social media. While these developments have improved access to information and connectivity, they have also introduced more complex forms of criminal activity. Traditional offenses have increasingly shifted into digital spaces, giving rise to cybercrime and creating new challenges for law enforcement agencies. The Philippine National Police plays a major role in responding to these emerging threats. The creation of the Anti-Cybercrime Group and the operationalization of local anti-cybercrime teams reflect the government's response to technology-based criminality. In Quezon City, the Quezon City Police District Anti-Cybercrime Team was established to address online scams, online threats, identity theft, hacking, and related offenses. Its functions include cyber patrolling, monitoring cybercrime-related complaints, providing technical assistance, conducting awareness lectures, and promoting online safety among residents.

The related literature emphasizes that social media is both a tool for public communication and a venue for cybercrime. It allows people to connect, exchange information, and access public safety messages, but it also enables offenders to exploit users through scams, fraud, harassment, hacking, phishing, and identity-related crimes. In an era defined by digital connectivity, social media has become both a powerful tool and a breeding ground for illicit activities, making proactive public protection necessary, particularly in Quezon City. (Reyes, Camilo, et al). Social media awareness campaigns are presented as important instruments for cybercrime prevention because they help the public recognize warning signs, understand cyber threats, and adopt protective online behavior. The literature suggests that the effectiveness of such campaigns depends on clarity of message, relevance to the target audience, cultural and social appropriateness, sustained content delivery, and the ability to encourage actual behavioral change. Awareness is not limited to knowing that cybercrime exists; it also includes the capacity to identify scams, report suspicious activities, and practice safer online behavior. The literature also recognizes that social media can shape individual behavior and social attitudes. Marleya, M (2002) emphasized the influence of media in shaping society and culture, while Isler M. (2010) highlighted the role of social media in exposing and apprehending offenders. However, the same platform may also serve as an avenue for undesirable activities, showing the dual nature of social media as both a preventive and enabling environment for cybercrime. At the national level, the study is situated within the Philippine government's policy direction on technology, innovation, and cybercrime prevention. Article XIV, Section 10 of the Philippine Constitution emphasizes the role of science and technology in national development. Republic Act No. 10844, or the Department of Information and Communications Technology Act of 2015, promotes the use of ICT for good governance, competitiveness, and citizen-centered services. Republic Act No. 11293, or the Philippine Innovation Act, further supports the role of innovation and technology in productivity, development, and quality of life. Republic Act No. 10175, or the Cybercrime Prevention Act of 2012, provides the legal framework for defining, preventing, investigating, and prosecuting cybercrime in the Philippines. Locally, the Quezon City Police District Anti-Cybercrime Team addresses cybercrime incidents within the city through cyber patrolling, digital forensic support, public awareness lectures, and complaint monitoring. The study focuses on common cybercrimes reported within the Quezon City Police District, including vishing, phishing, online threats, online tasking or investment scams, cyber libel, Facebook hacking, Lalamove booking scams, middleman scams, unjust vexation, and identity theft. The study was conducted from December 2025 to February 2026. Globally, cybercrime is not limited to one locality or country. The study recognizes that the emergence of cybercrime is connected to broader technological progress and digital mobility. Since online scams and fraud operate through digital platforms that can cross geographic boundaries, local campaigns must be continuously improved and aligned with changing cybercrime tactics.

The study is anchored on a conceptual framework that links social media awareness campaigns with awareness level, behavioral change, and the reduction of scam and fraud incidents. The framework follows an input-process-output orientation. The inputs include campaign strategies against scams and fraud, the Quezon City Police District Anti-Cybercrime programs, and platform-related problems. The process involves measuring awareness through interviews and identifying factors associated with anti-cybercrime initiatives. The expected output is a proposed intervention program to enhance strategies or approaches to combat cybercrime in the area. The study also draws from Protection Motivation Theory, developed by Ronald Rogers in 1975, which explains how individuals adopt protective behaviors based on their appraisal of risk and their belief that they can implement effective protective measures. In this context, citizens are viewed as vulnerable to cyber threats, while the Quezon City Police District Anti-Cybercrime Team provides protective interventions through its cybercrime prevention programs. The study further uses Empowerment Theory by Julian Rappaport as a more fitting theoretical lens. This theory suggests that people become empowered when their specific problems are addressed and when they are provided with resources that help them make informed decisions. In the context of anti-cybercrime campaigns, empowerment involves identifying citizens' needs for protection against scams, enhancing self-efficacy in online safety, and promoting autonomy in managing personal cybersecurity.

