International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Cybercrime Prevention Initiatives Among the Pnp's Affecting Public Trust and Collaboration of the Community

Daniel Allan a Pasia

Emilio Aguinaldo College
Manila, Philippines

ABSTRACT

This study examined the assessment of public trust and collaboration between the Philippine National Police Anti-Cybercrime Group (PNP-ACG) and community stakeholders in relation to the implementation of cybercrime prevention initiatives. It aimed to determine the respondents' demographic profile, evaluate their perceptions on trust and collaboration, identify their assessments of the PNP's cybercrime programs, and analyze differences across socio-demographic variables. The study also investigated the correlation between public trust components and the effectiveness of cybercrime prevention efforts.

Employing a descriptive-correlational research design, the study involved 120 respondents composed of police personnel and community residents. Quantitative data were gathered through a validated survey instrument measuring four dimensions of public trust (mutual trust, open dialogue, shared responsibility, and transparent processes) and four components of cybercrime prevention initiatives (online safety awareness, cybercrime reporting, victim support, and community-led digital literacy programs). Statistical tools including t-test, ANOVA, and Pearson correlation were used to analyze the data.

Findings revealed that respondents generally agreed that public trust and collaboration with the PNP-ACG are evident, particularly in the areas of mutual trust and open dialogue. Likewise, cybercrime prevention initiatives were positively perceived, especially in terms of victim support and online safety awareness. However, shared responsibility and community-led digital literacy efforts received comparatively lower ratings, highlighting areas for enhancement. Significant differences were found based on group affiliation, sex, age, and educational attainment, reflecting varied perceptions across demographic sectors. Notably, a strong positive correlation was observed between mutual trust and online safety awareness ($r = .860$, $p = .000$), while other correlations between trust and program effectiveness were either weak or non-significant.

The study concludes that while foundational trust and public engagement are evident, strategic alignment between institutional trust-building and cybercrime program delivery remains fragmented. It recommends strengthening community-based digital literacy, improving reporting accessibility,

institutionalizing trauma-informed victim support, and developing an integrated public trust-cybercrime strategy to ensure a more participatory, inclusive, and sustainable digital security framework.

Keywords: PNP's cybercrime prevention and trust initiatives.

INTRODUCTION

Crime is an action that against in any prohibitory rules or law that is considered as an offense, which has legitimate sanctions for violating it (University of Glasglow, 2019). It can be done by violating the rights of an individual or by stealing or destroying their properties. Also, crime can be done by crime pattern or modus operandi.

There are different ways in committing crime which is known as modus operandi. This is a recognizing characteristic or behavioral pattern that we use to classify somebody through the way they commit a crime. It's how investigators begin the luminary process of narrowing down the field of probable suspects based on whether or not the facts of the crime suit their "modus operandi". It is also important to realize that aspects of an MO can change over time. Yet, the fundamental natures of a consistent method usually remain the same; therefore, they are an excellent gauge of whether a suspect might be connected (University of Manchester, 2022).

In modern days, the offenders adopted technology to conveniently commit misconduct. With the technology innovations there are devices and systems that help us to easily access different information that is known as digital technology. Digital technologies are a various range of tools, systems, and devices that use digital information and processes to improve several activities (BAJ, 2023).

According to Wu, L., Peng Q., and Lemke, M. (2023) cybercrime is the popular term that encompasses a range of criminal activities that happened with the help of internet or within a computer system to exploit vulnerabilities in complex information system or infrastructure. Most of cybercriminals practice cybercrimes to produce profit, some cybercrimes are carried out against computers or devices to directly damage or disable them. Others use computers or networks to spread malware, illegal information, images or other materials. Some cybercrimes do both, like target computers to infect them with a computer virus, which is then spread to other machines and, sometimes, entire networks (Brush, K., & Cobb M., 2024). In today's generation, almost all have access to the internet and smartphones. According to Kemp (2023), internet users in the Philippines rose to 85.16 million as of January 2023, wherein 84.45 million use social media platforms, equating to 72.5% of the total population. In addition, he stated that the total number of cellular mobile connections active in the Philippines is 168.3 million as of early 2023. With that being said, Filipinos are overexposed on technology advancement. They can even become victims or those who took advantage of advanced technology, committing nefarious acts against each other. In connection to that, de Santos (2023) stated that according to PNP Chief Rodolfo Azurin Jr., cybercrime is the greatest threat that Filipinos will face. Also, the PNP will focus more on cybercrimes as it was said to be one of the fastest-growing transnational crimes by PNP Chief Azurin Jr.

In the Philippines one of the primary agency responsible in preventing and suppressing cybercrime is the Philippine National Police. Cybercrime cases increase by 21.84 percent in the first quarter of 2024, according to the police Anti-Cybercrime Group (ACG). The Anti-Cybercrime Group recorded 4,469 cases of cybercrime from the first quarter of 2024 compared to 3,668 reported cases in 2023. According to ACG director Maj. Gen. Sidney Hernia The top three crimes that contributed to the

spike were online selling scams at 990 cases, debit and credit card fraud at 309 and investment scams at 319. The possible caused of the rise of cybercrimes activity are increased online activity, sophisticated cybercrime tactics and the public's lack of awareness, The growing reliance on online platforms for shopping, financial transactions and investment opportunities has paved way for a larger pool of possible targets for cybercriminals, Hernia noted (Tupas, E., 2024).

Misusing ICT can result in illegal acts against the law and cybercrime. Cybercrime has become a significant threat to the security and privacy of internet and technology users. Cybercrime is any illegal activity conducted via computer network, system, or internet (Chounlamountry, 2023). It has become a worldwide transnational crime affecting almost all countries around the globe. Cyberattacks have increased since the coronavirus outbreak due to people's dependency on technology.

Also, Lalu (2023) mentioned that according to the Cybercrime Investigation and Coordination Center (CICC), the latest data released during the Joint Anti-Bank Robbery and Cybercrime Coordinating Committee Second Quarter Meeting for 2023 held in Taguig City showed that 6,250 cases of cybercrime were recorded from January to June 2023. The CICC also noted that online scams almost tripled to 4,446, from 1,551 reported in the first half of 2022. With that, the Republic Act No. 10175, also known as the Cybercrime Prevention Act of 2012, took action against those apprehended.

As stated by the Official Gazette (2012), Republic Act No. 10175, "Cybercrime Prevention Act of 2012," aims to protect and safeguard the integrity. of computers, computer and communications systems, networks, and databases and the confidentiality, integrity, and availability of information and data stored therein from all forms of misuse, abuse, and illegal access by making such conduct or conducts punishable under the law.

However, using the internet was not the only thing included in cybercrime. It also consists of those that took advantage of technology, such as text messages, calls, and emails that contain a message used for fraudulent schemes. With digital technology dominating the market, those who have evil intent also step up their game and start spreading fraudulent schemes using cellular phones, especially with the use of SIM. The majority of SMS falls into the category of scam or fraud, defined as a campaign to entice the recipient into taking some action that unwittingly results in information disclosure or financial loss. In a TransUnion-commissioned consumer survey across 18 countries and regions globally, 52% of respondents indicated that they were targeted by digital fraud via email, online, phone call, or text messaging in the three months beginning September 2022.

Among Filipinos surveyed, 71% said they were targeted by digital fraud attempts across these communications channels, and 11% among all surveyed fell victim over this period. Phishing (fraudulent emails, social posts, websites, and QR codes) and smishing (fraudulent mobile text messages), both at 46%, were the most commonly reported fraud schemes experienced by Filipinos, followed by third-party seller scams at 33% and identity theft at 25%, (TransUnion, 2023).

The Philippines was also found to be one of the most susceptible countries in Southeast Asia to cyber threats. From 2004, it is estimated that some 124 million accounts in the country have been compromised, ranking second in the region. High numbers of compromised accounts put significant risks at risk, such5 as identity theft and extortion. (BUSINESS.INQUIRER, 2024)

The Philippine National Police Anti Cybercrime Group is responsible to implement, enforce and investigate the all-major cybercrime laws and other cyber related crimes (Cyber Security Intelligence, 2025). In the CALABARZON region (Region IV-A), which includes the provinces of Cavite, Laguna, Batangas, Rizal, and Quezon, the PNP has been proactive in addressing cybercrime. As of July 2023, the

PNP has trained 52 police officers from CALABARZON in cybercrime investigation, with plans to train additional personnel from other regions within the year. (Philstar, 2024)

The Philippine government has responded to the increasing threat of cybercrime by formulating the National Cyber Security Plan (NCSP) 2023-2028. This is a multi-faceted approach, which involves the private sector, government, and international partnerships to enhance the country's cybersecurity posture. The NCSP aims to secure the nation's cyberspace and promote a culture of cybersecurity resilience and awareness (Luna, 2024). The NCSP focuses on three major outcomes proactive protection and security in cyberspace, increase cyber security workforce capabilities, and strengthened cyber security policy framework (Digwatch,2024).

According to Hagan (2021) Crimes is an act that defies the societal moral values through an act that violates legal norms. Also, he highlights that the criminality is socially constructed which means it was set by the society to determine the wrongdoings with the action in one area may be considered a crime but, in some areas, it can be considered legal. The idea of deviance is frequently linked to crime. According to White and Haines (2021) deviance is behaviors that disrupts social norms, while crime is the nonconformity of codified law.

Crime is an act strongly disapproved by society. Crime includes murder, fraud, rape, etc. Each society has its own perception about crime. For commission of crime, there should be a criminal intent and a criminal action. No one is a born criminal; the criminal intent and behaviors of an individual are outcome of various social, economic, biological and psychological roots (Thotakura, S., 2011).

To sum up crime is an act that violates the social standards that shaped by legal, cultural and social forces. Committing actions that violates the formal written rules and regulation is considered as lawbreaking.

The growth of cybercrime has remarkable concern in the digital age, that’s affecting the nation, organization and individuals. Cybercrime is a rising threat concerning networked technologies, affecting various circumstances. It's repeatedly perceived as a challenge to Cybersecurity, emphasize the need for improved engagement and ideas exchange (Chaurasia &Thakur, 2024). Cybercrime is activities that carried out through the use of computers or the internet.

According to Deora and Chudasama (2021) cybercrime is a serious challenge to the society that may harm individuals by being the target of their activities like phishing scams, online harassment, identity theft, malware, hacking, ect., which used computer as a tool or a target in the commission of the crime. In addition, cybercrime is a current and deteriorating problem all over the world. Numerous types of cybercrimes such as hacking, identity theft, harassment, and various forms of financial fraud are rampant. Further, although cybercrimes using information and communication technology (ICT) are extensive, effective measures and legislation to prevent or cope with them are in short supply. These circumstances warrant an analysis from a criminal's perspective of the reasons and methods for committing cybercrimes. Additionally, cybercrime has impacts in businesses, that focuses on economic consequences. The businesses especially the small and medium enterprises, encountered significant economic losses because of cyberattacks (Baker & Green 2020).

According to Keller, R., Moore, J., & Tanish, S. (2021) during pandemic the world shifted to work from home basis that paved the increase on the reliance on digital communication, that the cybercriminals adapted. Morever, cybercrime syndicates committed large-scale attacks by carry out data breaches, financial fraud, and identity theft.

According to Kaspersky (2023), cybercrime is a criminal activity mainly using or targeting computers, networks, or devices as its instrument. Most criminals or hackers take advantage of advanced technology primarily for money.

Other than that, criminals also have other intent aside from making a profit from misusing artificial intelligence. These could be political or personal. Cybercrimes can be carried out by an individual or a group of people, primarily organizations. They are highly technically skilled and use advanced techniques to commit fraudulent schemes.

Furthermore, Cisco (2023) stated that cybercrime is an illegal activity involving the internet, computers, and networks. Cybercriminals commit identity theft, phishing attacks, spread malware, and instigate others and digital attacks, prejudicing others. Cybercrimes attack any person, government, or property that

can leave a significant financial and social impact on governments, businesses,and individuals with the intent to damage them.

Coll (2022) also cited cybercrime as a serious concern in the digital age. Cybercrime is any criminal act involving computers, networks, laptops, and the Internet. Criminals steal personal information and use those credentials for them

own benefit. The goal is to extract as much value from the stolen credentials as possible before the owner notices, leaving the victim with the bill and serious damage to their credit.

To sum up cybercrime is an act that uses digital technologies such as computers as a tool or target in the commission of crime.

Technology

Technology is putting knowledge to innovate that serves its purpose to improve life and solve problems (intothecommerce, 2024). According to Anderez, et. al. (2021) technological innovation can offer a lot of opportunities for crime. However, it can also be one of the forces that can may help to improve the approaches in preventing crime.

Some research is concerned with the analytical techniques and methods employed to detect and fight cybercrime. Adnan et al. (2024) have discussed the application of artificial intelligence-powered cybersecurity analytics to analyze cybercrime detection. This illustrates the capability of AI to improve cybercrime detection. Moreover, D. Suganthi, Mythili, and Prabhu (2025) have come up with automated malware and phishing website detection techniques using cluster ensemble methods for preventing cybercrime, highlighting certain strategies to detect malicious online content. Swetha and Sivaraman (2024) came up with a SMART Model for identifying cybercriminals based on smartphone data, highlighting innovative ways to track cybercriminals via mobile device forensics.

Ali et al. (2024) presented an extended overview of types of cybercrimes and computer forensic tools with the aim to highlight the modes of cybercrimes and mechanisms used to inquire about them. Ashraf and Javaid (2025) studied convicted cheats and their enterprises and business modes with a consideration of how global regulations influence the modus operandi of cybercriminals.

Ortega Anderez et al. (2021) investigated how technology has taken center stage in crime prevention and talked about opportunities, challenges, and practitioner prospects in using technology to fight crime. Gautam and Renu (2024) researched incorporating artificial intelligence in cybercrime investigation, discussing challenges and the way forward for AI in cybercrime investigation. Chaurasia and Thakur (2024) gave a general overview of new technologies that are emerging to be used in cybercrime in cyberspace.

In short, though technology has created new opportunities for cybercrime, it also provides effective means of detection and prevention. The challenge is to remain ahead of the cybercriminals by continually advancing and enhancing these technologies.

Digital Technologies

According to Johnstone K., Kervin L., and Wyeth P., (2022) Digital technologies are firmly situated as cultural tools. Also, it is any electronics that help to increase the productivity and efficiency of the employee such as electronic tools, devices, systems, and resources organizations that keep data (Digital Adoption, 2022).

United Nation (2019) stated that digital technologies were used to identify the issues in agriculture, health, environment, and or to perform daily tasks such as navigating traffic or paving bill. Digital technologies can be an instrument that can protect and exercise human rights. Having data-powered technology can protect the personal data of an individual which may be there an asset if there were better regulation of personal data ownership. However, this can also be used to violate others.

To sum up digital technologies enhanced the life of an individuals by offering innovative solutions that improves the productivity, communications, and accessibilities across different sectors. However, even these digital technologies provide advancement there is also present of challenges such as cybersecurity risks, privacy concerns, and social inequalities.

Modus Operandi

According to Li, Y.S, and Qi, L.Y, (2019) modus operandi is the behavior and process of action needed in the completion of the crime while concealing the identity and facilitating escape following the offense. In addition, the term frequently abbreviated as M.O. which establish the pattern of how the criminal or suspect commits a crime (Insuranceopedia, 2025). Also, these M.O. shows different patterns that are specific in cultures. These M.O. may vary depends on their target and geographic location and it may transform as values grows (Kenton, W. et.al., 2024).

Additionally, the cybercriminals used variety of procedures to take advantage of merging in the vulnerabilities of digital systems and networks. Malware is a malicious software designed to compromise the system or network of an individual or institutions. Moreover, ransomware is one of the most damaging forms of malware, in this attack the profile or data of the subject will be lock out of their system and asked for ransom payment for the decryption key (Harris, 2020).

To sum up the modus operandi is the process on how the perpetrators commit their crime, set their target victims, and identify the tool needed in accomplishing their criminal acts. It is also applicable in cybercrime by having their process by determining the platform and the way how they execute their acts.

Crime Prevention

According to Monroe Community College (2023), crime prevention is anticipating crime risk and initiating action to remove or reduce it. Crime prevention is a shared responsibility as a societal problem that needs the community's cooperation. There are three main factors as to why people commit crimes: desire, ability, and opportunity. A person may want to commit a crime because they have the ability to do so, but if we deny them the opportunity to do so, then no crime can be committed.

Additionally, the European Commission (2023) stated that crime is a social phenomenon. Hence, crime prevention includes all activities that aim to halt and reduce crimes. It is an action mainly contributed

by law enforcement agencies, the government, and the judicial system, with the community's cooperation and the media's support.

To sum up, crime prevention is the barricade between lawful and unlawful acts. Without the opportunity of the offender, crime cannot exist. Crime prevention is an essential factor in lessening the commission of crimes, especially cybercrime. Crime prevention helped the researchers strengthen this study and the SIM Registration Act's credibility in fighting against cybercrimes.

Strategies in Cybercrimes

Cybercrime is now a complex system that exploits weaknesses in corporate networks, using psychological hacking, technical sophistication, and flexibility. One of the most widespread techniques employed by cybercriminals is psychological manipulation, in particular using social engineering attacks such as phishing. Such attacks typically appeal to emotions like urgency or fear to persuade victims to give up sensitive information or do things like transfer money. Bundala (2024) outlines that attackers impersonate trusted entities, e.g., banks or government agencies, to introduce fake credibility, whereas Hawdon (2021) explains that manipulative triggers in the form of threats of litigation or financial penalty are employed to obfuscate judgment. Such tactics are particularly effective against individuals with lower cybersecurity awareness, stressing the need for education and training to enable them to identify manipulative techniques.

Technically, the used of advanced tools like AI-based malware, ransomware, and deepfakes to systematize the attacks and evade detection. Singh and Lukose (2022) stated that the cybercriminals are using machine learning models to create targeted phishing operations or perform genuine user activity. Additionally, Bundala (2024) states that multi-stage attacks relating a combination of reconnaissance, weaponization, and data exfiltration, often utilizing zero-day vulnerabilities are reasons of APTs. Non innovation of technology and crypto are the difficulties in the investigation of such crime which enables money laundering. As the cybercriminals modify their methods in commission of crimes, innovation in technology is necessity to equally counterstrategies.

Resources in Combating Cybercrimes

Combating cybercrime is a very intricate problem that takes a multifaceted approach involving human behavior as well as technological and policy approaches to prevent it. Newer research highlights the use of very inventive and diverse resources to address these changing threats. For instance, cybercrime still weighs heavily on digital forensics, which is the backbone of investigation into cybercrime.

Hamad and Eleyan (2022) conducted a comparative analysis of forensic tools such as EnCase, FTK, and Autopsy, revealing that the effectiveness of these tools depends on factors like data recovery accuracy, compatibility with encrypted systems, and ease of integration into legal processes. The findings underscore the need for flexible tools that can counter new threats, including AI-forged deepfakes or blockchain-based fraud**.** Criminals are also using new technologies, they note, raising issues of the tools produced becoming obsolete quickly, and requiring continual updates for investigators and training.

