



National University  
Manila

College of Computing and Information Technologies  
Computer Science Department

**ClickSmart: An Informative AI Chatbot-Supported Website for Cybercrime Awareness**

A Thesis Presented to the Faculty of the  
College of Computing and Information Technologies  
National University - Manila

In Partial Fulfillment of the Requirements for  
Thesis 2

By:

Abalos, Hanst Diether B.

Castillo, John Russell M.

Dia, Joshua M.

Montalban, Farrah V.

So, Vlademer Zane A.

Professor  
Susan S. Caluya

February 2025

## Table of Contents

Chapter	Page No.
<b>Chapter 1: Introduction</b>	
Background of the Study .....	1
Statement of the Problem.....	3
Objectives of the Study .....	5
<i>General Objective</i> .....	5
<i>Specific Objectives:</i> .....	5
Definition of Terms .....	6
Beneficiary of the Study .....	7
Significance of the Study .....	9
<b>Chapter 2: Review and Related Literature</b>	
Cybercrime and Cybersecurity in the Philippines (Pre to Post-Pandemic) .....	10
Attacker Methods and Tactics.....	18
Roles of AI Chatbots in Cybersecurity .....	21
Cybersecurity Awareness and Education .....	22
Technological Innovations in Cybercrime Detection and Prevention .....	24
Gaps in the Literature.....	28
Synthesis of the Reviewed Literature and Studies.....	29

### **Chapter 3: Methodology**

<i>Theoretical Framework: Protection Motivation Theory</i> .....	32
<i>Framework for Chatbot Model</i> .....	34
Research Design.....	40
Research Locale .....	41
Data Gathering Procedure.....	41
Research Instrument.....	42
Respondents of the Study.....	42
Data Analysis .....	43
Ethical Considerations .....	44

### **Chapter 4: Results and Discussion**

Comparative Analysis of Cybercrime Cases: Q4 2023 vs. Q1 2024 .....	45
Cybercrime Analysis of District 3 in Quezon City (January to June of 2024) .....	46
Cybercrime Analysis of District 4 in Quezon City (January to June of 2024) .....	49
Cybercrime Analysis of District 5 in Quezon City (January to June of 2024) .....	51
Cybercrime Analysis of District 6 in Quezon City (January to June of 2024) .....	53
Summary of Data Across Districts in Quezon City (January–June 2024).....	54
Qualitative Analysis of Cybercrime Trends Based on Interviews .....	57
Evaluation of Pre-Trained and Post-Trained Chatbot Model .....	63
Rule-Based Chatbot Integration for ClickSmart.....	66

### **Chapter 5: Summary of Findings, Conclusions and Recommendations**

Summary of Findings.....	68
Conclusions.....	69
Recommendations.....	70

## **APPENDICES**

APPENDIX - A.....	73
A. Advisory Request Letter.....	73
APPENDIX - B.....	77
Interview Questionnaire.....	78
APPENDIX – C .....	80
A. Interview at Kamuning Police Station .....	80
B. Interview at Quezon City Police District Headquarters Camp Caringal.....	87
APPENDIX – D .....	91
APPENDIX – E .....	92
REFERENCES .....	93

## **Chapter 1: Introduction**

### **Background of the Study**

Cybercrime is growing in the Philippines, with more cases reported over the last six years. Unfortunately, many of these crimes go unreported because victims often feel that their financial losses are too small to bother reporting. Additionally, many people don't realize that cybercriminals often take advantage of special occasions. For example, there are more love scams around Valentine's Day and holiday-related scams during Christmas. This behavior confuses both local law enforcement and the public. Cybercriminals may change their methods, but their strategy stays the same: they wait for the right time to attack. While this tactic isn't new, it has become more noticeable in recent trends (Col. J. P. Abrazado, personal communication, September 18, 2024).

The Philippine National Police (PNP) Anti-Cybercrime Group (ACG) has consistently recorded an upsurge in offenses such as online libel, scams, voyeurism, identity theft, threats, hacking, and more. In the first quarter of 2024 alone, cybercrime rates surged by 22%, with ACG Chief Maj. Gen. Sidney Hernia attributing this rise to a lack of public awareness. A total of 4,469 incidents were reported compared to 3,668 during the same period in 2023. The top three offenses included online selling scams (990 cases), debit and credit card fraud (309 cases), and investment scams (319 cases). Key contributing factors to the rise in cybercrime included increased online activity, more sophisticated criminal tactics, and a general lack of public awareness (Caliwan & Tupas, 2024). These incidents prove the urgent need for enhanced public education to address the growing threat of cybercrime.