Although the Quezon City Police District Anti-Cybercrime Team has implemented campaigns and programs against scams and fraud, there remains a need to evaluate how citizens perceive these efforts and how such campaigns affect public awareness and behavior. The study responds to this need by examining the common cybercrimes experienced by the subjects, the programs undertaken by the QCPD Anti-Cybercrime Team, the perceived impact of awareness campaigns, the problems encountered in relation to these programs, and the intervention program that may be proposed to enhance cybercrime prevention strategies. The rationale of the study lies in its practical value to the Quezon City Police District, Quezon City residents, policymakers, the Philippine National Police, social media users, researchers, and the wider Filipino community. The study provides a feedback mechanism for improving campaign strategies, strengthening public protection, increasing vigilance among residents, supporting policy formulation, and contributing to literature on cybercrime prevention. Since almost 73.6% Filipinos are generally hooked up with social media and are fanatics of social media activities, (Nicanor, Edilberto, 2022), the need for awareness and responsible online behavior becomes more significant.

The study is aligned with SDG 4 – Quality Education because it emphasizes public awareness, information dissemination, and educational campaigns that help citizens understand cybercrime risks and adopt safer online practices. It also supports SDG 9 – Industry, Innovation and Infrastructure by addressing the responsible and secure use of digital technology, ICT

systems, and online platforms in a society increasingly shaped by technological innovation. The study is strongly connected to SDG 11 – Sustainable Cities and Communities because it focuses on improving safety, protection, and public vigilance within Quezon City. It also aligns with SDG 16 – Peace, Justice, and Strong Institutions because it evaluates law enforcement campaigns, public trust, crime prevention, and the role of institutional strategies in protecting citizens from scams and fraud. Finally, it supports SDG 17 – Partnerships for the Goals because cybercrime prevention requires cooperation among police units, barangays, government agencies, social media users, and the wider community.

This study contributes to multidisciplinary sustainability by linking criminology, public administration, technology, communication, education, governance, and community safety. From a public safety and governance perspective, it supports stronger institutional responses to cybercrime and provides a basis for improving policies, manuals, procedures, and future anti-cybercrime initiatives. From an educational sustainability perspective, it emphasizes awareness-building and citizen education as tools for prevention. From a technological and digital sustainability perspective, the study promotes safer and more responsible use of social media and online platforms. From a socio-economic sustainability perspective, it addresses scams and fraud that may harm individuals' financial security, privacy, reputation, and well-being. From a community sustainability perspective, the study supports the development of vigilant, informed, and protected citizens who can recognize cybercrime risks and participate in maintaining a safer digital environment.

2. Material and methods

2.1 Research Design

The study employed a qualitative research design intended to produce a detailed description and interpretation of the respondents' experiences rather than to generate predictions or causal explanations. The design allowed the researcher to contextualize and interpret the gathered data based on existing norms and observed realities. Documentary analysis was also used by examining previous records, claims, and research findings related to cybercrime. A thematic approach was applied to organize the cases according to subjects or emerging themes.

2.2 Locale of the Study

The study was conducted within the jurisdiction of the Quezon City Police District, particularly in areas covered by its police stations and barangays. The identified areas included La Loma, Masambong, Talipapa, Novaliches, Fairview, Batasan, Cubao, Project 4, Anonas, Kamuning, Galas, Eastwood, Bagong Silangan, Holy Spirit, Project 6, and Pasong Putik. These areas served as the source of respondents and reported cybercrime cases relevant to the study.