Another critical component in combating cybercrime concerns the human factor. Dupuis and Jones (2024) identify demographic victim characteristics that correlate with security tool usage, such as VPNs or multi-factor authentication, including levels of income and education. Conversely, those with higher levels of neuroticism often avoid these tools altogether because of feelings of anxiety or distrust towards technology. This necessitates custom campaigns that transcend mere technical training by addressing emotional barriers. For example, one could build interactive simulations for security protocols that, in doing so, enhance confidence and reduce reluctance among less technically inclined users. Ho et

al. (2023) further demonstrated the effectiveness of cyberplace managers—professionals whose responsibility it is to remotely monitor and secure the cyber environments. The work of these managers is twofold: increasing security while also providing an educational aspect along the bridge between technical solutions and user behavior.

Yet, another unique challenge posed by cryptocurrencies in the combat against cybercrime. For Tuleun (2021), in his account of the Nigerian cybercrime landscape, the cutting-edge blockchain technology offers transparency, but its anonymity features also facilitate money laundering and ransomware payments. The Nigerian regulatory response reflects this horizontal cleavage—firstly banning all crypto transactions, then opening doorways for regulated exchanges; this balance is drawn between nurturing innovation and curbing criminal activities. Tuleun argues that smart regulation, such as imposing Know-Your-Customer protocols on virtual asset providers, will deter persons from criminally abusing the said assets without inhibiting legitimate transactions. This is in line with global trends such as the EU's MiCA (Markets in Crypto-assets) regulation intended to harmonize regulation with promoting blockchain development.

Indeed, interdisciplinary collaboration is also an important discrete area in its own right to support in efficient management of cyber risks. Cremer et al.(2022) have stated that the singularity of the term cyber risk encompasses all the risks that arise from interconnected vulnerabilities that have the potential to cause cascading effects over various networks. Such a wide spectrum of interrelationships requires the promotion of partnerships among actuarial science, computer engineering, and behavioral economics to produce workable solutions. For instance, insurance models price cyber-risk policies more accurately by adopting real-time threat intelligence from AI-powered platforms. "Red teaming" exercises conduct simulated attacks by members of an ethical hacking group trained to identify weaknesses in the corporate systems before a malicious cyber actor can exploit them.

Resource provision against cybercrime should advance hand-in-hand with innovation in counteraction against it. Major strategies would involve investing in adaptive forensic tools that utilize machine learning to detect new attacks; priority should also be given to user education through gamified training to help avoid psychological barriers to adoption of security; strengthened public-private partnerships would facilitate intelligence sharing and enforcement of regulation. Cybercrime solutions are, as Tuleun (2021) aptly puts it, a double-edged sword; as innovation becomes an agent in threatening and defending, the amalgamation of technological agility plus human insight paired with strong governance is the only way back to society outsmarting cybercriminals and withstanding their attacks.

Legal Constraint in Cybercrime

The above has again been driving the latest studies into the real and deferred challenges to the international community in the fight against cyber crime. In almost all walks of life in these post-modern eras, with the increasing proliferation of technologies, this highly complicated pack of cyber threats cannot be otherwise tackled without a multidisciplinary approach. Bridging the gap that exists between law enforcement and cybersecurity practitioners has also emerged as yet another major concern. According to Boutros (2023), interdisciplinary approaches and joint training programs shall be significant to advancing investigations and preventing cybercrime-related issues. This is the special melding of a legal perspective with a technical perspective that is imperative for holistic solutions to the complex world of cyber threats.

Next is the age-old question of jurisdiction. The matter of jurisdiction in cyber space has been elaborately dealt with by the likes of Khalifa (2020) and SAQF AL HAIT (2014) who reveal that it is from anywhere in the world where a crime might be committed. The borderless nature of the internet does not

help in pinpointing the location of the perpetrator, if he is located, and where the victim is unless he or she is actually in the location with the perpetrator. This has been added credibility by Dragojlović (2023) when he reiterated the urgent need for uniform legal statutes and coordination treaties among states. This reiterative concern was communicated by Hasan (2024) in evaluating the barriers encountered by justice in transnational cybercrime and therefore underscoring international interdependence.

The legal implications remain a subject of current inquiry. Atrey (2023) considers the issues and frameworks applicable to cybercrime, including jurisdiction, privacy, and digital evidence. The cross-border ease of committing crimes with attributing responsibility is a good reason for adaptable legal frameworks. Focused on the search warrant provisions under the Cybercrimes Act and their relationship with the Criminal Procedure Act, du Toit (2023) indicated that it is critical to have clear guidelines for the obtaining and execution of search warrants in a cybercrime investigation.

Current issues in the legal environment of cybercrime are also being studied. Amoo et al. (2024) give a thorough review of the challenges that emerge in the criminal justice system, which include the emerging forms of cybercrimes and the challenges facing its prosecution. Nishnianidze (2023) opines that current regulations appear outdated, which struggle to catch up in respect of handling the evolving threats present in cyberspace.

In all, a coordinated effort is required to tackle these problems in collaboration with law enforcement agencies, cybersecurity practitioners, and policymakers, along with the international community. Harmonizing legal frameworks, imparting technical skills but enhanced cooperation can pave the way to combating the menace that is cybercrime efficiently.

Background of the Study

The prevention of cybercrime is an odyssey marred by hard challenges arising from legal, technological, and social complexities. Recent studies pinpoint such obstacles and stress that unless they are tackled through integrated measures, they would be incapable of standing in the way of such determined attacks. A lead challenge has development in law in the fast-pacing cyber world. Ivanova (2023) speaks about cybercrimes within the BRICS countries and touches upon divergences in legal structures and enforcement mechanisms. The mentioned conflicts make it hard to apply uniform standards for prosecution and prevention-most in cross-border issues where there is a tussle for jurisdiction. Gupta and Lunia (2024) lay emphasis on the difficulties behind prosecution owing to obsolete laws and obtaining admissible digital evidence. Cybercrime per se is a peak hindering bond. Chen et al. (2023) discuss the worldwide landscapes of cybercrime, joys with prominent drivers inclusive of economic disparities and technical accessibility, creating an impetus for growth. Shehu et al. (2024) in Kebbi State outline local bottlenecks affecting these efforts in crime prevention: limited resources available for law enforcement, as well as a low level of public awareness of cyber threats. Therefore, it is paramount to run targeted education campaigns to raise the level of digital literacy.

Technologically based impediments also increase the difficulty of preventing cybercrime. Bin Baharudin (2022), in questioning the hurdles to investigation into cybercrime, declares methods of criminals such as the use of encryption and anonymization tools that conceal their footprints. Apparent need here for standardized forensic tools and training in their usation is emphasized by Horan and Saiedian (2021), as investigators are prevented from collecting and analyzing digital evidence properly.

The social context is also imperative in the prevention of cybercrime. Althibyani and Al-Zahrani (2023) examined the knowledge, conviction, and digital citizenship skills of students with regard to their

role in preventing cybercrime, thus demonstrating that education to foster a culture of responsible behavior online can greatly lessen vulnerabilities**.** In their turn, Namrata and Chethan (2024) notice that the rise in awareness among society is essential in combating cybercrime because societies that are aware of the impact of cybercrime are better placed to adopt preventive measures.

The prevention of cybercrime will require gaps, laws, technological enhancements, and awareness in society. By virtue of aligning international legal regimes, providing tools for better investigations, and improving digital literacy, stakeholders can therefore act on these fronts together to mount a resilient defense against cyber threats. However, as pointed out by Vitus (2023), to create a safe digital environment, the stakeholders, that is, government, law enforcement, the private sector, and the public at large, will need to engage in continued collaboration.

Theoretical Framework

This study is anchored on the **Collaborative Governance Theory** as proposed by Ansell and Gash (2008), which emphasizes the importance of inclusive, participatory, and consensus-driven decision-making processes in addressing complex public issues. In the context of cybercrime prevention, this theory provides a relevant and powerful lens through which to analyze the dynamics of public trust, community engagement, and institutional collaboration in the efforts of the Philippine National Police (PNP), particularly its Anti-Cybercrime Group (ACG).

Collaborative Governance Theory posits that governance is no longer the sole responsibility of the government but a shared undertaking involving multiple stakeholders, including citizens, civil society organizations, private sectors, and public institutions. The theory underscores that effective policy implementation in highly technical and evolving issues such as cybercrime requires **mutual trust, open dialogue, shared responsibility**, and **transparent processes**.

In the case of the PNP's cybercrime prevention initiatives, the theory helps frame the investigation of how collaborative mechanisms are designed and implemented, how the public perceives these efforts, and to what extent these relationships promote a trust-based environment that enables effective cybercrime prevention. The involvement of the public is crucial, especially in areas such as **online safety awareness, cybercrime reporting, victim support, and community-led digital literacy programs**. Collaborative governance emphasizes that such involvement is more successful when trust in law enforcement institutions is strong, and when citizens feel they are legitimate partners in public safety.

Research Framework

Figure 1 is the research paradigm of this study. The first box represents the demographic profile of respondents in terms of age, sex, and length of service. The first rectangular shape Inside the big box is the public trust and collaboration in terms of mutual trust, open dialogue, shared responsibility, and transparent processes. The second rectangular shape are the PNP's cybercrime prevention initiatives in terms of the online safety awareness, cybercrime reporting, victim support, and community-led digital literacy programs. The ultimate objective of this study is to come up with an inputs in preventing and suppressing cybercrime offenses.

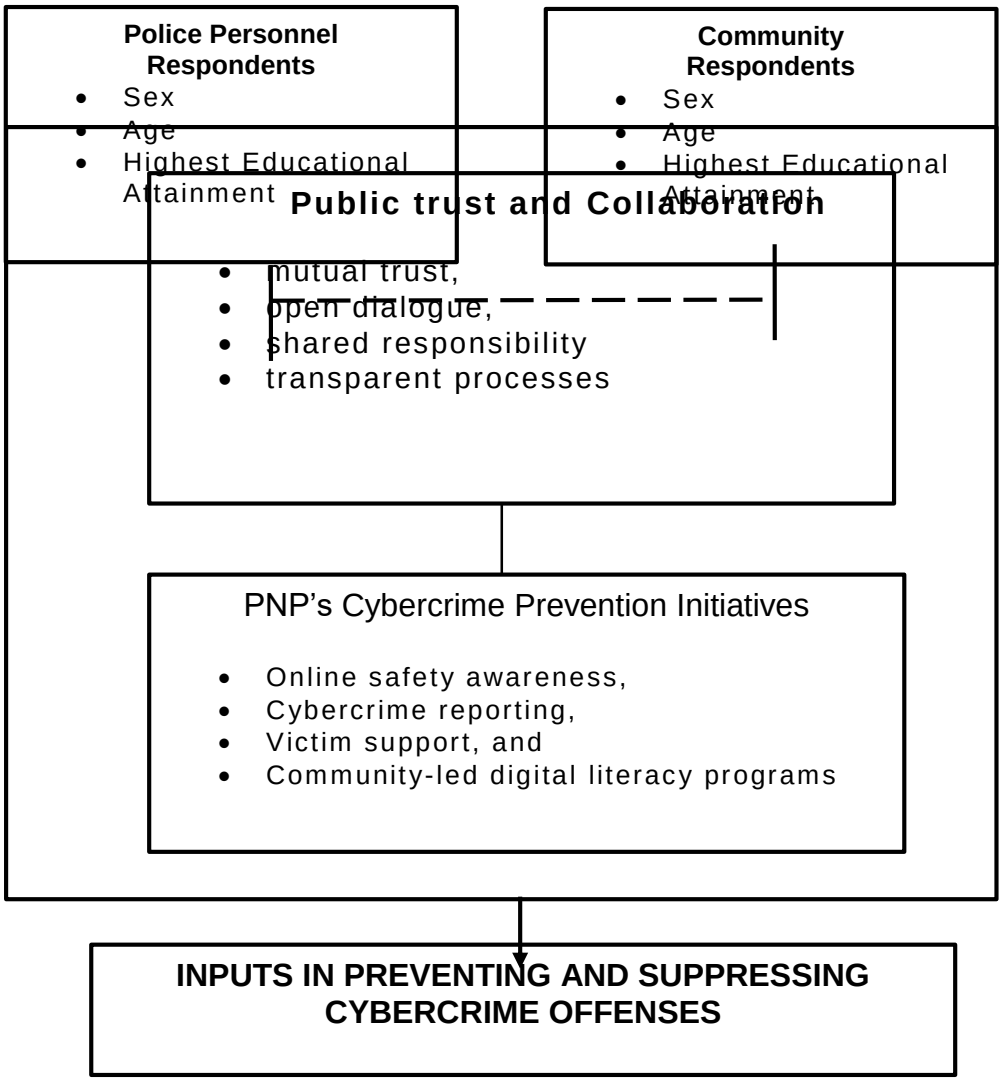

Figure 1. Research Paradigm

Statement of the Problem

This study determined the public trust and collaboration in the PNP's cybercrime prevention initiatives. Specifically, it answered the following

1. What is the demographic profile of the respondents in terms of:
   1.1. age,
   1.2. sex, and
   1.4 Educational attainment?
2. What is the assessment of the two groups respondents on the public trust and collaboration in terms of:
   2.1. mutual trust,
   2.2 open dialogue,
   2.3 shared responsibility, and
   2.4 transparent processes**?**
3. Is there significant difference in the assessment of the two groups respondents on the public trust and collaboration when their profile is taken as test factor?

4. What is the assessment of respondents on the PNP's cybercrime prevention initiatives in terms of the following:

4.1 online safety awareness,

4.2 cybercrime reporting,

4.3 victim support, and

4.4 community-led digital literacy programs?

5. Is there significant difference in the assessment of respondents on the PNP's cybercrime prevention initiatives when their profile is taken as test factor?

6. Is there significant relationship in the assessment of respondents between the public trust and collaboration and the PNP's cybercrime prevention initiatives?

7. Based on the results of the study what inputs in preventing and suppressing cybercrime offenses can be proposed?

Hypotheses of the Study

1. There is no significant difference assessment of the two groups respondents on the public trust and collaboration in terms of mutual trust, open dialogue, shared responsibility, and transparent processes when their profile is taken as test factor.

2. There is no significance difference in the assessment of respondents on the PNP's cybercrime prevention initiatives in terms of the online safety awareness, cybercrime reporting, victim support, and community-led digital literacy programs.

3. There is no significant relationship in the assessment of respondents between the public trust and collaboration and the PNP's cybercrime prevention initiatives.

Significance of the Study

This study is significant in light of the growing prevalence of cybercrime in the Philippines and the increasing need for responsive, transparent, and collaborative public safety mechanisms. The findings of this research will contribute to a deeper understanding of how public trust and citizen collaboration impact the success of the Philippine National Police Anti-Cybercrime Group (PNP-ACG), particularly in the context of Region IV-A, where digital connectivity, socioeconomic diversity, and public engagement levels vary widely.

For **Policymakers and Law Enforcement Leaders**, the study offers evidence-based insights into how institutional design, facilitative leadership, and collaborative governance practices can be enhanced to better engage citizens. The results can inform the development or refinement of policies, training programs, and outreach strategies that prioritize trust-building, transparency, and inclusion in anti-cybercrime efforts.

For the PNP-ACG and Local Government Units (LGUs), the study highlights the critical role of community participation in preventing cyber threats. It will provide practical recommendations for strengthening partnerships with schools, non-government organizations (NGOs), the private sector, and civil society in Region IV-A. These recommendations may lead to the institutionalization of collaborative mechanisms such as digital literacy campaigns, cybercrime reporting protocols, and multi-stakeholder forums.

For Academic and Research Institutions, the study expands the application of Collaborative Governance Theory in the realm of cybersecurity and law enforcement. It contributes to the body of

knowledge in criminal justice, public administration, and digital governance by presenting a localized analysis of public-police relations in cyberspace.

For Citizens and Civil Society Organizations, the study emphasizes their role not only as beneficiaries but also as active collaborators in cybercrime prevention. Understanding the determinants of trust and participation can empower citizens to play a more informed, confident, and strategic role in ensuring digital safety and accountability.

Finally, this research will serve as a foundational reference **for future studies** on cybercrime prevention, digital trust, and collaborative governance in the Philippines and comparable contexts. It supports the broader national goal of strengthening digital public safety infrastructure through inclusive, multi-sectoral, and trust-based approaches.

Scope and Delimitations of the Study

This study focused on the assessment of public trust and collaboration in the cybercrime prevention initiatives implemented by the Philippine National Police Anti-Cybercrime Group (PNP-ACG) in Region IV-A, which includes the provinces of Cavite, Laguna, Batangas, Rizal, and Quezon. The study is limited to assessment of the two groups respondents on the public trust and collaboration in terms of mutual trust, open dialogue, shared responsibility, and transparent processes when their profile is taken as test factor. Likewise, on the PNP's cybercrime prevention initiatives in terms of the online safety awareness, cybercrime reporting, victim support, and community-led digital literacy programs.

Definition of Terms

For better understanding the following terms and phrases are operational define:

Cybercrime, Illegal acts committed through the use of digital technology, particularly involving computers, networks, or the internet. This includes phishing, cyberbullying, hacking, online scams, and child pornography.

Philippine National Police Anti-Cybercrime Group (PNP-ACG). The specialized unit of the PNP tasked with addressing cybercrime threats and enforcing laws related to cybersecurity and cyber offenses.

Region IV-A (CALABARZON). A region in the Philippines comprising the provinces of Cavite, Laguna, Batangas, Rizal, and Quezon. It is the focus area of this study due to its growing urbanization and digital activity.

Public Trust – The confidence and belief of the general public in the integrity, capability, and responsiveness of the PNP to protect them against cybercrime.

Collaboration – The active participation and cooperative efforts between the public, local stakeholders, and the PNP-ACG in cybercrime prevention programs.

Collaborative Governance Theory – A framework that promotes the inclusion of multiple stakeholders, including government, citizens, and civil society, in public decision-making and implementation processes.

Mutual Trust. The degree of confidence shared between the PNP-ACG and the public in Region IV-A, measured through indicators such as perceived reliability, integrity, and consistency of actions in cybercrime prevention efforts.

Open Dialogue. A communication mechanism between the PNP-ACG and the community that involves regular, inclusive, and transparent discussions—such as town hall meetings, forums, or online consultations—on issues related to cybercrime and digital safety.

Shared Responsibility. The extent to which both the PNP and the public acknowledge and act upon their respective roles in cybercrime prevention, demonstrated by joint initiatives, public participation in awareness programs, and support for local digital safety policies.

Transparent Processes. The clarity, openness, and accountability of PNP cybercrime procedures—such as case handling, reporting protocols, and feedback mechanisms—evaluated by citizen access to information and satisfaction with how cases are managed.

Online Safety Awareness. The level of public knowledge and understanding regarding safe internet practices, measured through participation in digital literacy campaigns, school programs, and self-reported knowledge of cyber threats and prevention measures.

Cybercrime Reporting. The act of formally communicating a cybercrime incident to the PNP or other authorized agencies, operationalized by the frequency, ease of access, and responsiveness of reporting systems such as hotlines, websites, or mobile apps.