Cybercrime refers to any illegal activities conducted through computers or the internet. These can include stealing sensitive information, demanding ransom to prevent attacks, injecting malicious viruses into systems, or hacking government networks. Moreover, emerging cybercrime trends involve AI-driven social engineering, ransomware as a service (RaaS), commercial spyware, and extortionware. These attacks can cause significant damage to victims, including reputational harm to businesses, legal consequences due to data breaches, and personal data loss ("Hackers Think in All Directions. End-to-end Security Is the Answer," 2024).

Cybercriminals exploit the anonymity and ubiquity of the internet to carry out their illegal activities. However, the public often finds it difficult to report cybercrimes due to the complex processes and unfamiliar legal terminology involved. This lack of awareness contributes to a more vulnerable environment, leading to a rise in cybercrime incidents. As Maj. Levy Lozada, spokesperson for the PNP ACG, pointed out, "the more people use the internet, the greater the number of vulnerable communities," especially if they are unaware of the internet's do's and don'ts (Gonzales, 2019).

To combat the rising cybercrime issues, law enforcement agencies like the PNP ACG conduct seminars, awareness campaigns, and investigations. However, they face significant challenges, including a lack of personnel and outdated equipment to address the rapidly evolving nature of cybercrime technologies. Additionally, geographical disparities across the country contribute to differing levels of public awareness, with urban areas exhibiting higher awareness compared to remote regions (Gonzales, 2019). In 2024, the PNP ACG also recorded cases involving new methods of fraud, including the use of Non-Fungible Tokens (NFTs), cryptocurrencies, and online casinos (Sunnexdesk & Sunnexdesk, 2023).

Despite these advancements, PNP spokesperson Col. Jean Fajardo acknowledged that many police investigators are not properly trained to handle cybercrime cases due to outdated information and communications technology (ICT) systems, limiting their ability to effectively address modern cyber threats (Caliwan, 2024). As a result, the PNP ACG has become overwhelmed by the volume of reported cybercrime incidents. To address this challenge, the PNP ACG aims to educate local government offices and various sectors to manage basic cybercrime cases, allowing the PNP ACG to focus on more complex and highly technical incidents.

Additionally, in 2021, the PNP ACG launched a website to assist the public in verifying whether a suspicious phone number was associated with scammers. Victims could input the number into the system, which would check for any history of cybercriminal activity, including common scams like fake lottery winnings. Unfortunately, the PNP system underwent a preventive shutdown, which affected the functionality of the PNP ACG website (Col. J. P. Abrazado, personal communication, September 18, 2024).

### **Statement of the Problem**

The increasing incidence of cybercrime in the Philippines, particularly in high-risk areas such as Quezon City, remains a critical issue. As mentioned by the local reports, cybercrime activities such as phishing, hacking, and identity theft have seen a sharp rise, despite of ongoing awareness efforts by the Philippine National Police (PNP) and the Anti-Cybercrime Group (ACG), resulting in incidents affecting both individuals and businesses. Based on the interviews with PNP officials and ACG, several key issues have emerged:

- **Cybercrime is heavily under-reported**, particularly in low-income areas where victims may not realize they have been targeted or cannot afford the time and resources

to report crimes. For example, losses as small as ₱500 or ₱2,000 often go unreported due to the perceived hassle of traveling to report the incident.

- There is a **lack of user-friendly, and easily accessible resources for cybercrime awareness platforms**, forcing citizens to visit physical offices, which may contribute to under-reporting.

The researchers aim to investigate the growing issue of cybercrime in the Philippines, particularly focusing on the lack of public awareness and understanding of cybersecurity practices that contribute to this trend. Specifically, the study seeks to answer the following questions:

1. What is the current level of public awareness regarding cybersecurity measures among residents of high-risk areas in Quezon City based on the data from the Quezon City Kamuning Police Station and the Quezon City Police District Headquarters Camp Tomas Caringal, specifically in terms of:

- 1.1. Understanding of common cyber threats;

- 1.2. Awareness of protective measures; and

- 1.3. Familiarity with the reporting process and available reporting channels (e.g., Facebook pages, official hotlines)?