2.3 Respondents of the Study

The respondents consisted of sixteen subjects identified from blotter records presented to the researcher by the Quezon City Police District. The respondents represented different barangays and stations under the district and had reported or experienced cybercrime-related incidents. PNP personnel directly involved in the Anti-Cybercrime Team were also considered because of their role in evaluating and responding to cybercrime concerns. The respondent cases included unjust vexation, cyber libel, online threat, middleman scam, Facebook hacking, identity theft, investment scam, vishing, online scam, text scam, phishing, recruitment scam, and employment scam.

2.4 Sample and Sampling Procedure

The study considered sixteen primary subjects selected from blotter records provided by the Quezon City Police District. In compliance with The Data Privacy Act of 2012 (Republic Act No. 10173), personal information was not disclosed, and only details relevant to the study were extracted from the records. The community respondents were selected using both probability and non-probability sampling to reduce bias, although priority was given to individuals who had reported cases with the Quezon City Police District because they had direct experience and firsthand information related to the study.

2.5 Research Instrument

The main instrument used in the study was a structured set of open-ended questions for face-to-face interviews. The questions focused on the common cybercrimes experienced by the subjects, the programs undertaken by the Quezon City Police District Anti-Cybercrime Team, the perceived impact of awareness campaigns against scams and fraud, and the problems encountered by the subjects in relation to these campaigns. An unstructured questionnaire was also used to validate responses and allow additional information to emerge during the interview. The instrument was developed from operational manuals, police station reports, client responses, and the identified research problems. It was reviewed by experts, revised to remove undesirable statements, and validated through policemen from a random police station who were not members of the Quezon City Police District Anti-Cybercrime Team. Their comments and difficulties were used to improve clarity, openness, and neutrality of the questions.

2.6 Data Gathering Procedure

Data were gathered through behavior-based face-to-face interviews, documentary analysis, and immersion. The interviews used structured open-ended questions to obtain firsthand information from the subjects. Documentary analysis was conducted by reviewing available cybercrime-related resources from police stations, particularly blotter records and classified records accessed with permission from higher authorities. Immersion was also used, as the researcher personally engaged with selected cybercrime-related experiences with caution to better understand the physical, psychological, and emotional setbacks experienced by victims. The researcher's membership in the Quezon City Police District team facilitated access to the study setting.

2.7 Data Analysis Techniques

The gathered data were analyzed qualitatively through thematic organization and documentary comparison. Interview responses were categorized into themes based on the study problems, while documentary data from blotter records and related sources were used to support and validate the narratives. The study also used triangulation by comparing the respondents' accounts with available records and published or documented cybercrime-related information. This process strengthened the validity and reliability of the qualitative findings.

2.8 Ethical Considerations

The study was guided by RA 10173, or the Data Privacy Act, which protects personal information in both government and private sectors. Respondents were assured that their responses would be treated with the highest confidentiality. The study considered informed consent, confidentiality and anonymity, protection of vulnerable scam victims from possible re-traumatization, secure handling of sensitive data, the possible impact of the study on QCPD operations or reputation, and proper collaboration with QCPD for approval of the research steps undertaken.

3. Results and Discussion

3.1 Common Cybercrimes within the Quezon City Police District

3.1.1 Types of Cybercrime Experienced by the Subjects

The findings showed that the subjects experienced different forms of cybercrime, including unjust vexation, cyber libel, online threat, middleman scam, Facebook hacking, identity theft, investment scam, vishing, phishing, text scam, online scam, recruitment scam, and employment scam. These incidents involved reputational harm through social media, fraudulent job offers, unauthorized use of personal information, financial deception, and manipulation through online platforms. The reported cases reflected how cybercrime has entered ordinary community life and affected residents across different ages, occupations, and social backgrounds. The findings suggest that cybercrime in Quezon City is not limited to one form of online offense but covers both personal and financial violations. The cases also show that digital platforms have become common instruments for deception, harassment, and exploitation. This supports the view that modern criminality has shifted from purely physical spaces to digital environments, making cybercrime prevention a necessary component of community safety and law enforcement practice.