Victim Support. The availability and effectiveness of services provided by the PNP-ACG and partner institutions to individuals affected by cybercrime, including legal assistance, psychological counseling, and case updates, as perceived by the community.

Community-led Digital Literacy Programs. Educational initiatives organized by local groups, schools, or NGOs in collaboration with the PNP-ACG that aim to increase public understanding of internet safety, digital rights, and cybercrime prevention at the grassroots level.

METHODOOGY

This study utilized the evaluation survey **Research Design**. Creswell, John W. and J. David, Creswell. 2018, explain that evaluation research study is a “process used to determine and identify the purpose of the survey research and accordingly, the primary purpose is to answer questions about variables of interest to the researcher. Since the main objective of this study is to assess by the respondents the public trust and collaboration in terms of mutual trust, open dialogue, shared responsibility, and transparent processes when their profile is taken as test factor. Likewise, on the PNP’s cybercrime prevention initiatives in terms of the online safety awareness, cybercrime reporting, victim support, and community-led digital literacy programs.

This study is generally quantitative. Quantitative descriptive research design provides a description of an event or define a set of attitudes, opinions, or behaviors that are observed or measured at a given time and environment (Creswell, John W. and J. David, Creswell, 2018). It typically involved large samples. This design gathered information from the respondents in their assessment on the public trust and collaboration in terms of mutual trust, open dialogue, shared responsibility, and transparent processes when their profile is taken as test factor. Likewise, on the PNP’s cybercrime prevention initiatives in terms of the online safety awareness, cybercrime reporting, victim support, and community-led digital literacy programs.

The **Research Locale** of the study confined in the assessment of respondents on the public trust and collaboration in the cybercrime prevention initiatives implemented by the Philippine National Police

Anti-Cybercrime Group (PNP-ACG) in Region IV-A, which includes the provinces of Cavite, Laguna, Batangas, Rizal, and Quezon.

The **population and sampling procedure** (Babbie, 2015; & Fowler, 2014 cited by Creswell, John W. and J. David, Creswell, 2018) provide for the essential aspects of the population and sample describe in a research plan. The research has a total population of 120 broken down as follows: 50 police personnel and 70 community residents.

Research Instrument

As part of the rigorous data collection, the Research Instrument used by this researcher, a self-made questionnaire designed with the help of his adviser. The designed and the developed survey questionnaire is for the assessment of the respondents on the public trust and collaboration in terms of mutual trust, open dialogue, shared responsibility, and transparent processes when their profile is taken as test factor. Likewise, on the PNP's cybercrime prevention initiatives in terms of the online safety awareness, cybercrime reporting, victim support, and community-led digital literacy programs

Gathering of data

Introductory letter to the respondents was included requesting them to answer all the items needed to completely gather the data required. In particular, the letter explains the objective of the study to the respondents. The main body of the survey questionnaire consists of three (3) parts. The first part demographic profile of respondents in terms of is the assessment of the two groups respondents on the public trust and collaboration in terms of mutual trust, open dialogue, shared responsibility, and transparent processes.

For the detailed presentation of the survey instrument. please find attached, Annexed "A", entitled, "Survey Questionnaire".

The following rating scales used by the respondents in their assessments, to wit:

For the detailed presentation of the survey instruments please find attached, Annexed "A", entitled, "Survey Questionnaire". used the following rating scales:

Scale	Range	Degree
4	3.51-4.00	Strongly Agree (SA)/Highly Evident (HE)
3	2.51-3.50	Agree (A)/ Evident (E)
2	1.51-2.50	Disagree (DA)/Slightly Evident (SE)
1	1.00-1.50	Strongly Disagree (SD)/ Not Evident (NE)

In the gathering of data, the researcher initially wrote a letter to the Chief of police, where the respondents are actually located. The respective approval of those personnel in charge are extremely necessary.

Statistical Treatment of Data

The following statistical tools that were used in this study are:

The **weighted mean**. The following rating scales used by the respondents in their assessments, to wit:

Scale	Range	Degree
4	3.51-4.00	Strongly Agree (SA)/Highly Evident (HE)
3	2.51-3.50	Agree (A)/ Evident (E)
2	1.51-2.50	Disagree (DA)/Slightly Evident (SE)
1	1.00-1.50	Strongly Disagree (SD)/ Not Evident (NE)

To test the hypothesis of no significant difference in the assessment of the two (2) groups of respondents on the assessment of the two groups respondents on the public trust and collaboration in terms of mutual trust, open dialogue, shared responsibility, and transparent processes. Likewise, the significant difference in the assessment of the two (2) groups of respondents the **Analysis of Variance (ANOVA)** was used.

Pearson's r were used to test the relationship of the assessment of the two groups of respondents on the significant relationship in the assessment of respondents between the public trust and collaboration and the PNP's cybercrime prevention initiatives.

Ethical Considerations

In conducting this study, the researcher ensured that several ethical considerations were carefully observed to protect the rights and welfare of the respondents. First, the respondents were fully briefed on the purpose of the research. They were provided with a clear explanation of the study's objectives, the scope of the investigation, and how their participation would contribute to the overall research. This step ensured that respondents were well-informed before agreeing to take part in the study.

Second, it will be made explicitly clear to all respondents that their participation was entirely voluntary. There was no pressure or obligation to participate, and respondents were free to withdraw from the study at any point without any negative consequences. This voluntary aspect helped ensure that all data collected was from individuals who chose to contribute freely.

Third, the researcher will take care to describe the data collection and analysis procedures clearly to the respondents. This transparency ensured that they understood exactly what they would be asked to do, how their data would be collected, and how it would be analyzed. By clarifying the process, the researcher aims is to make participants feel comfortable and knowledgeable about their role in the research.

Additionally, respondents will be provided with letter of consent prior to their participation. These forms will detail the purpose of the study, the voluntary nature of participation, the confidentiality measures in place, and the right to withdraw. Proceeding in answering the questionnaire indicated that the respondents had been informed of their rights and agreed to participate under those conditions.

Finally, the confidentiality and anonymity of the respondents will be strictly maintained throughout the study. Any personal information collected will be kept secure, and no identifying details were shared in the analysis or final report. By protecting their anonymity, the researcher ensured that the respondents' privacy was respected and that their personal data remain confidential. These ethical practices will be vital in fostering trust between the researcher and the participants and upholding the integrity of the study.

RESULTS AND ANALYSIS

This section presents the analysis and interpretation of data gathered in the study. It involves the examination and interpretation of the collected data to uncover patterns, trends, and insights related to the research objectives and questions. It focuses on presenting and analyzing the data in a systematic and organized manner, using appropriate statistical techniques and qualitative methods as applicable.

1. ON THE DEMOGRAPHIC PROFILE OF THE RESPONDENTS IN TERMS OF: AGE, SEX, AND EDUCATIONAL ATTAINMENT.

Table 1
Profile of Respondents

Variable	Category	Frequency	Percentage
Group	Police Personnel	50	41.7%
	Community Residents	70	58.3%
Sex	Male	74	61.7%
	Female	46	38.3%
Age	Below 25	23	19.2%
	25-35	16	13.3%
	36-45	26	21.7%
	46-55	18	15.0%
	55-65	27	22.5%
	65 above	10	8.3%
Highest Educational Attainment	High School	14	11.7%
	Vocational	28	23.3%
	Bachelor's	52	43.3%
	Postgraduate	26	21.7%
Total		**120**	**100**

The respondents of the study were composed of two groups: police personnel and community residents. Of the 120 total respondents, 50 or 41.7% were identified as police personnel while 70 or 58.3% were community residents. This indicates a higher proportion of community participants, which is appropriate in a study examining mutual trust and collaboration, as it suggests greater representation of civilian perspectives. This balance between law enforcement and community members may enrich the validity of the findings, particularly in understanding bidirectional trust dynamics.

In terms of sex, the sample was predominantly male, with 74 male respondents accounting for 61.7% of the total, compared to 46 females or 38.3%. This distribution aligns with expectations in studies involving police personnel, where males traditionally

dominate. However, the inclusion of a significant percentage of female participants ensures that both gender perspectives are captured. Gender representation is essential in trust-related studies, given that perceptions of police integrity and community engagement may vary across sexes.

The age profile of the respondents reveals a broad distribution across six age brackets. The highest percentage of respondents falls within the 55–65 age group, comprising 22.5% of the sample, closely followed by the 36–45 age group with 21.7%, and the below-25 bracket at 19.2%. This indicates that both younger and older generations are adequately represented, with a slight concentration among middle-aged and near-retirement individuals. Interestingly, those in the 25–35 age group are the least represented at 13.3%. The presence of senior individuals (8.3% aged 65 above) suggests that cybercrime issues and trust concerns transcend generational boundaries and affect even older populations.

Regarding educational attainment, a considerable portion of the respondents held a bachelor's degree, accounting for 43.3% of the total. This is followed by those with vocational training (23.3%) and postgraduate education (21.7%). Only 11.7% of the participants had completed only high school. This relatively high level of education, with two-thirds having at least a bachelor's degree, is likely to influence perceptions of institutional integrity and civic responsibility. Education level can significantly affect respondents' ability to critically evaluate trustworthiness and collaborative potential with law enforcement.

To summarize, the profile of respondents shows a well-distributed representation across police and civilian groups, with more male participants and a spread across age brackets that leans slightly toward older respondents. The educational background is notably high, which implies that respondents may possess the capacity for critical assessment in matters of cybercrime and institutional trust. This demographic distribution lays a sound foundation for analyzing perceptions of mutual trust and collaborative capacity in addressing cybercrime.

2. ON THE ASSESSMENT OF THE TWO GROUPS RESPONDENTS ON THE PUBLIC TRUST AND COLLABORATION IN TERMS OF: MUTUAL TRUST, OPEN DIALOGUE, SHARED RESPONSIBILITY, AND TRANSPARENT PROCESSES

Table 2

Assessment of Respondents on Public Trust and Collaboration in terms of Mutual Trust

Indicator	WM	SD	QD	VI	RANK
I believe that the PNP Anti-Cybercrime Group acts with integrity when handling cybercrime cases	3.45	0.74	Agree	Evident	1

There is mutual respect and trust between the police and the community in addressing cybercrime issues	3.39	0.78	Agree	Evident	3.5
The public can rely on the PNP to maintain confidentiality when a cybercrime is reported	3.39	0.8	Agree	Evident	3.5
Community members trust the competence of the PNP-ACG in resolving cybercrime incidents	3.11	0.91	Agree	Evident	7
The PNP actively demonstrates trust in the community's capacity to cooperate in cybercrime prevention	3.24	0.84	Agree	Evident	5
Previous interactions between the police and the community have strengthened our mutual trust	3.14	0.86	Agree	Evident	6
Both the police and residents are open to working together based on shared trust and responsibility in combating cybercrime	3.43	0.72	Agree	Evident	2
Overall Mean	3.31	0.34	Agree	Evident	

Legend: 3.51 – 4.00 (Strongly Agree-Highly Evident); 2.51 – 3.50 (Agree- Evident); 1.51 – 2.50 (Disagree-Slightly Evident); 1.0-1.50 (Strongly Disagree-Not Evident)

The data on public trust and collaboration in terms of mutual trust reflects an overall favorable perception among respondents, with an overall mean score of 3.31 and a standard deviation of 0.34. This places the general assessment in the "Agree" category, signifying that mutual trust between the community and the PNP Anti-Cybercrime Group (PNP-ACG) is evident, though not strongly affirmed. The relatively low standard deviation implies consistency in the responses across indicators.

Among the seven indicators, the statement "I believe that the PNP Anti-Cybercrime Group acts with integrity when handling cybercrime cases" received the highest mean score of 3.45. This suggests that the integrity of the PNP-ACG is recognized and appreciated by the public and personnel alike. It reflects positively on the internal practices and transparency measures of the unit in handling sensitive cybercrime issues. Close to this, the statement regarding shared trust and responsibility ("Both the police and residents are open to working together…") received a high mean of 3.43, underscoring a strong willingness on both sides to foster cooperative relations in combating cybercrime.

Conversely, the lowest-rated item was "Community members trust the competence of the PNP-ACG in resolving cybercrime incidents," which garnered a mean of 3.11. While this still falls under the "Agree" category, it reflects a more cautious stance

regarding operational effectiveness rather than ethical conduct. This indicates that while the PNP may be trusted in terms of integrity, there may be lingering doubts about their technical capacity or response efficiency in resolving cybercrime issues.

Other indicators received moderate but consistent levels of agreement. For example, the belief that "There is mutual respect and trust between the police and the community" and "The public can rely on the PNP to maintain confidentiality" both garnered identical means of 3.39, suggesting these aspects are perceived positively, but with room for reinforcement. Similarly, the perception that "The PNP actively demonstrates trust in the community's capacity to cooperate" had a lower mean of 3.24, hinting at a possible asymmetry—where the community may be more open to trust than perceived reciprocation by the police.

The moderate to high agreement across all indicators confirms that mutual trust exists and is evident in cybercrime-related interactions, but it is not yet robust or unequivocal. The community recognizes ethical intentions and openness, but expectations around technical competence and reciprocal empowerment could be improved. Notably, previous interactions were rated at 3.14, suggesting that past experiences may have positively influenced trust-building but have not been wholly transformative.

In conclusion, the data from this table confirms that trust and collaboration are present and functionally evident, but not yet deeply entrenched. The PNP-ACG enjoys a reputation for integrity and confidentiality, but perceived competence and mutual empowerment require further strengthening. These results highlight an important opportunity to deepen trust by enhancing technical training, ensuring community involvement, and fostering positive, reciprocal engagements in cybercrime prevention and response.

Table 3
Assessment of Respondents on Public Trust and Collaboration in terms of open dialogue

Indicator	WM	SD	QD	VI	RANK
The PNP-ACG regularly communicates with the community about cybercrime issues and prevention strategies	3.17	0.84	Agree	Evident	6
Community members are given opportunities to express their concerns and suggestions regarding cybercrime prevention	2.81	0.78	Agree	Evident	7
There are open forums or discussions between the police and the public that address digital safety and cyber threats	3.5	0.64	Agree	Evident	3

I feel comfortable initiating conversations with the PNP regarding online security concerns	3.62	0.61	Strongly Agree	Highly Evident	1
The police provide timely and understandable information to the community on cybercrime developments	3.48	0.78	Agree	Evident	4
Community feedback is acknowledged and considered in the planning of anti-cybercrime initiatives	3.18	0.63	Agree	Evident	5
Open and transparent communication exists between the PNP and the community regarding ongoing cybercrime cases and prevention programs	3.57	0.79	Strongly Agree	Highly Evident	2
Overall Mean	**3.33**	**0.33**	**Agree**	**Evident**	

Legend: 3.51 – 4.00 (Strongly Agree-Highly Evident); 2.51 – 3.50 (Agree- Evident); 1.51 – 2.50 (Disagree-Slightly Evident); 1.0-1.50 (Strongly Disagree-Not Evident)

The overall mean score of 3.33, with a standard deviation of 0.33, suggests that open dialogue between the Philippine National Police Anti-Cybercrime Group (PNP-ACG) and the community is evident and consistently perceived as favorable by the respondents. This indicates a generally positive perception of communication and exchange of information related to cybercrime prevention efforts. The small standard deviation further implies that the responses are closely aligned, suggesting that both police personnel and community residents share similar perceptions regarding the openness of communication channels.

Among the items measured, the statement “I feel comfortable initiating conversations with the PNP regarding online security concerns” garnered the highest mean score of 3.62, placing it in the “Strongly Agree” and “Highly Evident” category. This is a particularly important finding because it reflects the respondents’ confidence in approaching law enforcement authorities about their cyber-related concerns. The comfort to engage indicates trust not only in the institution's approachability but also in its willingness to listen and act.

Another item that rated highly is “Open and transparent communication exists between the PNP and the community regarding ongoing cybercrime cases and prevention programs,” with a mean of 3.57. This suggests that transparency in communication is a key strength of the PNP-ACG. Respondents perceive that there is deliberate effort on the part of the police to keep the public informed about cybercrime cases and that such communication fosters greater collaboration and mutual understanding.

The lowest rating, though still within the "Agree" range, is the item "Community members are given opportunities to express their concerns and suggestions regarding cybercrime prevention," with a mean score of 2.81. This reflects a slight gap between information dissemination and actual participatory dialogue. While the PNP-ACG may be transparent in delivering information, there seems to be a limited framework for feedback mechanisms or formal consultations where citizens can actively influence anti-cybercrime strategies.

Another key observation lies in the item "The police provide timely and understandable information to the community on cybercrime developments," with a mean of 3.48. This is close to the upper limit of the "Agree" category and highlights the perceived responsiveness and clarity of communication. Moreover, the presence of open forums between the police and public, rated at 3.5, also confirms that structured discussions are happening, although their frequency or inclusivity may require further exploration.

In sum, the assessment reveals that the police-community relationship benefits from a strong foundation of communication and openness. However, the findings also point toward the need to strengthen two-way communication—particularly in terms of creating more opportunities for the community to voice their opinions and be part of policy or strategy formation. The relatively high scores in comfort and transparency underscore a strong institutional effort that could be further enhanced through participatory structures.

Table 4
Assessment of Respondents on Public Trust and Collaboration in terms of Shared Responsibility

Indicator	WM	SD	QD	VI	Rank
Both the police and the community have important roles to play in preventing cybercrime	3.06	0.85	Agree	Evident	3
The community actively supports PNP-ACG efforts by reporting suspicious online activities	2.73	0.96	Agree	Evident	7
I believe that cybercrime prevention should not be left solely to the police	3.07	0.71	Agree	Evident	2
The PNP encourages citizens to take part in educational campaigns about online safety	2.88	0.84	Agree	Evident	6
There is a shared commitment between the police and the community to reduce cybercrime incidents	2.9	0.83	Agree	Evident	5

The success of cybercrime prevention in our area depends on collaboration between the police and the public	3.17	0.68	Agree	Evident	1
The PNP and community members jointly participate in initiatives that promote responsible internet use.	3.00	0.59	Agree	Evident	4
Overall Mean	2.97	0.27	Agree	Evident	

Legend: 3.51 – 4.00 (Strongly Agree-Highly Evident); 2.51 – 3.50 (Agree- Evident); 1.51 – 2.50 (Disagree-Slightly Evident); 1.0-1.50 (Strongly Disagree-Not Evident)

The overall mean score of 2.97 suggests that the principle of shared responsibility between the police and the community in cybercrime prevention is moderately evident. This falls within the "Agree" category, indicating general support for collaborative efforts, though not with overwhelming consensus. The relatively low standard deviation of 0.27 indicates that respondents' views were closely aligned across various indicators.

The highest scoring item in this construct is "The success of cybercrime prevention in our area depends on collaboration between the police and the public," which scored 3.17. This finding reinforces the importance of cooperative engagement and mutual roles in crime prevention. Respondents generally acknowledge the necessity of synergy between the two groups, signaling an awareness of collective efficacy as a prerequisite for combating cyber threats.