2. How does the Philippine National Police (PNP) categorize barangays as high-risk for cybercrime, and what criteria are used for this classification?

3. Do demographic factors (e.g., age, gender, occupation) affect vulnerability to cybercrime?



By answering these questions, the study aims to show that cybercrime is a real and growing problem, emphasizing the urgent need for better public education and the development of accessible, technology-driven solutions.

## **Objectives of the Study**

### ***General Objective***

This study aims to create an informative website called *ClickSmart*, which includes an AI-powered chatbot that focuses on cybercrime. The goal is to raise awareness and make it easier for people to report cybercrime. The website will educate the public by providing simple explanations, safety tips, and guidance on how to recognize and report cyber threats. By spreading awareness, it helps people take steps to protect themselves from cybercrime.

### ***Specific Objectives:***

1. To collect and create a dataset for developing an AI chatbot that will be integrated into the ClickSmart website to provide users with useful cybercrime information.
2. To analyze data and insights from interviews with the PNP Anti-Cybercrime Group (PNP ACG) and integrate the findings into the ClickSmart website's statistics page.
3. To train and evaluate a GPT-2-based chatbot model using a domain-specific dataset, assessing its performance through key evaluation metrics such as Exact Match (EM) and BERTScore to ensure accuracy and reliability in generating responses related to cybercrime awareness.
4. To integrate a rule-based system into the ClickSmart chatbot to handle non-cybercrime-related queries, such as greetings, typos, FAQs about ClickSmart, and reporting guidance, complementing the AI model to enhance accuracy, contextual understanding, and user experience.

## **Scope and Limitations**

This study focuses on investigating cybercrime activity in Quezon City by analyzing data provided by the PNP-ACG. It uses both quantitative data and qualitative interviews for data collection.

Originally, this study aims to identify the top five high-risk barangays in Quezon City based on cybercrime cases. However, due to data privacy restrictions, the PNP only provides general data on cybercrime incidents. As a result, the researcher relies solely on the available information shared by the PNP.

The data of the study is limited to cybercrime cases reported in barangays within Districts 3 to 6, covering incidents that occur between January and June 2024. Additionally, it includes the available data on the number of cybercrime victims from the 4th quarter of 2023 to the 1st quarter of 2024. The study also develops a website designed for public use, featuring a cybercrime-focused chatbot that interacts and accepts inputs only in English. Furthermore, journal articles and literature reviewed for this study are limited to publications from 2016 to 2024 to ensure relevance.

## **Definition of Terms**

The following terms used in the study are defined conceptually and/or operationally to ensure clarity and better understanding.

**Cybercrime** - Illegal activities that involve computers or the internet, like fraud, hacking, and identity theft.

**AI Chatbot** - A computer program that uses artificial intelligence to chat with users and answer questions automatically.

**Cybercriminals** - People who commit crimes using the internet or digital technology.

**Scam** - A dishonest scheme to trick people into giving away money or personal information.

**Anonymity** - The state of being unknown or unidentifiable, especially online.

**Demographic** - Data about people, like their age, gender, income, and location.

**Streamline** - Making a process simpler and more efficient.

**Jargon** - Special words or phrases used by a specific group, often hard for others to understand.

**Framework** - A basic structure used to organize ideas or solve problems.

### **Beneficiary of the Study**

This study is important in sharing information and raising awareness among the following groups:

#### ***Government***

The government, particularly law enforcement agencies like the PNP Anti-Cybercrime Group, can use the research to improve their cybercrime prevention and response efforts.

#### ***Individual***

People gain valuable knowledge about cyber threats and how to protect themselves in the digital world. The benefits include:

- **Increased Awareness:** The public becomes more aware of how cybercrime affects local communities, making them more vigilant and less prone to cybercrime activity.

### *Students*

Studying cybersecurity, information technology, or related fields will gain practical insights into real-world cybercrime trends, threats, and incidents.

- **Educational Resource:** Students may utilize this research as a valuable educational resource to gain insights into the current landscape of cybercrime, cybersecurity measures, and the importance of awareness.