3.1.2 Factors Contributing to Cybercrime Victimization

The results revealed that vulnerability to cybercrime was associated with excessive social media use, limited digital literacy, blind trust in online information, age-related difficulty in using technology, and economic need. Some respondents admitted that their strong engagement with social media exposed them to risks, while others became victims because they lacked sufficient knowledge of online safety or were persuaded by promises of income, employment, investment, or financial benefit. These findings indicate that cybercrime victimization is shaped by both technological and human factors. Human vulnerability especially to internet is very high (Agpalso 2019), particularly when users lack awareness, digital skills, or caution in dealing with online offers. Economic status was also found to have a strong bearing on victimization, as records showed that many victims came from low-income groups or those without stable employment. This supports the study of Avance, (2018) on the Economic Factors Related to Cybercrime, which connects economic condition with susceptibility to online schemes.

3.1.3 Trust in the QCPD Anti-Cybercrime Team

The findings showed that respondents generally expressed trust and appreciation for the Quezon City Police District Anti-Cybercrime Team. Several participants viewed the team as responsive, helpful, and accessible, especially when cybercrime incidents were reported. Some victims relied on the team for resolution because they lacked the financial capacity or willingness to pursue court action. This result implies that the QCPD Anti-Cybercrime Team serves not only as an enforcement unit but also as a practical support mechanism for victims. The respondents' confidence in the team reflects the importance of accessible police assistance in cybercrime cases. It also suggests that community trust can strengthen reporting behavior, encourage cooperation, and support the broader goal of cybercrime prevention.

3.2 Programs Undertaken by the QCPD Anti-Cybercrime Team

3.2.1 Community Engagement and Public Access

The results showed that the QCPD Anti-Cybercrime Team implemented programs focused on public access, community engagement, and immediate reporting. Respondents identified the establishment of offices, availability of hotlines, use of Facebook pages, barangay visits, seminars, and information campaigns as helpful measures. These programs gave residents a direct channel for assistance, reporting, and continuous updates on cybercrime prevention. These findings show that cybercrime campaigns become more effective when they are visible, accessible, and community-based. The presence of offices, hotlines, and online platforms helped reduce the gap between law enforcement and residents. The use of Facebook also strengthened communication because it allowed the QCPD Anti-Cybercrime Team to provide reminders, updates, and educational content in a platform already familiar to many citizens.

3.2.2 Institutional Capacity and Collaboration

The findings further revealed that the QCPD strengthened its cybercrime response through the creation of the Anti-Cybercrime Team, the provision of digital forensic equipment, continuous training, the mobilization of more than 400 volunteers, and collaboration with other government agencies. The team also adopted Information, Education and Communication activities through seminars, flyers, brochures, and social media-based information dissemination. The results suggest that cybercrime prevention requires both institutional capacity and multi-agency cooperation. Since cybercrime is technology-driven, law enforcement personnel need updated equipment, training, and technical competence. Collaboration with other agencies also strengthens response capability by expanding resources, technical support, and coordination in handling complex cybercrime incidents.

3.3 Impact of Awareness Campaigns against Scams and Fraud

3.3.1 Reduction of Cybercrime Cases

The results indicated that the QCPD anti-cybercrime programs contributed to the reduction of cybercrime cases in Quezon City. Records showed a nearly 34 percent decrease in cybercrime cases, from 159 incidents in July to 105 incidents in August. Police also resolved 146 cases or 92.38 percent of reported cases in August, while the previous month recorded a 91.82 percent resolution rate. The QCPD also reported a general decline in crime volume in the city, from 1,350 to 1,060 cases. These findings suggest that the awareness campaigns and operational strategies of the QCPD Anti-Cybercrime Team had a positive effect on cybercrime prevention and response. The decline in reported cases and the high resolution rate indicate that public awareness, reporting mechanisms, and police intervention may help reduce cybercrime exposure. However, the findings also imply that continued reinforcement is necessary because cybercrime remains persistent and constantly evolving.