Another relatively high-scoring item is "I believe that cybercrime prevention should not be left solely to the police," with a mean of 3.07. This reinforces the notion that the public understands and accepts a degree of accountability and involvement in addressing cybercrime. Importantly, this reflects a broader cultural shift from reactive dependence on authorities to proactive civic participation.

On the other hand, the lowest mean value was recorded for the item "The community actively supports PNP-ACG efforts by reporting suspicious online activities," which received a 2.73 mean. Although still within the "Agree" bracket, this lower score suggests some degree of hesitation or lack of initiative among community members to report cybercrime incidents. This could be attributed to fear, lack of awareness of reporting channels, or limited confidence in the system's responsiveness.

The statement "The PNP encourages citizens to take part in educational campaigns about online safety" garnered a 2.88 mean, which, although moderately positive, points to an area needing reinforcement. Community involvement in educational campaigns is critical for sustainability in crime prevention, and the moderate score suggests that either the invitations to participate are insufficiently communicated or that public interest remains limited.

Overall, this table reveals that while there is agreement on the concept of shared responsibility, its operationalization remains limited. The community sees the importance of cooperation, yet actual participation in specific initiatives like reporting or campaigns appears to be suboptimal. These findings suggest a need for the PNP-ACG to enhance its outreach, particularly by emphasizing the value of citizen action and by facilitating easier access to engagement platforms.

Table 5
Assessment of Respondents on Public Trust and Collaboration in terms of Transparent Processes

Indicator	WM	SD	QD	VI	RANK
The PNP and community members jointly participate in initiatives that promote responsible internet use.	2.63	0.8	Agree	Evident	7
Citizens are informed about the status and progress of their reported cybercrime complaints	3.22	0.76	Agree	Evident	3.5
The PNP uses transparent methods in handling cybercrime investigations and public concerns	3.51	0.62	Strongly Agree	Highly Evident	1
There are accessible channels for the public to verify information about cybercrime cases and prevention programs	3.38	0.7	Agree	Evident	2
The police provide regular updates to the community on cybercrime statistics and trends	3.06	0.8	Agree	Evident	5
I trust that the PNP follows due process in managing cybercrime incidents involving members of the public	3.22	0.74	Agree	Evident	3.5
The guidelines and responsibilities of both police and citizens in cybercrime prevention are clearly communicated and understood	2.88	0.87	Agree	Evident	6
Overall Mean	3.13	0.27	Agree	Evident	

Legend: 3.51 – 4.00 (Strongly Agree-Highly Evident); 2.51 – 3.50 (Agree- Evident); 1.51 – 2.50 (Disagree-Slightly Evident); 1.0-1.50 (Strongly Disagree-Not Evident)

The dimension of transparent processes scored an overall mean of 3.13, indicating that transparency in cybercrime operations and communication by the PNP-ACG is generally evident to the respondents. This score, while within the "Agree" range, reveals that although transparency is observed, it is not uniformly robust across all measured items. A standard deviation of 0.27 further underscores the consistency in respondents' perceptions.

The highest scoring item is "The PNP uses transparent methods in handling cybercrime investigations and public concerns," which received a mean of 3.51. This falls in the "Strongly Agree" category and indicates a high level of public confidence in the institutional integrity and accountability of the PNP-ACG. It suggests that transparency in investigative procedures and how public concerns are addressed is a standout strength of the group.

The next highest items are "There are accessible channels for the public to verify information about cybercrime cases and prevention programs" (mean = 3.38) and "Citizens are informed about the status and progress of their reported cybercrime complaints" (mean = 3.22). These scores suggest that respondents feel sufficiently informed and that appropriate channels for verification and updates exist, though they may not be maximally utilized or uniformly accessible.

The lowest-rated item is "The PNP and community members jointly participate in initiatives that promote responsible internet use," which received a mean score of 2.63. This low score highlights a critical area for improvement. While transparency may be visible in information sharing and due process, joint initiatives—especially those that build digital citizenship—remain underdeveloped. This implies a gap between transparency as a principle and its translation into participatory action.

The item "The guidelines and responsibilities of both police and citizens in cybercrime prevention are clearly communicated and understood" scored 2.88. Although within the "Agree" range, this suggests there is a need to improve clarity and dissemination of policies or procedural expectations, possibly through more localized or simplified campaigns to reach diverse segments of the population.

In summary, this table reveals that transparency is one of the stronger aspects of the PNP-ACG's public engagement framework, especially in the context of investigation handling and communication. However, transparency alone does not necessarily lead to participation, and the data suggests the need to focus on converting transparency into co-owned action. The challenge lies in bridging the gap between being informed and being involved.

Table 6
Summary on the Assessment of Respondents on Public Trust and Collaboration

Indicator	Weighted Mean	Standard Deviation	Qualitative Description	Verbal Interpretation	Rank
1. Mutual Trust	3.31	0.34	Agree	Evident	2
2. Open Dialogue	3.33	0.33	Agree	Evident	1

3. Shared Responsibility	2.97	0.27	Agree	Evident	4
4. Transparent Processes	3.13	0.27	Agree	Evident	3
Overall Mean	3.19	0.14	Agree	Evident	

Legend: 3.51 – 4.00 (Strongly Agree-Highly Evident); 2.51 – 3.50 (Agree- Evident); 1.51 – 2.50 (Disagree-Slightly Evident); 1.0-1.50 (Strongly Disagree-Not Evident)

This summary table synthesizes the assessments from the four thematic dimensions: mutual trust, open dialogue, shared responsibility, and transparent processes. The overall mean of 3.19 affirms that the respondents "Agree" with the presence and effectiveness of public trust and collaboration initiatives by the PNP-ACG, categorized as evident. A very low standard deviation of 0.14 underscores the consistency of perceptions across the respondents, indicating little variability and a shared understanding of the status of police-community relations in the cybercrime context.

Open dialogue emerged with the highest mean score of 3.33, followed closely by mutual trust at 3.31. These figures suggest that communication and trust form the strongest pillars of the police-community relationship. Open dialogue, in particular, implies that the community feels seen and heard in interactions with the police, and that accessible avenues for information exchange are in place. Mutual trust is likewise strong, confirming the general integrity and reliability of the PNP-ACG as perceived by the respondents.

Transparent processes scored 3.13, indicating that while transparency is evident, it slightly lags behind in strength compared to trust and dialogue. This dimension may benefit from more community visibility in police operations and sustained updates on cybercrime statistics and ongoing cases. It remains a moderately strong component of the collaboration, but further reinforcement could lead to deeper institutional credibility.

The dimension with the lowest score is shared responsibility, with a mean of 2.97. While still within the "Agree" category, the relatively lower score highlights a perceptual gap between recognizing and acting on one's civic role in cybercrime prevention. This suggests that although the community and police conceptually accept that both parties are involved, operational collaboration such as reporting, campaign participation, and co-designed initiatives is not yet optimal.

Overall, this synthesis affirms a generally favorable view of the PNP-ACG's efforts in building public trust and collaborative structures. The findings point toward a well-established foundation of communication and trust, with opportunities for growth in co-responsibility and participatory program design. To progress toward a more integrated cybercrime prevention model, the PNP-ACG may focus on translating transparency and dialogue into tangible joint actions that deepen community ownership and engagement.

3. ON THE SIGNIFICANT DIFFERENCE IN THE ASSESSMENT OF THE TWO GROUPS RESPONDENTS ON THE PUBLIC TRUST AND COLLABORATION WHEN THEIR PROFILE IS TAKEN AS TEST FACTOR

This table 7 presents the comparison between the assessments of police personnel and community residents across various dimensions of public trust and collaboration. The results reveal both convergence and divergence in perceptions, with statistical significance noted in two of the four dimensions. For mutual trust, police personnel reported a higher mean (3.39) compared to community residents (3.24). With a t-value of 6.391 and a significance level of 0.013, the null hypothesis is rejected, indicating a significant difference. This suggests that police personnel are more confident in the level of trust between them and the community than the residents themselves are. It may reflect a perceptual gap wherein the police overestimate the degree of mutual trust, or alternatively, community members may feel that trust has not been fully established.

Table 7
Differences in the Assessment of the Two Groups of Respondents on Public Trust and Collaboration

Indicator	Group	Mean	t	Sig.	Decision on Ho	Interpretation
Mutual Trust	Police Personnel Community Residents	3.39 3.24	6.391	.013	Rejected	Significant
Open Dialogue	Police Personnel Community Residents	3.09 3.50	13.565	.000	Rejected	Significant
Shared Responsibility	Police Personnel Community Residents Police Personnel Community Residents	3.07 2.91	.336	.563	Accepted	Not Significant
Transparent Processes	Police Personnel Community Residents	3.10 3.15	.057	.812	Accepted	Not Significant
Overall	Police Personnel Community Residents	3.16 3.20	1.808	.181	Accepted	Not Significant

The results for open dialogue are particularly striking. Community residents reported a notably higher mean (3.50) than police personnel (3.09), and the t-test yielded a value of 13.565 with a p-value of 0.000. This highly significant result indicates a clear disparity in the perceived openness of communication. Community residents appear to value or perceive more opportunities for communication than the police recognize providing, or police may underestimate the extent to which dialogue is occurring and being received by the public. This disconnect is critical, as it implies that while mechanisms for communication may be in place, they are not equally acknowledged or appreciated by both groups.

In contrast, no significant differences were found in the dimensions of shared responsibility and transparent processes, with p-values of 0.563 and 0.812 respectively. This suggests that both police and community members share similar views about the extent to which responsibilities are shared and processes are transparent. The means for shared responsibility were close—3.07 for police and 2.91 for residents—indicating moderate agreement. Likewise, both groups rated transparency similarly, with a mean of 3.10 for police and 3.15 for residents. These findings suggest that when it comes to procedural fairness and shared obligations, perceptions are relatively aligned.

The overall mean comparison yielded 3.16 for police and 3.20 for community residents, with a p-value of 0.181. The difference was not statistically significant, indicating that despite variation in specific areas, the general sentiment regarding public trust and collaboration is relatively similar between the two groups. However, the significant differences in mutual trust and open dialogue underscore the need for improved alignment in expectations and evaluations of trust-building strategies and communication platforms.

In summary, while there is general agreement between police personnel and community residents on shared responsibility and transparency, there are notable perceptual gaps in mutual trust and especially in open dialogue. Bridging these gaps is essential for advancing holistic community-police collaboration in addressing cybercrime effectively.

Table 8

Differences in the Assessment of Respondents on Public Trust and Collaboration in Terms of Sex

Indicator	Sex	Mean	F	Sig.	Decision on Ho	Interpretation
Mutual Trust	Male Female	3.30 3.33	4.726	.032	Rejected	Significant
Open Dialogue	Male Female	3.32 3.34	3.438	.066	Accepted	Not Significant
Shared Responsibility	Male Female	2.96 2.99	4.209	.042	Rejected	Significant
Transparent Processes	Male Female	3.14 3.12	.032	.857	Accepted	Not Significant

Overall	Male Female	3.18 3.19	7.544	.007	Rejected	Significant

The assessment of public trust and collaboration according to sex reveals both significant and non-significant differences across the various indicators. For mutual trust, female respondents (mean = 3.33) scored slightly higher than males (mean = 3.30), and the F-value of 4.726 with a p-value of 0.032 indicates statistical significance. This suggests that female respondents may perceive greater trust between the police and community, or are more optimistic about the integrity and responsiveness of law enforcement in cybercrime contexts.

In terms of open dialogue, there was only a marginal difference in mean scores between males (3.32) and females (3.34), and the resulting p-value of 0.066 leads to an acceptance of the null hypothesis. This indicates that both sexes perceive the level of dialogue and communication with law enforcement similarly. While the difference is negligible, it still reflects a consistently favorable view of open communication from both male and female respondents.

Significant differences were observed in shared responsibility, where female respondents (mean = 2.99) rated this construct slightly higher than males (mean = 2.96), with an F-value of 4.209 and a p-value of 0.042. Though the mean difference is small, the statistical significance implies that female respondents may be more inclined to acknowledge their own role or the community's role in cybercrime prevention efforts. It is possible that female respondents are more engaged or willing to participate in civic initiatives related to cybersecurity education or community policing.

Regarding transparent processes, the mean scores for males (3.14) and females (3.12) were nearly identical, and the F-value of 0.032 with a high p-value of 0.857 confirms there is no significant difference in this domain. This consistency suggests a shared understanding across genders about the transparency of the PNP's actions, especially in communicating procedures and updates on cybercrime.

Finally, the overall mean was slightly higher for females (3.19) than males (3.18), and the difference was statistically significant ($F = 7.544$, $p = 0.007$). This indicates that females, on average, hold a more favorable view of public trust and collaboration with the PNP-ACG. Such findings can guide future gender-sensitive programs that recognize and build upon women's openness to collaborative safety initiatives.

Overall, the data reveal that while both males and females largely share similar views, female respondents consistently rate trust and shared responsibility slightly higher, leading to statistically significant differences. This opens possibilities for gender-specific engagement strategies to sustain and improve civic-police cooperation.

Table 9 examining how perceptions vary by age group, the data from Table 9 reveal several significant differences. For mutual trust, the highest means were reported by those aged 65 and above (3.59) and 46–55 (3.54), whereas the lowest was from the 36–45 age group (3.04). The analysis yielded an F-value of 9.217 with a p-value of 0.000, indicating a significant difference. These results suggest that older respondents have greater trust in the police-community relationship than middle-aged groups, which may be attributed to generational perspectives on authority and traditional respect for law enforcement. The younger groups—those below 25 and aged 25–35—reported moderate scores (3.24 and 3.29), suggesting that trust increases with age, possibly due to accumulated interactions or expectations.

Table 9
Differences in the Assessment of Respondents on Public Trust and Collaboration in Terms of Age

Indicator	Age	Mean	F	Sig.	Decision on Ho	Interpret a-tion
Mutual Trust	Below 25 25-35 36-45 46-55 55-65 65 above	3.24 3.29 3.04 3.54 3.38 3.59	9.217	.000	Rejected	Significant
Open Dialogue	Below 25 25-35 36-45 46-55 55-65 65 above	3.3 3.37 3.34 3.32 3.39 3.19	.610	.692	Accepted	Not Significant
Shared Responsibility	Below 25 25-35 36-45 46-55 55-65 65 above	2.98 3.11 2.87 3.04 2.93 3.04	2.286	.051	Accepted	Not Significant
Transparent Processes	Below 25 25-35 36-45 46-55 55-65 65 above	3.11 2.95 3.08 3.25 3.18 3.23	3.137	.011	Rejected	Significant
Overall	Below 25 25-35 36-45 46-55 55-65 65 above	3.16 3.18 3.08 3.29 3.22 3.26	7.457	.000	Rejected	Significant

For open dialogue, the differences among age groups were not statistically significant (p = 0.692), as indicated by the close clustering of mean scores across the spectrum (ranging from 3.19 to 3.39). This suggests a uniform perception of communication effectiveness with the PNP-ACG regardless of age. All age groups moderately agree that dialogue is evident, reflecting widespread access or exposure to communication platforms, whether traditional or digital.

Regarding shared responsibility, no significant difference was observed (p = 0.051), although this value approaches the margin of significance. The 25–35 age group recorded the highest mean (3.11), while

the 36–45 group reported the lowest (2.87). The data suggest that younger adults might feel more responsibility for cybercrime prevention than their middle-aged counterparts, who may be more detached from digital initiatives or feel overburdened by other responsibilities.

A significant difference was observed in transparent processes, with a p-value of 0.011. The 46–55 (3.25) and 65+ (3.23) groups perceived the highest levels of transparency, while the 25–35 group reported the lowest (2.95). These findings echo those of mutual trust, again indicating that older adults tend to express higher confidence in police processes. The difference may be related to expectations and communication styles that resonate more with older individuals.

The overall assessment also showed significant variation by age (p = 0.000), with the 46–55 (3.29) and 65+ (3.26) groups expressing the most positive overall views. In contrast, the lowest rating came from the 36–45 group (3.08), who consistently rated constructs lower across multiple indicators. This trend suggests that mid-life adults are more critical of public trust and collaboration measures, possibly due to increased exposure to systems inefficiencies or higher expectations for accountability.

In conclusion, age plays a significant role in shaping perceptions of mutual trust, transparency, and overall collaboration. Younger and older groups generally report more favorable views, while middle-aged respondents show more skepticism. Policymakers and law enforcement agencies may use this insight to design age-specific engagement and communication strategies to close the perceptual gap and foster cross-generational collaboration.

Table 10

Differences in the Assessment of Respondents on Public Trust and Collaboration in Terms of Highest Educational Attainment

Indicator	Highest Educational Attainment	**Mean**	**F**	**Sig.**	**Decision on Ho**	**Interpretation**
Mutual Trust	High School Vocational Bachelor's Postgraduate	3.43 3.10 3.38 3.32	5.694	.001	Rejected	Significant
Open Dialogue	High School Vocational Bachelor's Postgraduate	3.45 3.5 3.26 3.23	5.163	.002	Rejected	Significant
Shared Responsibility	High School Vocational Bachelor's Postgraduate	2.94 2.87 3.04 2.98	2.482	.064	Accepted	Not Significant
Transparent Processes	High School Vocational Bachelor's Postgraduate	3.18 3.12 3.11 3.15	.312	.817	Accepted	Not Significant
Overall	High School Vocational Bachelor's	3.25 3.15 3.20	1.992	.119	Accepted	Not Significant

	Postgraduate	3.17				

The results of Table 10 examine whether educational attainment influences how respondents perceive public trust and collaboration with the Philippine National Police Anti-Cybercrime Group (PNP-ACG). The findings demonstrate that educational attainment significantly affects two key dimensions—mutual trust and open dialogue—while no significant differences were found in shared responsibility, transparency, or overall assessments.

For the mutual trust construct, the highest mean was recorded among high school graduates (3.43), followed by bachelor's degree holders (3.38), postgraduate respondents (3.32), and those with vocational training (3.10). The F-value of 5.694 and the corresponding p-value of 0.001 indicate a statistically significant difference among the groups. Interestingly, trust was highest among those with lower formal education levels. This finding could suggest that respondents with less academic exposure may be more inclined to defer to authority or hold more favorable assumptions about institutional integrity. On the other hand, respondents with vocational, bachelor's, and postgraduate degrees may be more critical or evaluative in their trust assessments, possibly due to increased awareness of governance issues, digital policy, or past experiences with law enforcement institutions.

A similar pattern emerges under the open dialogue dimension, which also showed a significant difference ($F = 5.163$, $p = 0.002$). Vocational graduates scored the highest (3.50), followed closely by high school graduates (3.45). In contrast, those with bachelor's (3.26) and postgraduate (3.23) degrees rated this dimension notably lower. This inverse trend relative to educational attainment indicates that while the less formally educated perceive dialogue to be open and accessible, the more educated respondents may have higher expectations for quality, inclusivity, or technical responsiveness in police communication. The gap in perception could reflect differences in communication preferences, familiarity with digital platforms, or critical engagement levels with public services.