### *Future Researcher*

This study serves as a reference and baseline information to further develop new studies that enhance the knowledge of cybersecurity measures. Future researchers can benefit by:

- **Foundation for Further Research:** Future researchers may build upon the findings of this study, utilizing it as a foundational reference for exploring identified gaps, testing recommendations, or expanding upon the methodologies.
- **Framework for Understanding Cybercrime:** This research may provide a framework that future researchers can adopt to examine the dynamics of cybercrime, particularly within high-risk areas, offering insights into patterns and trends

## **Significance of the Study**

### ***Enhancing Public Awareness of Cybercrime***

Raising awareness about cybercrime is important in today's digital world, where many people fall victim to online threats like phishing and scams due to a lack of knowledge (John, 2020). This research helps bridge this gap by providing residents with easy-to-understand information. When people know how to protect themselves and report incidents quickly, it reduces the risk of cybercrime and makes it easier for law enforcement to respond. This awareness builds safer communities and supports national efforts to improve cybersecurity.

### ***Empowering Users through Interactive Learning***

Traditional ways of sharing information, like posters and flyers, don't always work well. This study introduces an informative website where users can learn cybercrime topics. It allows them to learn about common cybercrime questions where law enforcement officials usually ask the victim, making the reporting of cases easier.

### ***Bridging the Gap in Cybercrime Education***

There is often a gap between what people know about cybercrime and what they need to know to stay safe. This study bridges that gap by providing both cybercrime information and how to report a cybercrime guide on one platform. The website can also serve as a resource for students, researchers, and professionals, giving them insights into cybercrime.

## **Chapter 2: Review and Related Literature and Studies**

This chapter provides a review of related literature and studies that support the study and development of “ClickSmart,” An Informative AI Chatbot-Supported Website for Cybercrime Awareness. Additionally, a synthesis of the reviewed works highlights the similarities and differences between this study and prior research.

### **Cybercrime and Cybersecurity in the Philippines (Pre to Post-Pandemic)**

#### ***Year 2021***

At the start of this year, hybrid workplace starts to rise since the covid pandemic. The cybercriminals take advantage of this and focused on data breaches targeting the businesses organization. Philippines have an outdated cybersecurity system that the attackers find it advantage for them resulting a 623.3 million attack volume of ransom ware in 2021, this data is alarming since it is 105% higher than 2020`s data.

As for the malware, in the same year the study discovered a massive 5.4 billion malware attacks. To protect against this threat, IT team should adopt a holistic approach to cybersecurity (Esmeralda, 2022).

#### ***Year 2022-2023***

In the beginning of 2022, the Philippine National Police (PNP) recorded 13,890 cases of cybercrime, which escalated to 21,300 by 2023. The data indicated that most cybercrime activities were online scams, with 15,937 cases, followed by illegal online activities at 4,821 cases, and identity theft at 2,384 cases. This trend underscores the increasing influence of technology in cybercrime, highlighting the need for the police to adapt to these technological advancements (Presidential Communications Office, 2024).

Moving into the first half of 2023, cybercrime in Metro Manila surged by 152%. Despite the implementation of SIM card registration, ATM and credit card fraud remained prevalent, largely due to internet access exploited by both users and attackers (Lalu, 2023). Following this, cybercrime activities, such as financial crimes, online scams, and online wallet fraud, increased significantly. Reports indicated that these incidents rose from 70% in 2022 to 95% in 2023, primarily driven by victims clicking on scam links targeting online banking and wallets (Cabalza, 2023). Entering the latter half of 2023, the cybercrime rate continued to climb, reaching a 192% increase compared to the previous 152% rise in Metro Manila (Cabalza, 2023).