3.3.2 Community Awareness, Confidence, and Participation

The findings showed that respondents perceived the cybercrime programs as beneficial to the community. Participants reported that people gradually learned from the campaigns, became more aware of cyber threats, and gained confidence in the presence of anti-cybercrime programs. Parents also expressed reduced fear regarding their children's exposure to social media because of the existence of police-led cybercrime initiatives. These results show that the impact of the campaigns extends beyond crime reduction. The campaigns also helped build community confidence, encourage cooperation, and promote safer online behavior. The findings suggest that the success of cybercrime prevention depends not only on police operations but also on the willingness of residents, barangays, and stakeholders to learn, listen, cooperate, and support the program.

3.4 Challenges Encountered in Awareness Campaigns and Program Implementation

3.4.1 Public Awareness, Digital Literacy, and Resistance to Change

The findings revealed that limited awareness, weak understanding of cyber threats, resistance to change, and low digital literacy remained major challenges. Some respondents noted that many residents still refused to listen or cooperate, while older residents had difficulty understanding internet-based programs and digital safety messages. These conditions made some residents more vulnerable to scams, fraud, and online manipulation. This finding implies that cybercrime campaigns must be simplified, repeated, and tailored to different age groups and levels of digital literacy. Awareness campaigns cannot rely only on online communication because not all residents are comfortable with digital platforms. The result also shows the need for community-level education that is practical, understandable, and accessible to both younger and older citizens.

3.4.2 Infrastructure, Response Time, and Technological Limitations

The results showed that insufficient infrastructure, limited equipment, poor internet access, and delayed response affected the implementation of anti-cybercrime programs. Some respondents noted that not all households or barangays had reliable internet access, which slowed reporting and communication. The QCPD also faced limitations in facilities, equipment, manpower, and resources needed to respond quickly to cybercrime reports. These findings indicate that cybercrime prevention depends heavily on technological readiness and institutional resources. Since cybercriminals often use advanced tools and emerging technologies, law enforcement must be equipped with modern systems, updated equipment, and adequate personnel. Without sufficient infrastructure, even well-designed awareness programs may face delays and operational limitations.

3.4.3 Trust, Data Privacy, and Inter-Agency Cooperation

The findings also identified lack of trust in digital systems, data privacy concerns, sophisticated cyber threats, and limited cooperation among agencies as continuing challenges. Some residents hesitated to use digital technologies because of fear of losing money or personal information. The study also noted that emerging technologies, including AI, may allow perpetrators to attack with greater speed and precision. These results suggest that cybercrime prevention requires a balance between public education, institutional trust, data protection, and coordinated enforcement. Data privacy concerns must be properly addressed so that residents will feel safe in reporting incidents. At the same time, stronger cooperation among government agencies, law enforcement units, private organizations, and community stakeholders is necessary to respond to increasingly sophisticated cyber threats.

3.5 Proposed Intervention Program

3.5.1 Strengthening Awareness, Reporting, and Community Engagement

The proposed intervention focused on enhancing public awareness, improving reporting and response mechanisms, strengthening collaboration, and developing community participation in cybercrime prevention. The proposed strategies included awareness campaigns for residents and businesses, workshops, online campaigns, integration of cyber safety in schools, an online reporting portal, and the formation of a cybercrime prevention committee at the barangay or community level. The proposed intervention is consistent with the identified findings because the major challenges involved awareness gaps, delayed reporting, weak digital literacy, and limited community cooperation. By strengthening education, reporting systems, and community-based committees, the intervention can make cybercrime prevention more participatory and responsive. It also supports the study's goal of improving current strategies and further reducing cybercrime beyond the reported 34 percent decline.