In contrast, shared responsibility did not yield a significant difference across educational groups ($p = 0.064$), although some variation in mean scores was still observed. Bachelor's degree holders registered the highest mean (3.04), suggesting a relatively greater recognition of community roles in cybercrime prevention. Meanwhile, vocational respondents scored the lowest (2.87). Despite the statistical insignificance, the data hint that those with more formal education may be more willing to acknowledge their role in cybercrime mitigation or understand the distributed nature of cybersecurity responsibilities.

The dimension of transparent processes showed almost no difference across educational backgrounds, with all means tightly clustered between 3.11 and 3.18. The highest score was noted among high school graduates (3.18), and the lowest from bachelor's degree holders (3.11), but the F-value of 0.312 and p-value of 0.817 confirmed the absence of a statistically meaningful difference. This uniformity indicates that respondents across educational levels share relatively similar views regarding the transparency of police procedures and communication in managing cybercrime, which may point to a universally visible set of practices adopted by the PNP-ACG.

For the overall assessment, high school graduates again recorded the highest mean score (3.25), with bachelor's and postgraduate respondents scoring slightly lower at 3.20 and 3.17 respectively. However, the F-value of 1.992 and p-value of 0.119 resulted in the acceptance of the null hypothesis, indicating that educational attainment does not significantly impact the general perception of trust and

collaboration. This finding underscores a convergence of opinion across all groups when considering the totality of dimensions involved.

In conclusion, while mutual trust and perceptions of open dialogue are significantly influenced by respondents' educational backgrounds—with lower-educated respondents rating these dimensions more favorably—there is general uniformity in the assessments of shared responsibility, transparency, and overall collaboration. The results suggest that more educated individuals may possess more critical, perhaps nuanced views regarding institutional performance, while less educated respondents may rely more on personal interactions and general impressions. These findings highlight the importance of tailoring communication and engagement strategies according to the educational profile of the target audience, ensuring inclusivity and mutual understanding in cybercrime prevention efforts.

4. ON THE ASSESSMENT OF RESPONDENTS ON THE PNP'S CYBERCRIME PREVENTION INITIATIVES IN TERMS OF THE ONLINE SAFETY AWARENESS, CYBERCRIME REPORTING, VICTIM SUPPORT, AND COMMUNITY-LED DIGITAL LITERACY PROGRAMS.

Table 11

Assessment of Respondents on the Assessment of Respondents on the PNP's Cybercrime Prevention Initiatives in terms of Online Safety Awareness

Indicator	WM	SD	QD	VI
The PNP-ACG regularly conducts educational campaigns to raise awareness on safe internet practices	2.84	0.92	Agree	Evident
I have learned important online safety tips from the programs or materials provided by the police	3.39	0.78	Agree	Evident
The PNP collaborates with schools and community groups to promote responsible internet use	3.39	0.8	Agree	Evident
The community is more aware of cyber threats today due to the efforts of the PNP-ACG	3.11	0.91	Agree	Evident
The online safety materials distributed by the PNP are easy to understand and practical	3.24	0.84	Agree	Evident
The PNP effectively uses social media and other platforms to inform the public about cybercrime risks	3.14	0.86	Agree	Evident
The PNP's efforts in promoting online safety have increased my confidence in using the internet securely	3.43	0.72	Agree	Evident
Overall Mean	3.22	0.36	Agree	Evident

Legend: 3.51 – 4.00 (Strongly Agree-Highly Evident); 2.51 – 3.50 (Agree- Evident); 1.51 – 2.50 (Disagree-Slightly Evident); 1.0-1.50 (Strongly Disagree-Not Evident)

The overall mean of 3.22, with a standard deviation of 0.36, reveals that respondents agree the PNP-ACG's initiatives on online safety awareness are evident and positively perceived. The dimension remains within the "Agree" bracket, suggesting that while the efforts are acknowledged, there remains room for enhanced intensity, consistency, and reach. The moderate standard deviation reflects relatively consistent responses across indicators.

The highest-rated item, "The PNP's efforts in promoting online safety have increased my confidence in using the internet securely," obtained a weighted mean of 3.43. This is a strong result, suggesting that these initiatives have a tangible effect on individuals' sense of digital security. Close to this are two items—"I have learned important online safety tips from the programs or materials provided by the police" and "The PNP collaborates with schools and community groups to promote responsible internet use"—both scoring 3.39. These data points illustrate the dual impact of educational content and collaborative outreach on enhancing digital literacy.

The lowest-rated item, "The PNP-ACG regularly conducts educational campaigns to raise awareness on safe internet practices," received a mean of 2.84. This score, though still within the "Agree" category, suggests that the frequency or visibility of campaigns may be limited or inconsistent. Respondents might be unaware of ongoing initiatives, or the delivery mechanisms may not sufficiently penetrate communities. Similarly, "The PNP effectively uses social media and other platforms to inform the public about cybercrime risks" scored only 3.14, which may indicate a need for improved digital engagement strategies, particularly on platforms where citizens seek real-time and accessible information.

In summary, while the PNP-ACG's efforts in online safety are positively received—particularly in outcomes like user confidence and collaboration—the perceived infrequency or limited reach of campaigns remains a concern. Strengthening visibility and innovating delivery platforms may increase community penetration and improve overall awareness.

Table 12
Assessment of Respondents on the Assessment of Respondents on the PNP's Cybercrime Prevention Initiatives in terms of
Cybercrime Reporting

Indicator	WM	SD	QD	VI	
There are clear procedures established by the PNP-ACG for reporting cybercrime incidents	3.18	0.74	Agree	Evident	2
I know where and how to report a cybercrime if I encounter one	3.05	0.77	Agree	Evident	5

The reporting platforms provided by the PNP (e.g., website, hotline, walk-in) are accessible and user-friendly	2.97	0.73	Agree	Evident	6
The PNP responds promptly and professionally to reported cybercrime cases	3.19	0.9	Agree	Evident	1
Reporting cybercrimes to the police does not require complicated or time-consuming steps	3.09	0.84	Agree	Evident	3
The PNP encourages the public to report all types of cybercrime, regardless of severity	2.95	0.84	Agree	Evident	7
I feel safe and protected when I report a cybercrime to the authorities	3.06	0.84	Agree	Evident	4
Overall Mean	3.07	0.35	Agree	Evident	

Legend : 3.51 – 4.00 (Strongly Agree-Highly Evident); 2.51 – 3.50 (Agree- Evident); 1.51 – 2.50 (Disagree-Slightly Evident); 1.0-1.50 (Strongly Disagree-Not Evident)

The overall mean of 3.07 indicates that respondents perceive the cybercrime reporting mechanisms of the PNP-ACG as evident and moderately effective. This score confirms that while the public recognizes the infrastructure for reporting, the process is still in need of optimization to achieve full efficiency and accessibility. A standard deviation of 0.35 indicates moderate variability in responses, suggesting some disparities in user experience.

Among the indicators, the highest-rated statement was “The PNP responds promptly and professionally to reported cybercrime cases,” with a mean of 3.19. This reflects public confidence in the quality of service during the post-reporting phase. “There are clear procedures established by the PNP-ACG for reporting cybercrime incidents” also received a favorable score (3.18), indicating that the presence of reporting frameworks is appreciated.

On the lower end, “The PNP encourages the public to report all types of cybercrime, regardless of severity” garnered the lowest score (2.95). This suggests either a lack of public awareness of inclusive reporting encouragement or the perception that minor cases are not prioritized. Furthermore, “The reporting platforms provided by the PNP (e.g., website, hotline, walk-in) are accessible and user-friendly” scored only 2.97, highlighting a critical area for improvement in user interface, platform accessibility, or public familiarity.

The data underscore a working but underutilized system of cybercrime reporting. While professionalism in response is evident, broader public awareness and simplification of processes are needed to increase reporting rates. Community education

on where and how to report, as well as assurance of a non-intimidating experience, will be essential in strengthening this dimension.

Table 13
Assessment of Respondents on the Assessment of Respondents on the PNP's Cybercrime Prevention Initiatives in terms of Victim Support

Indicator	WM	SD	QD	VI	Rank
The PNP provides appropriate assistance to victims of cybercrime, including guidance on legal actions	3.78	0.54	Strongly Agree	Highly Evident	1
Victims of cybercrime receive timely updates regarding the progress of their cases	3.73	0.55	Strongly Agree	Highly Evident	2
Support services, such as counseling or referrals, are made available to cybercrime victims by the PNP or its partner agencies	3.02	0.87	Agree	Evident	6
The PNP ensures the privacy and protection of individuals who report being victimized online	3.38	0.58	Agree	Evident	5
Victims are treated with empathy, respect, and professionalism by responding officers	3.41	0.7	Agree	Evident	4
I am aware of specific programs or services offered by the PNP to support cybercrime victims	3.61	0.75	Strongly Agree	Highly Evident	3
The PNP has mechanisms in place to prevent secondary victimization or re-traumatization during the investigation process	2.97	0.72	Agree	Evident	7
Overall Mean	3.41	0.31	Agree	Evident	

Legend: 3.51 – 4.00 (Strongly Agree-Highly Evident); 2.51 – 3.50 (Agree- Evident); 1.51 – 2.50 (Disagree-Slightly Evident); 1.0-1.50 (Strongly Disagree-Not Evident)

The victim support component received an overall mean of 3.41, the highest among all dimensions assessed in the cybercrime prevention initiatives. This result suggests that respondents generally believe the PNP-ACG performs well in handling victims of cybercrime, with support mechanisms being both available and appreciated. A relatively low standard deviation of 0.31 indicates strong consistency in responses.

The highest-rated indicators were "The PNP provides appropriate assistance to victims of cybercrime, including guidance on legal actions" (3.78) and "Victims of

cybercrime receive timely updates regarding the progress of their cases" (3.73). Both fall in the "Strongly Agree" range, signifying not only procedural effectiveness but also timely case management. In addition, awareness of specific programs ("I am aware of specific programs or services offered by the PNP to support cybercrime victims") scored 3.61, suggesting relatively successful public dissemination of victim services.

Despite these strong points, areas for development remain. The item "The PNP has mechanisms in place to prevent secondary victimization or re-traumatization during the investigation process" received the lowest score in this table (2.97). This indicates a potential gap in trauma-informed investigative practices or protective measures during follow-up actions. Similarly, "Support services, such as counseling or referrals, are made available to cybercrime victims" rated at 3.02, suggesting that while assistance is available, it may not be widely implemented or consistently experienced.

Overall, the victim support system under the PNP-ACG is considered effective, especially in terms of legal guidance, updates, and professionalism. However, psychological safety, specialized services, and holistic victim care should be prioritized to make the system more comprehensive and empathetic.

Table 14
Assessment of Respondents on the Assessment of Respondents on the PNP's Cybercrime Prevention Initiatives in terms of
Community-Led Digital Literacy Programs

Indicator	WM	SD	QD	VI	Rank
The PNP collaborates with schools, barangays, and NGOs in organizing digital literacy activities	2.97	0.85	Agree	Evident	6
There are community-initiated programs in our area that teach safe internet use and online responsibility	2.82	0.76	Agree	Evident	7
I have participated in a local digital literacy seminar or campaign supported by the PNP-ACG.	3.31	0.84	Agree	Evident	1.5
Community-led efforts to promote digital safety are effective in helping residents prevent cybercrime	3.19	0.85	Agree	Evident	5
The PNP supports grassroots initiatives that aim to educate vulnerable groups (e.g., youth, elderly) about cyber threats	3.23	0.79	Agree	Evident	4
Digital literacy programs in our locality are accessible and inclusive to all sectors of the community	3.24	0.77	Agree	Evident	3

There is strong collaboration between the PNP and the community in planning and implementing digital literacy initiatives	3.31	0.94	Agree	Evident	1.5
Overall Mean	3.15	0.5	Agree	Evident	

Legend: 3.51 – 4.00 (Strongly Agree-Highly Evident); 2.51 – 3.50 (Agree- Evident); 1.51 – 2.50 (Disagree-Slightly Evident); 1.0-1.50 (Strongly Disagree-Not Evident)

The dimension of community-led digital literacy programs obtained an overall mean of 3.15, interpreted as "Agree" and "Evident." A higher standard deviation of 0.50 reflects greater variation in responses, indicating that access to and participation in these programs may differ significantly across localities.

The items with the highest mean scores were "There is strong collaboration between the PNP and the community in planning and implementing digital literacy initiatives" and "I have participated in a local digital literacy seminar or campaign supported by the PNP-ACG," both scoring 3.31. These responses affirm that respondents have seen or directly experienced co-led initiatives, indicating the program's reach and relevance.

In contrast, the lowest-rated item, "There are community-initiated programs in our area that teach safe internet use and online responsibility," received a mean of 2.82. This may imply a limited presence of grassroots digital literacy efforts, or that such programs exist but lack visibility or sustainability. Similarly, collaboration with schools and NGOs scored 2.97, reflecting moderate approval and suggesting opportunities for deeper institutional partnerships.

These results point to a need for expanding and institutionalizing digital literacy programs through community empowerment. The PNP may consider capacity-building efforts for local actors to initiate and sustain digital safety education, particularly for vulnerable groups. While the intent and support for such initiatives are evident, their reach and consistency across regions must be addressed.

Table 15
Summary on the Assessment of Respondents on the Assessment of Respondents on the PNP's Cybercrime Prevention Initiatives

Indicator	Weighted Mean	Standard Deviation	Qualitative Description	Verbal Interpretation	Rank
1. Online Safety Awareness	3.22	0.36	Agree	Evident	2
2. Cybercrime Reporting	3.07	0.35	Agree	Evident	4

3. Victim Support	3.41	0.31	Agree	Evident	1
4. Community-Led Digital Literacy Programs	3.15	0.5	Agree	Evident	3
Overall Mean	3.21	0.19	Agree	Evident	

Legend: 3.51 – 4.00 (Strongly Agree-Highly Evident); 2.51 – 3.50 (Agree- Evident); 1.51 – 2.50 (Disagree-Slightly Evident); 1.0-1.50 (Strongly Disagree-Not Evident)

The overall mean of 3.21 for all four dimensions indicates that the PNP-ACG's cybercrime prevention initiatives are generally effective and visible, though not strongly exemplary. The respondents "Agree" that these efforts are evident, supported by a low standard deviation of 0.19, indicating consistency in perceptions across initiatives.

Among all dimensions, victim support achieved the highest rating with a mean of 3.41. This suggests that direct services offered to individuals affected by cybercrime—such as legal guidance, case updates, and respectful treatment—are the strongest aspects of the PNP's cybercrime prevention framework. This dimension's strength lies in its visible and immediate impact on individuals, creating confidence in institutional responsiveness.

Online safety awareness was also rated favorably with a mean of 3.22. Respondents appreciate the educational value and the outcomes these programs have on internet usage behavior. However, concerns remain regarding the frequency and visibility of campaigns. These initiatives should be bolstered through more innovative platforms, particularly in low-access areas.

Community-led digital literacy programs and cybercrime reporting received the lowest means, at 3.15 and 3.07, respectively. The weaker ratings in these areas highlight systemic gaps in localized engagement and reporting infrastructure. Both dimensions reveal an opportunity for the PNP to reinforce community participation, build awareness of reporting channels, and improve reporting efficiency.

In conclusion, the PNP-ACG is perceived to be performing commendably in victim support and online safety education, while needing to enhance grassroots engagement and streamline reporting procedures. These findings serve as a strategic guide for prioritizing resource allocation, refining communication strategies, and fostering sustained community collaboration in the fight against cybercrime.

5. ON THE SIGNIFICANT DIFFERENCE IN THE ASSESSMENT OF RESPONDENTS ON THE PNP'S CYBERCRIME PREVENTION INITIATIVES WHEN THEIR PROFILE IS TAKEN AS TEST FACTOR

Table 16

Differences in the Assessment of the Two Groups of Respondents on the PNP's Cybercrime Prevention Initiatives

Indicator	Group	Mean	t	Sig.	Decision on Ho	Interpretation

Online Safety Awareness	Police Personnel Community Residents	3.38 3.10	3.260	.074	Accepted	Not Significant
Cybercrime Reporting	Police Personnel Community Residents	3.15 3.01	2.917	.090	Accepted	Not Significant
Victim Support	Police Personnel Community Residents Police Personnel Community Residents	3.35 3.46	3.405	.068	Accepted	Not Significant
Community-Led Digital Literacy Programs	Police Personnel Community Residents	3.55 2.86	24.196	.000	Rejected	Significant
Overall	Police Personnel Community Residents	3.36 3.11	.028	.866	Accepted	Not Significant

The results of Table 16 explore the perceptual differences between police personnel and community residents regarding the PNP's cybercrime prevention initiatives. In most indicators, the null hypothesis was accepted, indicating no statistically significant difference. This suggests a general consensus between the two groups in their evaluations. However, one area—Community-Led Digital Literacy Programs—showed a significant discrepancy.

The only statistically significant result was found in the assessment of community-led digital literacy programs, where police personnel reported a much higher mean (3.55) compared to community residents (2.86), with a t-value of 24.196 and a significance level of 0.000. This large gap and highly significant result suggest that police officers perceive much more robust collaboration and implementation of community-based digital literacy efforts than what is experienced or observed by community members. This disparity may point to a communication gap, limited visibility of initiatives, or overestimation by the police of their impact or reach in local communities.

On other indicators such as Online Safety Awareness (means: 3.38 for police and 3.10 for residents), Cybercrime Reporting (3.15 and 3.01), and Victim Support (3.35 and 3.46), the results were not statistically significant, with p-values of 0.074, 0.090, and 0.068, respectively. Although there are slight differences in means, they do not reflect a significant divide. Interestingly, community residents scored higher in victim support, which may reflect more direct or recent experiences with services provided, while police scored higher in awareness and reporting, possibly due to their direct involvement in program delivery.

The overall mean ratings—3.36 for police and 3.11 for residents—were also not statistically different (p = 0.866), suggesting that despite differing perspectives in specific areas, both groups share a generally favorable view of the PNP's cybercrime prevention efforts. The significance of community-led initiatives, however, points to the need for better coordination and communication to bridge this perceptual divide.

Table 17

Differences in the Assessment of Respondents on the PNP's Cybercrime Prevention Initiatives in Terms of Sex

Indicator	Sex	**Mean**	**t**	**Sig.**	**Decision on Ho**	**Interpretation**
Online Safety Awareness	Male Female	3.19 3.28	9.420	.003	Rejected	Significant
Cybercrime Reporting	Male Female	3.05 3.11	.493	.484	Accepted	Not Significant
Victim Support	Male Female	3.39 3.46	.035	.853	Accepted	Not Significant
Community-Led Digital Literacy Programs	Male Female	3.15 3.15	.409	.524	Accepted	Not Significant
Overall	Male Female	3.19 3.25	.652	.421	Accepted	Not Significant

Table 17 presents the gender-based analysis of respondents' assessments. The most notable finding is in the dimension of Online Safety Awareness, where female respondents rated this area significantly higher (mean = 3.28) than their male counterparts (mean = 3.19), with a significant t-value of 9.420 and a p-value of 0.003. This indicates a meaningful difference in perception, suggesting that female respondents may be more responsive to or appreciative of safety messaging and digital education campaigns.