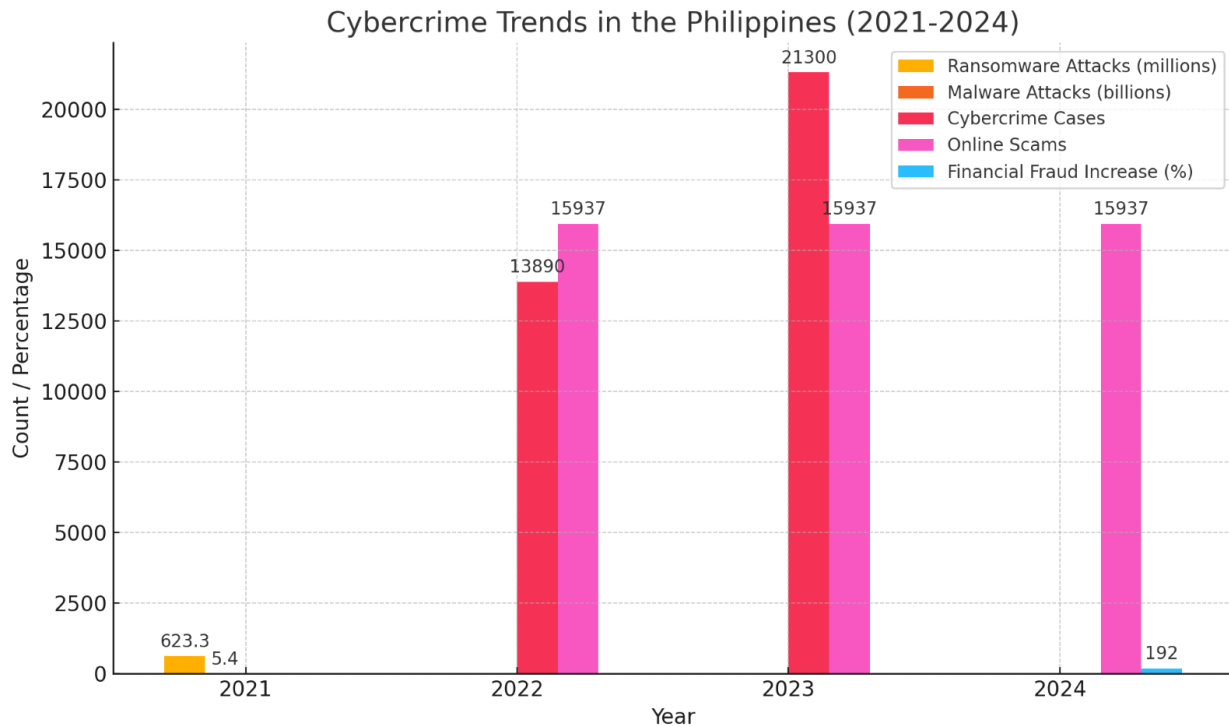
#### ***Year 2024***

In 2024, cases of 15, 000, mostly swindling or fraud scams, were recorded. They improved their tracking by tracing the SIM cards of the attackers. According to Acorda, the five most common cybercrimes in the country are illegal access with 4,000 cases, followed by identity theft with 2,000 cases, and credit card scams with almost 2,000 cases (Laqui, 2024).

In the following Q1 of the same year, the cases of cybercrime rose to 21.84 percent. Compared to the 2023 cases of 3, 668, it rises to 4, 469 cases due to the high volume of cases of online selling scams at 990 cases, credit scams at 309 cases, and investment scams at 319 cases. This case is due to the lack of awareness of the victims when it comes to online activity (Tupas, 2024).

Towards the end of March 2024, the cases dropped by 40.79 percent. The identified cases are illegal access, identity theft, online libel, and threats. They said that it is due to the increasing awareness of the people (Cybercrime Cases Fall by 40.79% in the Final Week of

March 2024 | ACG, 2024). Based on past cases, raising awareness really lessens the number of cases, which helps people avoid potential cyber threats.



### 1. Ransomware and Malware Attacks (2021):

- In 2021, there were 623.3 million ransomware attacks and 5.4 billion malware attacks. This shows a major cybersecurity threat as many organizations moved to hybrid work setups.
- Key Insight:** The sharp rise in these attacks points to weaknesses in cybersecurity that need immediate attention.

### 2. Cybercrime Cases (2022-2023):

- The number of cybercrime cases jumped from 13,890 in 2022 to 21,300 in 2023, marking a 53% increase.



- Key Insight: This increase highlights a growing trend in cybercrime, likely due to more people using digital platforms that are vulnerable to attacks.

### **3. Online Scams:**

- From 2022 to 2024, online scams remained high, with over 15,937 cases reported. This shows that online scams are a persistent issue, likely because more people are using the internet.
- Key Insight: Ongoing public education and awareness programs are essential to help people identify and avoid online scams.

### **4. Financial Fraud in 2024:**

- There was a significant 192% increase in reported financial fraud in 2024. This indicates that financial crimes are becoming more advanced and common.
- Key Insight: Even with regulations like SIM card registration, financial fraud remains a serious problem that needs more effective prevention strategies.