3.5.2 Capacity Building, Partnerships, and Sustainability

The proposed program also emphasized capacity building for law enforcement and government agencies, partnership with international organizations, knowledge sharing, and adoption of best practices. The implementation plan included needs assessment, development of awareness materials, launching of reporting mechanisms, establishment of cybercrime committees, community meetings, evaluation of program effectiveness, and sustainability planning. The estimated budget ranged from 500,000.00 to 800,000.00, with potential partners from government agencies, the private sector, international organizations, barangays, community organizations, schools, students, and business sectors. This intervention highlights that cybercrime prevention must be sustained through institutional capacity, adequate resources, and stakeholder collaboration. The expected outcomes include increased awareness, improved reporting of cybercrime incidents, better investigation and response, enhanced collaboration, and stronger community pride among stakeholders. Overall, the proposed program provides a practical direction for reinforcing QCPD's existing anti-cybercrime efforts and building a more informed, protected, and cooperative community.

4. Conclusion & Recommendations

The study concluded that cybercrime is not only a concern within Quezon City but also part of a wider national and international problem brought by technological progress. Although technological advancement cannot be stopped, cybercrime may be prevented, reduced, and controlled through effective anti-cybercrime programs. The findings showed that the Quezon City Police District Anti-Cybercrime Team has contributed to cybercrime prevention through its campaigns, programs, public awareness efforts, and continued community engagement. Citizens recognized that the efficiency of these programs supports progress toward a safer and more protected community, especially when the police and the public work cooperatively toward the same goal.

The study recommends strengthening police training and capacity building through regular workshops on cybercrime investigation, digital forensics, and cybersecurity; improving infrastructure and resources by equipping the Quezon City Police District with modern tools that can match the capabilities of perpetrators; increasing public awareness and education on cyber safety, online threats, and reporting procedures; establishing a dedicated cybercrime unit; orienting incoming trainees and PNP personnel on cybercrime concerns; empowering the community through initiatives such as "Be Wais"; enhancing collaboration with government agencies, private entities, and organizations; building public trust through partnerships with credible institutions; and using targeted campaigns focused on common scams such as online shopping scams, fake deliveries, and impersonation.

The study was limited to the impact of the social media awareness campaign of the Quezon City Police District Anti-Cybercrime Team against scams and fraud within the Quezon City Police District. It covered only the cybercrime cases provided by the Quezon City Police District and those experiences that subjects were willing to disclose. The study focused on common reported cybercrimes such as vishing, phishing, online threats, online tasking or investment scam, cyber libel, Facebook hacking, Lalamove booking, middleman scam, unjust vexation, and identity theft, and was conducted from December 2025 to February 2026.

Compliance with ethical standards

The study was conducted in accordance with institutional ethical standards, with voluntary participation, informed consent, and confidentiality of all information observed throughout the research process. Ethical approval was secured when applicable, and the authors declare no conflict of interest. All contributors were properly acknowledged, authorship responsibilities were observed, and copyright ownership and other relevant ethical considerations were respected.