For the other three areas—Cybercrime Reporting, Victim Support, and Community-Led Digital Literacy Programs—the differences between male and female respondents were not statistically significant. Mean scores were close for each group, particularly in Cybercrime Reporting (3.05 for males

and 3.11 for females) and Community-Led Programs (3.15 for both). These results suggest a shared understanding of the effectiveness and availability of these services, irrespective of gender.

The overall mean was slightly higher for female respondents (3.25) than for males (3.19), though the difference was not statistically significant (p = 0.421). In general, while both male and female respondents agree on the relevance of PNP initiatives, females appear slightly more favorable in terms of safety awareness—perhaps reflecting differing risk perceptions or digital behavior patterns between genders.

Table 18

Differences in the Assessment of Respondents on the PNP's Cybercrime Prevention Initiatives in Terms of Age

Indicator	Age	Mean	F	Sig.	Decision on Ho	Interpretation
Online Safety Awareness	Below 25 25-35 36-45 46-55 55-65 65 above	3.11 3.21 3.05 3.40 3.25 3.51	4.537	.001	Rejected	Significant
Cybercrime Reporting	Below 25 25-35 36-45 46-55 55-65 65 above	3.14 3.09 3.13 3.05 2.99 2.97	.803	.549	Accepted	Not Significant
Victim Support	Below 25 25-35 36-45 46-55 55-65 65 above	3.36 3.44 3.48 3.53 3.29 3.47	1.974	.088	Accepted	Not Significant
Community-Led Digital Literacy Programs	Below 25 25-35 36-45 46-55 55-65 65 above	3.14 3.15 3.19 3.03 3.21 3.14	.294	.915	Accepted	Not Significant
Overall	Below 25 25-35 36-45 46-55 55-65 65 above	3.19 3.22 3.21 3.25 3.18 3.28	.589	.709	Accepted	Not Significant

Table 18 shows how age influences respondents' perceptions of the PNP's cybercrime prevention efforts. Only Online Safety Awareness shows a statistically significant difference, with an F-value of 4.537 and a p-value of 0.001. The highest ratings were from the oldest age group (65 and above, mean = 3.51), followed by those aged 46–55 (mean = 3.40). The lowest rating was from the 36–45 group (mean = 3.05). These findings suggest that older respondents feel more positively about safety initiatives—possibly due to the novelty or perceived usefulness of such interventions for older, less digitally native individuals.

For Cybercrime Reporting, Victim Support, and Community-Led Digital Literacy Programs, there were no significant differences. Mean scores across age groups were relatively close, particularly for reporting, where scores ranged narrowly from 2.97 to 3.14. These results suggest that access to reporting mechanisms and victim services is consistently perceived across age demographics.

While not statistically significant, the overall mean gradually increased with age, from 3.19 (below 25) to 3.28 (65 and above). This upward trend reflects a general pattern where older individuals may be more appreciative or trusting of institutional interventions. This suggests a need for targeted efforts to better engage middle-aged and younger demographics who may hold more critical or less involved views regarding government-led initiatives.

Table 19
Differences in the Assessment of Respondents on the PNP's Cybercrime Prevention Initiatives in Terms of Highest Educational Attainment

Indicator	Highest Educational Attainment	Mean	F	Sig.	Decision on Ho	Interpretation
Online Safety Awareness	High School Vocational Bachelor's Postgraduate	3.27 2.98 3.30 3.29	6.332	.001	Rejected	Significant
Cybercrime Reporting	High School Vocational Bachelor's Postgraduate	3.06 2.98 3.17 2.96	3.169	.027	Rejected	Significant
Victim Support	High School Vocational Bachelor's	3.45 3.49 3.35 3.45	1.491	.221	Accepted	Not Significant

	Postgraduate					
Community-Led Digital Literacy Programs	High School Vocational Bachelor's Postgraduate	2.91 2.82 3.26 3.42	11.029	.000	Rejected	Significant
Overall	High School Vocational Bachelor's Postgraduate	3.17 3.07 3.27 3.28	10.135	.000	Rejected	Significant

Table 19 reveals several statistically significant differences across levels of educational attainment. Notably, the Online Safety Awareness dimension shows a significant difference ($F = 6.332$, $p = 0.001$), with bachelor's (3.30) and postgraduate (3.29) degree holders reporting higher levels of awareness than vocational graduates (2.98). This may indicate that higher education correlates with increased exposure to or appreciation of digital safety initiatives. Similarly, Cybercrime Reporting also shows significant variation ($F = 3.169$, $p = 0.027$), with bachelor's degree holders again giving the highest ratings (3.17), suggesting that education enhances one's capacity to navigate reporting systems.

For Community-Led Digital Literacy Programs, the differences are even more pronounced ($F = 11.029$, $p = 0.000$). Postgraduate respondents gave the highest score (3.42), while vocational respondents provided the lowest (2.82). This pattern may stem from varying levels of engagement or awareness across education levels. Those with higher academic attainment may be more likely to participate in or lead community initiatives, thus giving higher ratings.

Though Victim Support did not yield statistically significant differences ($p = 0.221$), all educational groups reported generally high scores, indicating uniform satisfaction with services. In terms of overall assessment, the result was significant ($F = 10.135$, $p = 0.000$), with postgraduate (3.28) and bachelor's degree holders (3.27) again giving more favorable ratings compared to vocational graduates (3.07).

These findings imply that education shapes awareness, accessibility, and appreciation of the PNP's initiatives. Those with higher educational attainment may be more informed, more engaged, or more capable of interacting with digital systems, which positively influences their perceptions. Thus, tailoring educational campaigns to less formally educated sectors may help close perceptual and participatory gaps.

6. ON THE SIGNIFICANT RELATIONSHIP IN THE ASSESSMENT OF RESPONDENTS BETWEEN THE PUBLIC TRUST AND COLLABORATION AND THE PNP'S CYBERCRIME PREVENTION INITIATIVES

Table 20

Correlation Between Assessment of Respondents Between the Public Trust and Collaboration and the PNP's Cybercrime Prevention Initiatives

Public Trust and Collaboration	PNP's Cybercrime Prevention Initiatives	Computed r	Sig.	Decision	Interpretation
Mutual Trust	Online Safety Awareness	.860**	.000	Rejected	Significant
	Cybercrime Reporting	-.014	.878	Accepted	Not Significant
	Victim Support	-.286**	.002	Rejected	Significant
	Community-Led Digital Literacy Programs	.143	.119	Accepted	Not Significant
Open Dialogue	Online Safety Awareness	-.238**	.009	Rejected	Significant
	Cybercrime Reporting	-.135	.142	Accepted	Not Significant
	Victim Support	-.124	.178	Accepted	Not Significant
	Community-Led Digital Literacy Programs	-.449**	.000	Rejected	Significant
Shared Responsibility	Online Safety Awareness	.078	.398	Accepted	Not Significant
	Cybercrime Reporting	.269**	.003	Rejected	Significant
	Victim Support	.046	.621	Accepted	Not Significant
	Community-Led Digital Literacy Programs	.189*	.039		
Transparent Processes	Online Safety Awareness	-.096	.295	Accepted	Not Significant
	Cybercrime Reporting	.066	.471	Accepted	Not Significant
	Victim Support	.154	.093	Accepted	Not Significant

	Community-Led Digital Literacy Programs	.044	.630	Accepted	Not Significant
Overall Public Trust and Collaboration	**Overall PNP's Cybercrime Prevention Initiatives**	.096	.295	Accepted	Not Significant

Table 20 presents a correlational analysis to examine the relationships between components of public trust and collaboration and the PNP's cybercrime prevention initiatives. While some pairings revealed statistically significant relationships, the majority were found to be weak or non-significant. These findings indicate that although there is some overlap between trust dynamics and perceptions of cybercrime programs, they largely function as distinct evaluative constructs in the eyes of the respondents.

The most notable finding is the strong and significant positive correlation between Mutual Trust and Online Safety Awareness ($r = .860$, $p = .000$). This high correlation coefficient suggests that respondents who perceive a high level of mutual trust between the police and the community also have strong confidence in the PNP's online safety campaigns. This supports the view that trust and awareness are mutually reinforcing: the more the community trusts the integrity and intention of the PNP, the more they accept and internalize its educational efforts regarding cyber safety.

Conversely, a moderate negative correlation was found between Mutual Trust and Victim Support ($r = –.286$, $p = .002$), indicating that respondents who rated victim support services more favorably tended to give slightly lower ratings to mutual trust. This inverse relationship may reflect different experiential touchpoints—those who directly accessed victim support may have had satisfactory individual experiences but may still harbor doubts about broader community-level trust or structural integrity. It suggests the importance of distinguishing between personalized service satisfaction and systemic relational trust.

Another significant but negative correlation exists between Open Dialogue and Community-Led Digital Literacy Programs ($r = –.449$, $p = .000$). This implies that respondents who perceive open communication between the police and community to be strong may not see community-led literacy efforts as effective or visible. This disconnect may indicate that while institutional dialogue exists, it does not always translate into empowering communities to take ownership of digital safety initiatives. It also reflects a possible gap between top-down communication efforts and grassroots mobilization.

Interestingly, Open Dialogue was also negatively correlated with Online Safety Awareness (r = –.238, p = .009), which could suggest a perceived over-reliance on police-initiated communication rather than mutual, participatory dialogue. Respondents who are aware of PNP-led safety programs may feel less agency in initiating discussions or expressing concerns, resulting in lower dialogue scores.

On the other hand, Shared Responsibility exhibited a positive and significant correlation with Cybercrime Reporting (r = .269, p = .003), suggesting that those who view cybercrime prevention as a shared duty are more likely to appreciate or engage with reporting mechanisms. There is also a weaker but statistically significant relationship between Shared Responsibility and Community-Led Digital Literacy Programs (r = .189, p = .039), indicating that civic engagement attitudes moderately influence support for grassroots education efforts.

Notably, Transparent Processes did not correlate significantly with any of the cybercrime prevention indicators. This suggests that perceptions of procedural transparency—such as due process, case updates, and public communication—are largely evaluated independently of the specific programmatic dimensions like awareness campaigns, victim support, or community initiatives. This finding calls for further inquiry into whether current transparency practices are too generic or detached from the preventive initiatives being deployed.

Lastly, the overall correlation between aggregated scores for Public Trust and Collaboration and Cybercrime Prevention Initiatives yielded an r-value of .096 with a p-value of .295, indicating a non-significant relationship. This means that while individual sub-dimensions may relate in specific contexts, public trust as a general perception does not strongly predict overall assessment of cybercrime prevention efforts. This could imply that trust-building and program evaluation are processed separately by respondents, highlighting the need for a more integrated and participatory approach to designing and evaluating digital security programs.

In summary, Table 20 reveals that while some specific correlations (such as between mutual trust and online safety awareness) are statistically significant, public trust and cybercrime prevention are largely perceived as independent constructs. The data suggest opportunities for the PNP to strengthen the alignment between its trust-building strategies and preventive initiatives by fostering participatory, community-anchored engagement models.

DISCUSSIONS

Summary of Findings

This following synthesizes the major findings of the study based on the profile of respondents, their assessment of public trust and collaboration with the PNP, the

differences in their perceptions, and their evaluation of the PNP's cybercrime prevention initiatives, including the statistical correlations between the two key constructs.

1. **Profile of the Respondents**. The study included 120 respondents composed of both police personnel (41.7%) and community residents (58.3%). Males (61.7%) outnumbered females (38.3%), with the majority falling within the 55–65 (22.5%) and 36–45 (21.7%) age brackets. The educational profile was generally high, with most having earned a bachelor's degree (43.3%) and a significant portion holding postgraduate degrees (21.7%). This demographic spread suggests a population capable of critical engagement and reflective assessment, ensuring diverse insights into cybercrime-related public trust issues. The mix of professional affiliation, age groups, and academic background helped balance institutional and civilian perspectives.

2. Assessment of Respondents on Public Trust and Collaboration. Respondents generally "agreed" that public trust and collaboration between the PNP and the community were evident, with the highest scores reported for open dialogue (M = 3.33) and mutual trust (M = 3.31). Transparent processes (M = 3.13) and shared responsibility (M = 2.97) received slightly lower, but still positive, assessments. Respondents highlighted strong communication lines and trust in police integrity, although community participation and shared accountability remain areas for further enhancement. The results affirm that while foundational trust and engagement are present, improvements are needed in creating balanced, reciprocal relationships, particularly in co-owned preventive strategies.

3. Differences in the Assessment of Respondents on Public Trust and Collaboration. Significant differences were observed between police personnel and community residents in terms of mutual trust and open dialogue, with police generally perceiving higher trust while community members reported more openness in communication. Gender-wise, females rated mutual trust and shared responsibility more favorably than males. Age significantly influenced perceptions of mutual trust and transparency, with older age groups (65 and above) providing the highest ratings. Educational attainment also played a role; those with lower education levels tended to perceive higher levels of mutual trust and dialogue. These results reflect differing lived experiences and expectations, emphasizing the need for more inclusive, adaptive strategies that resonate across demographic sectors.

4. Assessment of Respondents on the PNP's Cybercrime Prevention Initiatives. Overall, respondents agreed that the PNP's initiatives were evident and positively perceived, particularly in victim support (M = 3.41) and online safety awareness (M = 3.22). Initiatives in cybercrime reporting (M = 3.07) and community-led digital literacy programs (M = 3.15) were also rated favorably but suggest room for improvement, especially in community participation and ease of access to reporting mechanisms. Notably, the highest scores in victim support reflected confidence in legal guidance, case updates, and respectful treatment by authorities. However, grassroots involvement and digital outreach in underserved communities remain underdeveloped.

5. Differences in the Assessment of Respondents on the PNP's Cybercrime Prevention Initiatives. Statistically significant differences were found only in the dimension of community-led digital literacy programs, where police personnel gave much higher ratings than community residents. This signals a perceptual disconnect between implementers and recipients of community-based interventions. Differences by sex were minimal, except in online safety awareness where females gave significantly higher ratings. Age influenced perceptions of online safety awareness, with older respondents rating it more favorably. Education also influenced assessments, with bachelor's and postgraduate holders expressing greater appreciation for initiatives overall. These findings suggest that program visibility and accessibility must be enhanced, particularly for groups who perceive lower engagement or effectiveness.

6. Correlation Between Public Trust and PNP's Cybercrime Prevention Initiatives. Correlational analysis revealed a strong and significant relationship between mutual trust and online safety awareness ($r = .860$, $p = .000$), affirming that institutional trust amplifies the effectiveness of educational campaigns. Conversely, mutual trust was negatively correlated with victim support ($r = –.286$, $p = .002$), suggesting that personalized service experiences may not directly translate into systemic trust. Open dialogue was negatively associated with community-led digital literacy efforts ($r = –.449$, $p = .000$), indicating that communication does not necessarily result in grassroots mobilization. Shared responsibility showed modest but significant positive correlations with cybercrime reporting ($r = .269$) and digital literacy programs ($r = .189$), emphasizing the importance of civic engagement. The overall correlation between public trust and cybercrime initiatives, however, was not statistically significant, indicating that these constructs, while related in specific aspects, operate independently in the minds of the public. This highlights the need for integrative frameworks that explicitly connect trust-building strategies with cybercrime program outcomes.

Conclusion

1. The demographic profile of the respondents illustrates a mature, educated, and professionally diverse population composed of both institutional actors and community members. The balanced representation across sectors, age brackets, and educational attainment establishes a credible foundation for the assessment of public trust and perceptions regarding cybercrime prevention. This demographic composition ensures that the study reflects informed, multifaceted views that consider both policy implementation and lived community experiences.

2. The assessment of public trust and collaboration indicates that these constructs are generally evident in police-community relations. High ratings in mutual trust and open dialogue underscore the effectiveness of the PNP's integrity-based and communicative approaches. Nonetheless, areas such as shared responsibility and transparent processes require further strengthening. The findings point to the importance of enhancing participatory structures and ensuring that collaboration is not merely perceived but actively experienced by both police and citizens.

3. Differences in perception across demographic variables emphasize the nuanced nature of trust-building. Police personnel tend to rate trust and collaboration higher than community residents, while women, older individuals, and less formally educated respondents generally hold more favorable views. These disparities suggest the need for targeted strategies to address gaps in expectation and perception, especially among middle-aged, male, and highly educated groups, who appear more critical. Inclusive policy framing and differentiated engagement approaches may foster a more equitable trust environment.

4. With regard to the PNP's cybercrime prevention initiatives, overall assessments were favorable, particularly in victim support and online safety awareness. These findings indicate that the institution has made meaningful strides in service delivery and public education. However, lower ratings in cybercrime reporting and community-led digital literacy programs reveal limitations in reach, visibility, and grassroots participation. These dimensions must be enhanced through broader civic partnerships, streamlined platforms, and responsive program design.

5. Discrepancies in perceptions of cybercrime initiatives further reinforce the importance of aligning institutional delivery with community reception. The significant difference in ratings of community-led digital literacy efforts between police personnel and community residents reveals a misalignment in perceived impact and engagement. While demographic differences in other areas were largely not significant, recurring trends—such as more favorable ratings from women and older adults—underscore the necessity of demographic-sensitive programming and assessment.

6. The correlation results reveal that while certain dimensions of public trust—particularly mutual trust—positively influence perceptions of specific cybercrime initiatives like online safety awareness, the relationship between the two overarching constructs remains statistically weak. This suggests that trust and program effectiveness are not inherently interdependent in the public's perception. Hence, trust-building efforts should not be assumed to translate automatically into program acceptance or participation. An integrated framework that deliberately bridges institutional trust with program design, delivery, and evaluation is therefore necessary to create cohesive, effective, and sustainable cybercrime prevention strategies.

Recommendation

Based on the findings and conclusions of the study, the following recommendations are proposed to enhance public trust and strengthen the effectiveness of the Philippine National Police Anti-Cybercrime Group's (PNP-ACG) cybercrime prevention initiatives. These recommendations are structured according to the key thematic areas addressed in the study:

1. The PNP-ACG should intensify efforts to cultivate genuine partnerships with communities by institutionalizing mechanisms that encourage civic participation. This includes co-designing cyber safety programs with local stakeholders, involving residents in policy dialogues, and creating neighborhood-based reporting and education hubs. Greater emphasis should be placed on inclusive, bottom-up strategies that

empower citizens—especially those in underserved areas—to take an active role in cybercrime prevention.

2. Although online safety awareness is generally evident, there remains a need to increase the visibility and regularity of educational campaigns. The PNP-ACG should collaborate with schools, local government units, and civil society organizations to deliver targeted, audience-specific digital literacy initiatives. These should be designed in accessible formats and delivered through both traditional and digital platforms to maximize reach, especially among older adults, rural communities, and individuals with limited digital fluency.

3. While reporting procedures exist, their user-friendliness and accessibility require improvement. The PNP-ACG should develop a centralized and mobile-optimized reporting system that integrates online, SMS, hotline, and in-person options. The system must be intuitive, multilingual, and confidential. Information about where and how to report must be prominently disseminated through community outreach, social media, and public signage to build public awareness and trust in the system.