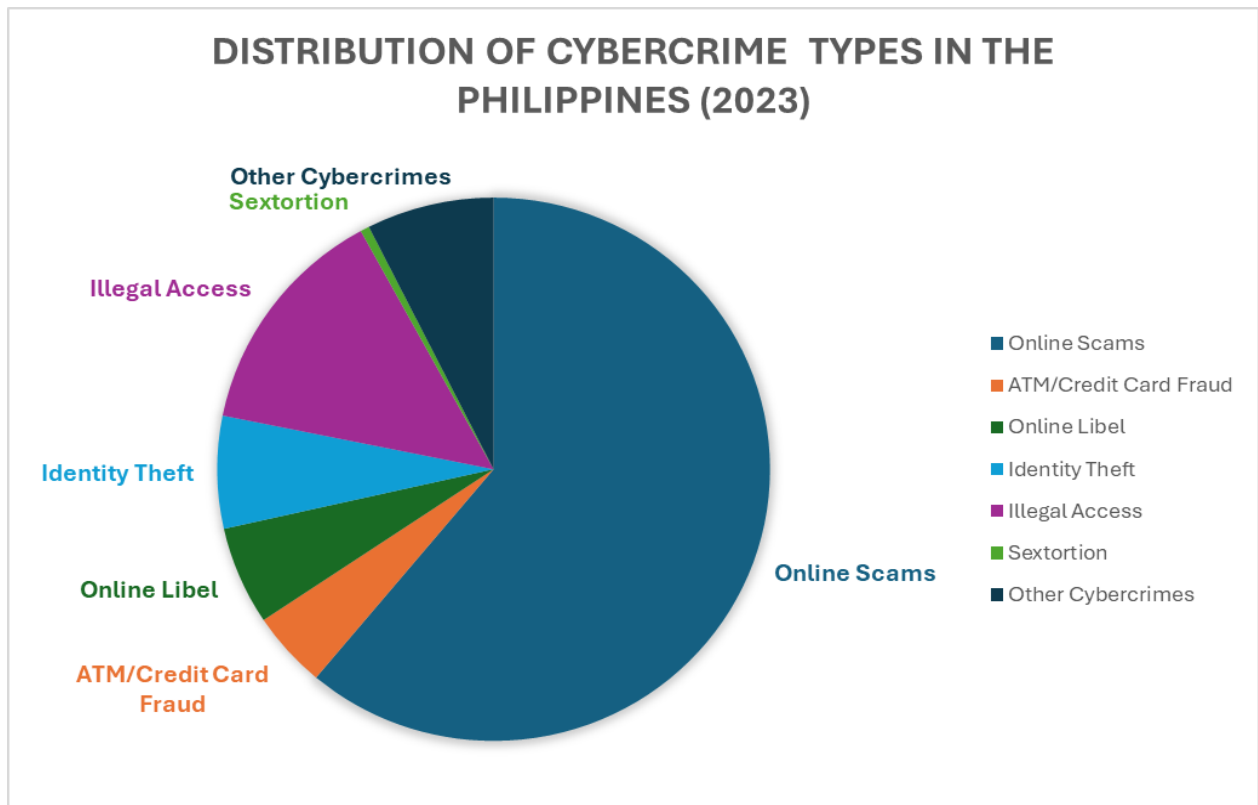
The data shows a troubling rise in cybercrime in the Philippines over the years, with many different types of attacks increasing. There is a clear need for better cybersecurity, more public education to help people avoid online scams, and improved law enforcement strategies to tackle the growing number of cyber threats. Since these issues keep happening, it is important to keep working hard to protect both individuals and organizations.

### **Open-Source Incident Reports**

Open-source data has become increasingly important in cybersecurity research, as it provides a source of information for understanding and mitigating cyber threats and incidents

(The Ultimate Guide to Open-Source Data [2023 Update], 2023.). Open-source data refers to publicly available data that is not proprietary or confidential, and can include incident reports, vulnerability disclosures, and other types of cybersecurity-related data. In addition, MERL Center highlights the benefits and drawbacks of open data, including increased accessibility and transparency, however, it comes with concerns about consent, privacy, and the misuse of data (“The Pros and Cons of Open Data,” 2021).