REFERENCES

- Ariola, B. P., Laure, E. R. F. O., Perol, M. L. A., & Talines, P. J. T. (2018). Cybercrime awareness and perception among students of Saint Michael College of Caraga, Agusan del Norte. *SMCC Higher Education Research Journal (Criminal Justice)*, 1(1). <https://doi.org/10.18868/cje.01.060119.03>
- Balita, C. (2023, December 21). *Cybersecurity and cybercrime in the Philippines: Statistics & facts*. Statista. <https://www.statista.com/topics/11332/cybersecurity-and-crime-in-the-philippines/>
- Calupit, P. A. (2025). Exploring the PNP Regional Anti-Cybercrime Unit 5 capability on cybercrime challenges: An empirical analysis. *International Journal for Multidisciplinary Research*, 7(3). <https://www.ijfmr.com/papers/2025/3/43827.pdf>
- Concoles, C. R., Cristobal, N., Felonia, E., Jr., Tadtad, V. M., Villafuerte, K. A., & Lucas, T. V. D. (2024). Cybercrime awareness and cybercrime prevention attitude of criminology students. *Journal of Criminal Justice Studies*. https://cmc.edu.ph/images/files/research/1741921703_manuscript.pdf
- Danganan, M. J., & Maligalig, R. (2021). *Police involvement in the cybercrime investigation*. Manuel S. Enverga University Foundation Research. <https://mseuf.edu.ph/research/read/1513>
- De Ramos, N. M., & Esponilla, F. D., II. (2022). Cybersecurity program for Philippine higher education institutions: A multiple-case study. *International Journal of Evaluation and Research in Education*, 11(3), 1198–1209. <https://doi.org/10.11591/ijere.v11i3.22863>
- Drew, J. M. (2020). A study of cybercrime victimisation and prevention: Exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, 6(1), 17–33. <https://doi.org/10.1108/JCRPP-12-2019-0070>
- Fajardo, M. B., Abragon, M. N., Abuan, L. L., Hinlayagan, J. M., Marmol, D. J., Contreras, A. B., Basbas, R., Jr., & Villa, E. B. (2025). Challenges faced by PNP in resolving cybercrime cases. *International Journal of Multidisciplinary: Applied Business and Education Research*, 6(3). <https://doi.org/10.11594/ijmaber.06.03.23>
- Li, J. (2021). Cybercrime in the Philippines: A case study of national security. *Turkish Journal of Computer and Mathematics Education*, 12(11), 4224–4231. <https://turcomat.org/index.php/turkbilmat/article/view/6550>
- Mahinay, C. J. D., & Mamasalagat, M. P. (2025). Assessing cybercrime awareness and experiences among netizen: A study on the impact of R.A. 10175 in Pagadian City. *International Journal of Research and Innovation in Social Science*, 9(5), 2786–2802. <https://doi.org/10.47772/IJRIS.2025.905000216>
- Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International Journal of Research in Business and Social Science*, 11(4), 384–396. <https://doi.org/10.20525/ijrbs.v11i4.1714>
- Ngo, E. (2020). *Social media: The unseen risks of cybercrimes* [Honors thesis, Anna Maria College]. <https://annamaria.edu/wp-content/uploads/2021/06/Emily-Ngo-Fall-2020.pdf>
- Pamularco, G., & Zarseulo, R. (2021). *Study on various approaches in detecting cybercrime in the Philippines*. Manuel S. Enverga University Foundation Research. <https://mseuf.edu.ph/research/read/1449>
- Pasinhon, L. G., & 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*, 3(2), 31–44. <https://www.apjaet.com/wp-content/uploads/2024/06/CAPABI1.pdf>
- Pouani Tientcheu, P. (2021). *Security awareness strategies used in the prevention of cybercrimes* [Doctoral dissertation, Walden University]. Walden Dissertations and Doctoral Studies. <https://scholarworks.waldenu.edu/dissertations/11019/>
- Rosales, M. A., Magsumbol, J. V., Palconit, M. G. B., Culaba, A. B., & Dadios, E. P. (2020). Artificial intelligence: The technology adoption and impact in the Philippines. *2020 IEEE 12th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)*. <https://doi.org/10.1109/HNICEM51456.2020.9400025>
- Suminig, A., Jr., Abante, M. V., & Vigonte, F. G. (2025). *Safeguarding cyberspace: A comprehensive analysis of the Cybercrime Prevention Act of 2012 (RA 10175) and its role in Philippine digital governance*. SSRN. <https://doi.org/10.2139/ssrn.5270089>
- UNICEF Philippines. (2022, February 9). *Philippines sees increase in cyber tip reports in 2021; UNICEF calls for collective action on Safer Internet Day*. UNICEF. <https://www.unicef.org/philippines/press-releases/philippines-sees-increase-cyber-tip-reports-2021-unicef-calls-collective-action>
- Wu, L., Peng, Q., & Lembke, M. (2023). Research trends in cybercrime and cybersecurity: A review based on Web of Science Core Collection Database. *International Journal of Cybersecurity Intelligence and Cybercrime*, 6(1), 5–28. <https://doi.org/10.52306/OZMB2721>