4. Given the high regard for victim support services, the PNP-ACG should institutionalize trauma-informed protocols and ensure the availability of psychosocial services through referrals to partner agencies. Training should be provided to police officers on victim sensitivity, secondary victimization prevention, and data privacy. Regular feedback from victims should be collected to refine services, and case progress updates should be standardized to maintain transparency and reassure victims of ongoing support.

5. To address the perceptual disconnect—particularly on community-led digital literacy programs—the PNP-ACG should implement participatory feedback loops. These can take the form of community forums, citizen satisfaction surveys, and digital consultations. These mechanisms will ensure that police initiatives reflect public needs and that police personnel are informed of the real-world impact and reception of their programs.

6. The weak overall correlation between public trust and cybercrime prevention initiatives indicates the need for a more coherent, interlinked framework that explicitly ties institutional trust-building measures with program outcomes. The PNP should develop an integrated strategy that aligns its internal values of transparency, accountability, and service orientation with public-facing initiatives. This includes establishing clear performance metrics, accountability structures, and community-based monitoring systems to build confidence and reinforce the connection between trust and effectiveness.

OUTPUT OF THE STUDY
INPUTS IN PREVENTING AND SUPPRESSING CYBERCRIME OFFENSES

Rationale

The development of a strategic input framework to prevent and suppress cybercrime offenses is both timely and essential in the current digital landscape. The increasing complexity of cyber threats requires not only institutional preparedness but also a deeply embedded culture of public awareness and collaboration. The proposed key result areas (KRAs) directly address the interconnected challenges of limited digital literacy, underutilized reporting systems, inadequate victim support, and fragmented community involvement—identified in the study as gaps that weaken both cybercrime response and public trust.

Investing in Community Digital Literacy is foundational to empowering individuals with the skills necessary to recognize, avoid, and report cyber threats. Cybersecurity awareness must begin at the community level through grassroots initiatives. Barangay-based campaigns and partnerships with local schools and organizations are critical in equipping the public, especially vulnerable sectors such as youth and senior citizens, with practical knowledge of digital safety. Literacy is not only preventive but also confidence-building, enabling citizens to navigate online environments responsibly.

The enhancement of Accessible Cybercrime Reporting platforms responds to the observed gaps in system usability and visibility. Many victims of cybercrime do not report incidents due to perceived difficulty, lack of knowledge, or fear. A streamlined, multilingual, and secure reporting infrastructure—integrated across digital and offline modalities—ensures that all citizens can reach out to authorities with ease and trust. The effectiveness of these platforms will depend on both their technical functionality and the public's trust in their confidentiality and responsiveness.

Victim Support Services are equally vital. While respondents affirmed the PNP's professionalism and legal guidance in handling cybercrime victims, concerns remain regarding consistent access to emotional, psychological, and procedural support. Establishing formalized victim-centered protocols, with a clear referral system to legal and counseling services, will ensure a trauma-informed response. These support mechanisms must be sustained through partnerships with social workers, legal experts, and psychological service providers, creating a holistic care pathway for victims.

Strengthening Police-Community Engagement through continuous consultation and feedback mechanisms will bridge perceptual gaps between what the police implement and what the public experiences. The disparity in ratings of community-led digital literacy programs between police and community members, as evidenced in the study, illustrates the urgent need for dialogue-driven, co-created initiatives. Regular

community forums and structured feedback tools not only promote transparency and inclusion but also make citizens feel that they are part of the cybercrime solution.

Fostering Capacity-Building for PNP Personnel is an internal imperative. Cybercrime is dynamic and technically demanding; hence, the police force must remain updated with skills in digital forensics, trauma-informed investigation, data privacy, and ethical communication. Continuous professional development ensures operational excellence and enhances public confidence in the system's ability to respond effectively and sensitively to cyber incidents.

Finally, the creation of an Integrated Trust-Cybercrime Strategy is necessary to unify the objectives of public trust-building and cybercrime program delivery. The study revealed that while individual correlations exist between trust components and certain initiatives (e.g., mutual trust and online safety), public trust and cybercrime prevention are not always seen as interdependent. A formalized strategy that links transparency, accountability, communication, and civic participation with cybercrime prevention metrics will institutionalize trust as both a goal and a driver of effectiveness.

In summary, this rationale underscores the importance of a coordinated, multi-stakeholder, and data-informed approach to cybercrime prevention. The proposed inputs and their corresponding KRAs are designed not only to improve technical systems and service delivery but also to deepen institutional legitimacy, public empowerment, and sustainable digital security.

Key Result Areas (KRA)	**Objectives**	**Activities**	**Persons Involved**	**Performance Indicators**	**Timeframe**	**Budget (IN Peso)**
Community Digital Literacy	Enhance public knowledge and responsibility on online safety	Launch barangay-level digital literacy seminars and campaigns	PNP-ACG, LGUs, NGOs, Educators	Number of sessions conducted; participant reach; awareness improvement	Quarterly (Year-Round)	100,000
Accessible Cybercrime Reporting	Simplify and broaden access to cybercrime	Develop and publicize a multi-platform cybercrime	PNP-ACG, ICT Team, Civil Society Groups	Utilization rate of platforms; user satisfaction score	Implementation in Q2; Evaluation in Q4	50,000

	reporting systems	reporting system				
Victim Support Services	Ensure comprehensive and empathetic services for cybercrime victims	Institutionalize victim support protocols and referral services	PNP-ACG, Social Workers, Legal Aid, Counselors	Victim satisfaction; timeliness of updates; counseling uptake	Roll-out by Q2; Ongoing Evaluation	50,000
Police-Community Engagement	Promote participatory collaboration between police and community	Conduct quarterly community consultation and feedback forums	PNP-ACG, Barangay Leaders, Community Members	Level of community participation; feedback quality; action follow-through	Quarterly (Year-Round)	30,000
Capacity-Building for PNP Personnel	Strengthen internal capacities of PNP-ACG personnel for digital crime management	Train officers on digital forensics, data privacy, and trauma-informed care	PNP Training Division, IT Experts, External Trainers	Pre- and post-training assessments; certification rate	Bi-Annual Training Schedule	30,000
Integrated Trust-Cybercrime Strategy	Align public trust-building with cybercrime prevention outcomes	Create an integrated framework for public trust and cybercrime program evaluation	PNP Leadership, Policy Researchers, Community Reps	Adoption of framework; improvement in trust and program ratings	Framework Draft in Q2; Full Adoption by Q4	80,000

REFERENCES

1. BAJ, 2023 Digita l Technology: Shaping the Future https://baj.ac.uk/what-are-digital-technology/
2. Baker, L. M., & Green, K. P. (2020). The economic impact of cybercrime on businesses: A case study approach. Journal of Business Security, 19(2), 101-115. https://doi.org/10.1016/j.jbs.2020.05.004
3. Brush, K., & Cobb M., 2024. What is cybercrime and how can you prevent it? https://www.techtarget.com/searchsecurity/definition/cybercrime
4. Cisco. (2025). What is cybercrime. Retrieved from
5. Coll, L. (2022). What is Cybercrime. Retrieved from https://www.usnews.com/360reviews/privacy/whatiscybercrime?fbclid=IwAR240XGFtY56FbGLhBsb2urK0abm0LTw1cbIGGYPaAB_wkfBtduaOhg EpY
6. Cyber Security Intelligence (2025). "Philippine National Police Anti-Cybercrime Group (PNP-ACG)" https://www.cybersecurityintelligence.com/philippine-national-police-anti-cybercrime-group-pnp-acg-4731.html.
7. Deora, R.S., and Chudasama, D. "Brief Study of Cybercrime on an Internet" Journal of Communication Engineering & Systems https://www.researchgate.net/profile/Dhaval-Chudasama/publication/352121472_Brief_Study_of_Cybercrime_on_an_Internet/links/60ba1082a6fdcc22ead4cbe2/Brief-Study-of-Cybercrime-on-an-Internet.pdf DOI (Journal): 10.37591/JoCES.
8. Digital Adoption (2022) "What is digital technology" https://www.digital-adoption.com/what-is-digital-technology/
9. Digwatch (2024) Philippines' National Cybersecurity Plan (NCSP) 2023-2028 https://dig.watch/resource/philippines-national-cybersecurity-plan-ncsp-2023-2028.
10. European Commission. (2023). Crime Prevention. Retrieved from https://home-affairs.ec.europa.eu/policies/internal-security/organised-crime-and-human-trafficking/crimeprevention_en?fbclid=IwAR2vF2o2d4GD5B0lIEfhhXqbSbz3VRdqamG662_CI14NYvNiWnGkhT705DU
11. Hagan, F. E. (2021). Introduction to criminology: Theories, methods, and criminal behavior (12th ed.). Cengage Learning.
12. Harris, M., & Zhou, Q. (2024). Global legal responses to cybercrime: Strengthening international cooperation. Cybersecurity Policy Review, 16(1), 39-52. https://doi.org/10.1080/12345678.2024.1938930
13. Harris, S. (2020). The impact of ransomware attacks on businesses. Computer Weekly. https://www.computerweekly.com/news/252473195/The-impact-of-ransomware-attacks-on-businesses
14. https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1154&context=ijcic
15. https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybercrime.html
16. Insuranceopedia, (2025). "Modus Operandi" https://www.insuranceopedia.com/definition/5723/modus-operandi-mo-insurance
17. Johnstone K., Kervin L., and Wyeth P., (2022) "Defining digital technology" https://digitalchild.org.au/defining-digital-technology/

18. Kaspersky. (2023). What is cybercrime. Retrieved from https://www.kaspersky.com/resource-center/threats/what-is-cybercrime.
19. Keller, R., Moore, J., & Tanish, S. (2021). The rise of cybercrime during the COVID-19 pandemic: Trends, risks, and lessons. Cybersecurity Studies, 30(3), 154-171. https://doi.org/10.1016/j.cyber.2021.02.009
20. Kenton, W., Kelly, R.C., Khvilhuag, S. (2024). Modus Operandi: Meaning and Understanding a Business' M.O. https://www.investopedia.com/terms/m/modus-operandi.asp
21. Li, Y.S, and Qi, L.Y. (2019) " An approach for understanding offender modus operandi to detect serial robbery crimes. https://www.sciencedirect.com/science/article/abs/pii/S1877750319303412
22. Luna, J. (2024). The Philippines' National Cyber Security Plan 2023-2028: Roadmap to Cyberspace Resilience. Lumify Work. https://www.lumifywork.com/en-ph/blog/the-philippines-national-cyber-security-plan-2023-2028-roadmap-to-cyberspace
23. Monroe Community College. (2024). What is Crime Prevention. Retrieved from https://www.monroecc.edu/depts/pstd/crimepreventioninformation/?fbclid=IwAR2CWJ9NxcdlF5Gfi_Im4BiIdeNFzluZTsxCQ6sxxVppv1lSLoAxbMGv84
24. Philippine National Police. (2024, February 11). PNP: 19,000 cybercrimes recorded last year. The Philippine Star. https://www.philstar.com/headlines/2024/02/11/2332462/pnp-19000-cybercrimes-recorded-last-year
25. Piad, T. J. C. (2023). PH second most vulnerable in region to cyberthreats. Philippine Daily Inquirer. https://business.inquirer.net/428731/ph-second-most-vulnerable-in-region-to-cyberthreats
26. Thotakura, S., 2024 "Crime: A Conceptual Understanding" https://www.researchgate.net/publication/270238380_Crime_A_Conceptual_Understanding DOI:10.15373/2249555X/MAR2014/58
27. Tupas, E., 2024 "Cybercrime cases continue to rise, up 21.84 percent in Q1" PhilStar Global. https://www.philstar.com/headlines/2024/04/10/2346516/cybercrime-cases-continue-rise-2184-percent-q1
28. Khater, Abdullah & Al-Ma'adeed, Somaya & Ahmed, Abdulghani & Sadiq, Ali & Khan, Khurram. (2020). Comprehensive Review of Cybercrime Detection Techniques. IEEE Access. PP. 1-1. https://www.researchgate.net/publication/343144053_Comprehensive_Review_of_Cybercrime_Detection_Techniques
29. Bundala, Ntogwa. (2024). Understanding Cybercrime Modus Operandi: Techniques, Psychological Tricks, and Countermeasures. Asian Journal of Research in Computer Science. 17. https://www.researchgate.net/publication/387464283_Understanding_Cybercrime_Modus_Operandi_Techniques_Psychological_Tricks_and_Countermeasures#fullTextFileContent

30. Singh, Abhinav & Lukose, Sally. (2022). A Recent Advancement in Techniques for Investigating Cybercrimes, Digital Crimes and Audio Forensics. 14. 739-742. https://www.researchgate.net/publication/363505108_A_Recent_Advancement_in_Techniques_for_Investigating_Cybercrimes_Digital_Crimes_and_Audio_Forensics
31. Bundala, Ntogwa. (2024). Cybercrime: Psychological Tricks and Computer Securities Challenges. Asian Journal of Research in Computer Science. https://www.researchgate.net/publication/386340539_Cybercrime_Psychological_Tricks_and_Computer_Securities_Challenges
32. Rahman, Asia & Javaid, Tahir. (2025). The Role of Neutralization Techniques in Fraud Migration: Cybercrime Syndicates in West Africa. https://www.researchgate.net/publication/389776219_The_Role_of_Neutralization_Techniques_in_Fraud_Migration_Cybercrime_Syndicates_in_West_Africa
33. Hawdon, James. (2021). Cybercrime: Victimization, Perpetration, and Techniques. American Journal of Criminal Justice. https://www.researchgate.net/publication/356107265_Cybercrime_Victimization_Perpetration_and_Techniques
34. Aher, K. (2021). Detection techniques of cyber crime. International Journal of Innovative Research in Technology. https://www.academia.edu/64696531/Detection_Techniques_of_Cyber_Crime
35. Sahu, N. K., & Sahu, S. (2022). Comprehensive assessments of cybercrime detection techniques. In International Journal of Novel Research and Development, International Journal of Novel Research and Development (Vol. 7, Issue 9, pp. 893–894) [Journal-article]. https://www.ijnrd.org/papers/IJNRD2209106.pdf
36. Alghamdi, M. I. (2020). A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide. International Journal of Engineering Research & Technology (IJERT), 9–9(06), 731–731. A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide
37. Wu, L., Peng, Q., & Lembke, M. (2023b). Research Trends in Cybercrime and Cybersecurity: A review based on Web of Science Core Collection database. International Journal of Cybersecurity Intelligence and Cybercrime.https://www.researchgate.net/publication/373343178_Research_Trends_in_Cybercrime_and_Cybersecurity_A_Review_Based_on_Web_of_Science_Core_Collection_Database
38. Pandey, Purvi & Kapoor, Ashwarya. (2025). CYBERCRIME IN THE DIGITAL ERA: IMPACTS, AWARENESS, AND STRATEGIC SOLUTIONS FOR A SECURE FUTURE. https://www.researchgate.net/publication/388319800_CYBERCRIME_IN_THE_DIGITAL_ERA_IMPACTS_AWARENESS_AND_STRATEGIC_SOLUTIONS_FOR_A_SECURE_FUTURE
39. Yussuph, Toyyibat & Olalekan, M & Yusuf, Babatunde & Unuriode, Austine & Hafiz, Bolanle & Durojaiye, Olalekan. (2023). DATA PROTECTION AND PRIVACY AS A TOOL TO REDUCE FINANCIAL LOSS FROM CYBERCRIMES.

https://www.researchgate.net/publication/376312460_DATA_PROTECTION_AND_PRIVACY_AS_A_TOOL_TO_REDUCE_FINANCIAL_LOSS_FROM_CYBERCRIMES

40. Poulpunitha, Dr & Kalidasan, Manimekalai & P., Veeramani. (2020). Strategies to Prevent and Control of Cybercrime against Women and Girls. International Journal of Innovative Technology and Exploring Engineering. 9(3) 2278-3075. https://www.researchgate.net/publication/346623839_Strategies_to_Prevent_and_Control_of_Cybercrime_against_Women_and_Girls
41. Ezeji, Chiji. (2024). Emerging technologies and cyber-crime: strategies for mitigating cyber-crime and misinformation on social media and cyber systems. International Journal of Business Ecosystem & Strategy (2687-2293). https://www.researchgate.net/publication/386327138_Emerging_technologies_and_cyber-crime_strategies_for_mitigating_cybercrime_and_misinformation_on_social_media_and_cyber_systems
42. Kale, Dr. (2024). The Role of Legal Frameworks in Combating Cybercrime: Global Perspectives and Local Implications. African Journal OF Biomedical Research. https://www.researchgate.net/publication/387546329_The_Role_of_Legal_Frameworks_in_Combating_Cybercrime_Global_Perspectives_and_Local_Implications
43. Sarkar, G., Shukla, S. K., & Indian Institute of Technology, Kanpur. (2023). Behavioral analysis of cybercrime: Paving the way for effective policing strategies. In Journal of Economic Criminology (Vol. 2, p. 100034). Behavioral analysis of cybercrime: Paving the way for effective policing strategies - ScienceDirect
44. Tientcheu, P. (2021). Security awareness strategies used in the prevention of cybercrimes by cybercriminals [Thesis]. In Walden University & Walden University, Walden Dissertations and Doctoral Studies. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?params=/context/dissertations/article/12290/&path_info=PouaniTientcheu_waldenu_0543D_26802.pdf
45. Security Awareness Strategies Used in the Prevention of Cybercrimes by Cybercriminals
46. Solis-Diaz, C. J. (2023). EDUCATION AS a SOLUTION TO COMBAT RISING CYBERCRIME RATES AGAINST CHILDREN AND TEENAGERS (By California State University, San Bernardino, CSUSB ScholarWorks, & Electronic Theses, Projects, and Dissertations Office of Graduate Studies). https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=2993&context=etd
47. "EDUCATION AS A SOLUTION TO COMBAT RISING CYBERCRIME RATES AGAINST CHIL" by Christian Javier Solis-Diaz
48. 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, Accepted Manuscript [AM]. https://doi.org/10.1108/JCRPP-12-2019-0070
49. A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies | Emerald Insight

50. Back, S., & LaPrade, J. (2020b). Cyber-Situational Crime Prevention and the Breadth of Cybercrimes among Higher Education Institutions. International Journal of Cybersecurity Intelligence and Cybercrime, 3(2), 25–47. Cyber-Situational Crime Prevention and the Breadth of Cybercrimes among Higher Education Institutions
51. Dupuis, Marc & Jones, Emiliya. (2024). Cyber Victimization: Tools Used to Combat Cybercrime and Victim Characteristics. https://www.researchgate.net/publication/383285170_Cyber_Victimization_Tools_Used_to_Combat_Cybercrime_and_Victim_Characteristics#fullTextFileContent
52. Hamad, Noura & Eleyan, Derar. (2022). Digital Forensics Tools Used in Cybercrime Investigation -Comparative Analysis. https://www.researchgate.net/publication/360463703_Digital_Forensics_Tools_Used_in_Cybercrime_Investigation_-Comparative_Analysis
53. Tuleun, Washima. (2021). Cryptocurrency and cybercrime in Nigeria: A double-edged sword. Global Journal of Engineering and Technology Advances. https://www.researchgate.net/publication/388381702_Cryptocurrency_and_cybercrime_in_Nigeria_A_double-edged_sword
54. Ho, H., Gilmour, J., Mazerolle, L., & Ko, R. (2023). Utilizing cyberplace managers to prevent and control cybercrimes: a vignette experimental study. Security Journal, 37(1), 129–152. https://doi.org/10.1057/s41284-023-00371-8
55. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data. The Geneva Papers on Risk and Insurance - Issues and Practice, 698–736. https://doi.org/10.1057/s41288-022-00266-6 https://pmc.ncbi.nlm.nih.gov/articles/PMC8853293/
56. Ngunjiri, Ndirangu. (2024). TECHNOLOGICAL DEVELOPMENTS AND INNOVATIONS INFLUENCE CYBERCRIME RISE IN JUJA SUB-COUNTY. National Security. https://www.researchgate.net/publication/385516980_TECHNOLOGICAL_DEVELOPMENTS_AND_INNOVATIONS_INFLUENCE_CYBERCRIME_RISE_IN_JUJA_SUB-COUNTY
57. Adnan, Md Al & Rahman, Md Saifur & Maliha, Jeba & Shahrear, Shahjada & Tinny, Sejuti Sarker & Mohammad, Khalid & Haider, Syed. (2024). ANALYSIS OF IDENTIFICATION OF CYBERCRIMES USING CYBER SECURITY ANALYTICS POWERED BY ARTIFICIAL INTELLIGENCE. Chinese Science Bulletin (Chinese Version). https://www.researchgate.net/publication/383601718_ANALYSIS_OF_IDENTIFICATION_OF_CYBERCRIMES_USING_CYBER_SECURITY_ANALYTICS_POWERED_BY_ARTIFICIAL_INTELLIGENCE
58. Ali, S & Abo-Torkhoma, Al-Latif & Abo-Torkhoma, Mufleh & Al-Hossini, Mayasa & Al-Ahwal, Mohammed & Al-Wakif, Widad & Al-Latif, Abd & Abo-Torkhoma, H & Ali, Gameil & Al-Latif, Amat. (2024). Cybercrime Types and Digital Forensic Tools

:https://www.researchgate.net/publication/382967386_Cybercrime_Types_and_Digital_Forensic_Tools_review

59. D, Suganthi & Mythili, J & Prabhu, N. (2025). Automated Malware and Phishing Website Detection Using Cluster Ensemble Techniques for Cybercrime Prevention. International Journal of Scientific Research and Engineering Trends. https://www.researchgate.net/publication/389848192_Automated_Malware_and_Phishing_Website_Detection_Using_Cluster_Ensemble_Techniques_for_Cybercrime_Prevention
60. Nagathota, Joshua & Kethar, Jothsna & Gochhayat, Sarada. (2023). Effects of Technology and Cybercrimes on Business and Social Media. https://www.researchgate.net/publication/377349946_Effects_of_Technology_and_Cybercrimes_on_Business_and_Social_Media
61. Swetha, K. & Sivaraman, K.. (2024). SMART Model: A Robust Approach for Cyber Criminal Identification using Smartphone Data. Engineering, Technology & Applied Science Research. https://www.researchgate.net/publication/386391761_SMART_Model_A_Robust_Approach_for_Cyber_Criminal_Identification_using_Smartphone_Data
62. Ashraf, Faheem & Javaid, Tahir. (2025). Convicted Fraudsters and Their Business Strategy: How Cybercriminals Adapt to Global Regulations. https://www.researchgate.net/publication/389775553_Convicted_Fraudsters_and_Their_Business_Strategy_How_Cybercriminals_Adapt_to_Global_Regulations
63. Ortega Anderez, Dario & Kanjo, Eiman & Anwar, Amna & Johnson, Shane & Lucy, David. (2021). The Rise of Technology in Crime Prevention: Opportunities, Challenges and Practitioners Perspectives. https://www.researchgate.net/publication/349125315_The_Rise_of_Technology_in_Crime_Prevention_Opportunities_Challenges_and_Practitioners_Perspectives
64. Gautam, Y., & Renu, D. (2024). Integrating artificial intelligence into cybercrime investigation: Challenges and future directions. International Journal of Financial Management and Research, 6(5), 1–12. https://www.ijfmr.com/papers/2024/5/28909.pdf
65. Chaurasia, M. K., & Thakur, N. (2024). The emerging technology in cybercrime of cyberspace: An overview. International Journal for Multidisciplinary Research, 6(1), 1–10. https://www.ijfmr.com/papers/2024/1/14116.pdf
66. Boutros, C. (2023). BRIDGING THE GAP BETWEEN LAW ENFORCEMENT AND CYBERSECURITY (By Essia Hamouda, Ph.D & Conrad Shayo, PhD) [Thesis; PDF]. California State University, San Bernardino. https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=2914&context=etd
67. du Toit, Pieter. (2023). The search warrant provisions of the cybercrimes act and their relationship with the criminal procedure act. Obiter. https://www.researchgate.net/publication/366933719_THE_SEARCH_WARRANT_PROVISIONS_OF_THE_CYBERCRIMES_ACT_AND_THEIR_RELATIONSHIP_WITH_THE_CRIMINAL_PROCEDURE_ACT

68. Atrey, I. (2023). Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence. International Journal of Research and Analytical Reviews, 10(3), 183–185. https://ssrn.com/abstract=4789133
69. Carr, R. & Old Dominion University. (2023). Some legal and practical challenges in the investigation of cybercrime. In Cybersecurity Undergraduate Research. https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1060&context=covacci-undergraduateresearch
70. Amoo, N. O. O., Atadoga, N. A., Abrahams, N. T. O., Farayola, N. O. A., Osasona, N. F., & Ayinla, N. B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. World Journal of Advanced Research and Reviews, 21(2), 205–217. https://doi.org/10.30574/wjarr.2024.21.2.0438
71. Khalifa, A. M. M. (2020). Overcoming the conflict of jurisdiction in cybercrime. In AUC Knowledge Fountain. https://fount.aucegypt.edu/etds/846 https://fount.aucegypt.edu/cgi/viewcontent.cgi?article=1845&context=etds
72. SAQF AL HAIT, A. A. (2014). Jurisdiction in Cybercrimes: A comparative study. In Journal of Law, Policy and Globalization: Vol. Vol.22 (pp. 75–76). https://core.ac.uk/download/pdf/234649797.pdf
73. Nishnianidze, A. (2023). Some new challenges of cybercrime and the reason for its outdated regulations. European Scientific Journal ESJ, 19(39), 92. https://doi.org/10.19044/esj.2023.v19n39p92
74. Hasan, M. T. (2024). Cross-border cybercrimes and international law: Challenges in ensuring justice in a digitally connected world. International Journal of Cyber Law & Technology, 4(1), 1-20. https://ijrdo.org/index.php/lcc/article/download/6174/3916/
75. Dragojlović, J. (2023). Jurisdiction for criminal offenses of cybercrime: International and national standards. Pravo - Teorija I Praksa, 40(suppl), 63–83. https://doi.org/10.5937/ptp2300063d https://www.researchgate.net/publication/369520172_Jurisdiction_for_criminal_offenses_of_cybercrime_International_and_national_standards
76. Ivanova, Liliya. (2023). Criminal Liability for Cybercrimes in the BRICS Countries. BRICS Law Journal. 10(1), 59-87. https://doi10.21684/2412-2343-2023-10-1-59-87. https://www.researchgate.net/publication/372716795_Criminal_Liability_for_Cybercrimes_in_the_BRICS_Countries
77. Shehu, Anas & Kamba, Musa & Faruk, Amiru. (2024). Understanding the Landscape of Cybercrime in Kebbi State: Challenges, and Mitigation Strategies. https://www.researchgate.net/publication/384595100_Understanding_the_Landscape_of_Cybercrime_in_Kebbi_State_Challenges_and_Mitigation_Strategies#fullTextFileContent

78. Namrata, K., & Chethan, V. K. (2024). A study on cybercrime: Its impact and awareness towards society. *International Journal of Creative Research Thoughts*, *12*(4), 23–30. https://ijcrt.org/papers/IJCRT2404004.pdf
79. Curtis, J., & Oxburgh, G. (2022). Understanding cybercrime in 'real world' policing and law enforcement. The Police Journal Theory Practice and Principles, 96(4), 573–592. https://doi.org/10.1177/0032258x221107584
80. Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. Humanities and Social Sciences Communications, 10(1). https://doi.org/10.1057/s41599-023-01560-x
81. Althibyani, H. A., & Al-Zahrani, A. M. (2023). Investigating the effect of students' knowledge, beliefs, and digital citizenship skills on the prevention of cybercrime. Sustainability, 15(15), 11512. https://doi.org/10.3390/su151511512
82. Bin Baharudin, A. H. (2022). EXPLORING CHALLENGES IN CYBERCRIME INVESTIGATION AND PLAUSIBLE SOLUTION. In Universiti Teknologi Malaysia, Master of Business Administration [Thesis]. https://eprints.utm.my/102682/1/AkmalHamdyBaharudinMAHIBS2022.pdf.pdf
83. Horan, C., & Saiedian, H. (2021). Cyber Crime Investigation: landscape, challenges, and future research directions. J. Cybersecur. Priv., 580–596. https://doi.org/10.3390/jcp1040029
84. VITUS, E. N. (2023). Cybercrime and Online Safety: Addressing the challenges and solutions related to cybercrime, online fraud, and ensuring a safe digital environment for all users— A Case of African States [Journal-article]. TIJER - INTERNATIONAL RESEARCH JOURNAL, 10(9). https://philarchive.org/archive/VITCAO
85. Gupta, J. K., & Lunia, U. (2024). Cyber crime and the challenges of prosecution and prevention. International Journal of Law Management & Humanities, 7(4), 1038. https://ijlmh.com/wp-content/uploads/Cyber-Crime-and-the-Challenges-of-Prosecution-and-Prevention.pdf
86. United Nation (2019) "The impact of digital technologies" https://www.un.org/sites/un2.un.org/files/2019/10/un75_new_technologies.pdf
87. University of Glasglow, 2019. "What is crime? https://www.sccjr.ac.uk/wp-content/uploads/2019/10/1-What-is-crime-1.pdf
88. University of Manchester, 2022 "Criminal Justice: What is a Modus Operandi?" https://www.bolton.ac.uk/blogs/criminal-justice-what-is-a-modus-operandi
89. White, R., & Haines, F. (2021). Crime and criminology (9th ed.). Oxford University Press.
90. Wu, L., Peng Q., and Lemke, M., 2023 " Research Trends in Cyber ends in Cybercrime and Cybersecurity: A Re crime and Cybersecurity: A Review Based on Web of Science Core Collection Database, International Journal of Cyber Security Intelligence and Cybercrime.
91. Intothecommerce, (2024), What Is Technology? The Definition, Types, and Impacts https://intothecommerce.com/technology/what-is-technology/

Survey Questionnaire

Dear Respondents,

I am a student of Doctor of Philosophy in Criminal Justice and currently working on my dissertation paper entitled, "**CYBERCRIME PREVENTION INITIATIVES AMONG THE PNP'S AFFECTING PUBLIC TRUST AND COLLABORATION OF THE COMMUNITY**".

In line with this, I am humbly asking you to answer the following items in the questionnaire. Rest assured that every information from this survey will be treated with utmost confidentiality.

Thank you very much for your cooperation.

Respectfully yours,

DANIEL ALLAN A. PASIA
Researcher

Part 1. Category of Respondents

[ ] Police Personnel
[ ] Community Residents

Part 2. Demographic profile of the respondents

Age

[ ] Below 25 years old
[ ] 25-30 years old
[ ] 31-35 years old
[[36-40 years old
[ ] 41-45 years old
[ ]. Above 45 years old

Sex

[ ] Male
[ ] Female

Educational Attainment

[ ] High School Graduate
[ ] College Level
[ ] College Graduate
[[With Masteral Units
[ ] Masteral Grduate

[[With Doctoral Units
[ ] Doctoral Grduate

Part 3. Assessment on the on the public trust and collaboration. Please rate each statement by putting a check (/) mark which you believe reflects your assessment, using the following scale values.

4 Strongly Agree (SA)
3 Moderately Agree (MA)
2 Disagree (DA)
1 Strongly Disagree (SD)

Statements/Indicators	**4**	**3**	**2**	**1**
Mutual Trust				
1. I believe that the PNP Anti-Cybercrime Group acts with integrity when handling cybercrime cases				
2. There is mutual respect and trust between the police and the community in addressing cybercrime issues				
3. The public can rely on the PNP to maintain confidentiality when a cybercrime is reported				
4. Community members trust the competence of the PNP-ACG in resolving cybercrime incidents				
5. The PNP actively demonstrates trust in the community's capacity to cooperate in cybercrime prevention				
6. Previous interactions between the police and the community have strengthened our mutual trust				
7. Both the police and residents are open to working together based on shared trust and responsibility in combating cybercrime				
Open dialogue				
1. The PNP-ACG regularly communicates with the community about cybercrime issues and prevention strategies				
2. Community members are given opportunities to express their concerns and suggestions regarding cybercrime prevention				
3. There are open forums or discussions between the police and the public that address digital safety and cyber threats				
4. I feel comfortable initiating conversations with the PNP regarding online security concerns				

5. The police provide timely and understandable information to the community on cybercrime developments				
6. Community feedback is acknowledged and considered in the planning of anti-cybercrime initiatives				
7. Open and transparent communication exists between the PNP and the community regarding ongoing cybercrime cases and prevention programs				
Shared responsibility				
1. Both the police and the community have important roles to play in preventing cybercrime				
2. The community actively supports PNP-ACG efforts by reporting suspicious online activities				
3. I believe that cybercrime prevention should not be left solely to the police				
4. The PNP encourages citizens to take part in educational campaigns about online safety				
5. There is a shared commitment between the police and the community to reduce cybercrime incidents				
6. The success of cybercrime prevention in our area depends on collaboration between the police and the public				
7. The PNP and community members jointly participate in initiatives that promote responsible internet use.				
Transparent processes				
1. The PNP and community members jointly participate in initiatives that promote responsible internet use.				
2. Citizens are informed about the status and progress of their reported cybercrime complaints				
3. The PNP uses transparent methods in handling cybercrime investigations and public concerns				
4. There are accessible channels for the public to verify information about cybercrime cases and prevention programs				
5. The police provide regular updates to the community on cybercrime statistics and trends				
6. I trust that the PNP follows due process in managing cybercrime incidents involving members of the public				
7. The guidelines and responsibilities of both police and citizens in cybercrime prevention are clearly communicated and understood				

Part 4. Assessment on the on the PNP's cybercrime prevention initiatives. Please rate each statement by putting a check (/) mark which you believe reflects your assessment, using the following scale values.

4 Strongly Agree (SA)
3 Moderately Agree (MA)
2 Disagree (DA)
1 Strongly Disagree (SD)

Statements/Indicators	4	3	2	1
Online safety awareness				
1. The PNP-ACG regularly conducts educational campaigns to raise awareness on safe internet practices				
2. I have learned important online safety tips from the programs or materials provided by the police				
3. The PNP collaborates with schools and community groups to promote responsible internet use				
4. The community is more aware of cyber threats today due to the efforts of the PNP-ACG				
5. The online safety materials distributed by the PNP are easy to understand and practical				
6. The PNP effectively uses social media and other platforms to inform the public about cybercrime risks				
7. The PNP's efforts in promoting online safety have increased my confidence in using the internet securely				
Cybercrime reporting				
1. There are clear procedures established by the PNP-ACG for reporting cybercrime incidents				
2. I know where and how to report a cybercrime if I encounter one				
3. The reporting platforms provided by the PNP (e.g., website, hotline, walk-in) are accessible and user-friendly				
4. The PNP responds promptly and professionally to reported cybercrime cases				
5. Reporting cybercrimes to the police does not require complicated or time-consuming steps				
6. The PNP encourages the public to report all types of cybercrime, regardless of severity				

7. I feel safe and protected when I report a cybercrime to the authorities				
Victim support				
1. The PNP provides appropriate assistance to victims of cybercrime, including guidance on legal actions				
2. Victims of cybercrime receive timely updates regarding the progress of their cases				
3. Support services, such as counseling or referrals, are made available to cybercrime victims by the PNP or its partner agencies				
4. The PNP ensures the privacy and protection of individuals who report being victimized online				
5. Victims are treated with empathy, respect, and professionalism by responding officers				
6. I am aware of specific programs or services offered by the PNP to support cybercrime victims				
7. The PNP has mechanisms in place to prevent secondary victimization or re-traumatization during the investigation process				
Community-led digital literacy programs				
1. The PNP collaborates with schools, barangays, and NGOs in organizing digital literacy activities				
2. There are community-initiated programs in our area that teach safe internet use and online responsibility				
3. I have participated in a local digital literacy seminar or campaign supported by the PNP-ACG.				
4. Community-led efforts to promote digital safety are effective in helping residents prevent cybercrime				
5. The PNP supports grassroots initiatives that aim to educate vulnerable groups (e.g., youth, elderly) about cyber threats				
6. Digital literacy programs in our locality are accessible and inclusive to all sectors of the community				
7. There is strong collaboration between the PNP and the community in planning and implementing digital literacy initiatives				

CURRICULUM VITAE

DANIEL ALLAN A. PASIA
Home Address:
231 Brgy. Emmanuel Cuenca, Batangas
Batangas Province, 4217, Philippines
allanpasia23@gmail.com
0906-9101-013

BIOGRAPHICAL NOTE:

Mr. Daniel Allan A. Pasia, a Registered Criminologist,
one of the instructors of College of Criminal Justice Education (CCJE) in Batangas State University JPLPC-Malvar. Likewise, he participates in Research and serves as the College Coordinator of Community Extension Programs and Adviser of Council of Arts and Sciences Students (CASS), the recognized student organization of College of Arts and Sciences. He is currently the Head of National Service Training Office and Security Services Office.

EDUCATION

2023-2025
Doctor of Philosophy in Criminal Justice
Emilio Aguinaldo College
Ermita Manila

2020-2022
Master of Science in Criminal Justice with specialization in Criminology
Metro Manila Colleges
Novaliches, Quezon City

2017-2019
Master of Science in Criminal Justice with specialization in Criminology (36 units)
University of Manila
Sampaloc, Manila City

2010 – 2014
Bachelor of Science in Criminology
Lipa City Colleges
College of Criminology
Lipa City, Batangas

ELIGIBILITIES

Registered Criminologist
April 2014

ACHIEVEMENTS

Rank 1 Specialization Training in Forensic Polygraphy
March 2014

WORK EXPERIENCE

Instructor III Batangas State University- JPLPC Malvar Campus
January 2023-present

Instructor I Batangas State University- JPLPC Malvar Campus
August 2016-2022

Aviation Security Agent High Command Aviation Security Agency
PAIR-PAGS Center, NAIA Complex,
Parañaque City 1704
December 2014- May 2016

I hereby certify that the above information is true and correct to the best of my knowledge and belief.

DANIEL ALLAN A. PASIA