Moreover, as of early 2024, cybercrime incidents continued to escalate, with reports indicating a 21.8% increase in the first quarter compared to the same period in 2023. In 2023, the Philippines experienced a significant rise in cybercrime incidents, with the Philippine National Police (PNP) reporting a total of 19,472 cases. This marked an alarming increase of approximately 68.98% compared to the 11,523 cases recorded in 2022. Many of these incidents were attributed to online scams, which accounted for 14,030 cases—approximately 55.67% of the total. Other notable categories included illegal access (3,181 cases), identity theft (1,536 cases), online libel (1,342 cases), and ATM/credit card fraud (1,043 cases). Additionally, there were 121 documented sextortion cases and around 1,711 incidents categorized as "other cybercrimes," which included online threats and computer-related fraud. Thus, the rise in cybercrimes has prompted President Ferdinand Marcos Jr. to direct the PNP to enhance its cybersecurity measures (Tupas, 2024).



In this figure, the pie chart illustrates the distribution of various types of cybercrime cases in the Philippines for the year 2023. **Online scams** account for most cases, representing **55.67%** of the total with 14,030 reported incidents. This highlights the widespread occurrence of fraudulent activities conducted through online platforms. **Illegal access** follows at **12.8%**, with 3,181 cases involving unauthorized access to digital systems. Other significant categories include **identity theft** (**6.7%**), **online libel** (**5.8%**), and **ATM/credit card fraud** (**4.7%**). Although **sextortion** represents a smaller percentage at **0.5%**, it remains a critical concern. Additionally, **6.8%** of cases fall under the category of **other cybercrimes**, which includes online threats and computer-related fraud. This figure visualizes the urgent need for enhanced cybersecurity measures, particularly in combating online scams and unauthorized system access, which together constitute over two-thirds of the total reported incidents.

Additionally, in a significant incident occurred on May 17, 2024, when the Philippine National Police (PNP) Anti-Cybercrime Group (ACG) apprehended an online seller of registered SIM cards in Balintawak, Quezon City. The suspect was selling SIM cards registered under other people's identity, which is a violation of the new R.A. 11934 or SIM Registration Act and Cybercrime Prevention Act of 2012. The ACG conducted an entrapment operation and confiscated 50 SIM cards from the suspect. The apprehension of the online seller of registered SIM cards highlights the importance of cybersecurity measures in preventing cybercrimes. Cybercriminals often use registered SIM cards to conduct illegal activities online such as fraud and extortion (Cybercops Apprehended Online Seller of Registered SIM Cards | ACG, 2024).

On the other hand, another incident reported on May 8, 2024, involved the PNP-ACG Quezon City District Anti-Cybercrime Team (QCDACT), where two friends were deceived by an investment scam. The suspect convinced them to invest Php380,000.00 in forex trading via online fund transfer, promising substantial returns but later became unresponsive. The suspect's last communication to the victim was another request for an additional Php100,000.00 investment. This incident highlights the importance of trust in online transactions and the necessity for individuals to be cautious when investing in online schemes. It aligns with the concept of managing trust, which is a critical issue in today's digital age, and underscores the need for education and awareness in preventing online scams (Broken Trust, Two Friends Torn Apart by Investment Scam | ACG, 2024).

Lastly, on June 3, 2024, PNP-ACG arrested a male suspect for exploiting a minor-age girl in Payatas, Quezon City. The suspect was accused of using social media to lure and exploit the minor and was charged with violating the Anti-Child Abuse Law and the Cybercrime Prevention Act of 2012 (WCCPU Arrests Male Suspect for Exploiting a Minor | ACG, 2024).

In the study that provides a comprehensive review of online news and articles related to the sexual exploitation and abuse of children in the Philippines. The study highlights the prevalence of online child sexual abuse and exploitation in the country, including the use of social media and other online platforms to facilitate these crimes. Their study also identifies key factors that contribute to the perpetuation of these crimes, including poverty, lack of education, and cultural norms that promote the exploitation of children. These findings are relevant to the report by the Philippine National Police Anti-Cybercrime Group (PNP ACG) on the arrest of a male suspect for exploiting a minor. The report explains the importance of addressing the root causes of child sexual exploitation and abuse, including poverty and lack of education, and the need for increased awareness and education on these issues (Hernandez et al., 2018).

The National Institute of Standards and Technology (NIST) has published guidelines on cyber threat intelligence and information sharing, underscoring the value of open-source data in cybersecurity. According to NIST, sharing open-source data helps organizations develop comprehensive threat intelligence capabilities. This data includes indicators of compromise, threat actor tactics, techniques, and procedures, which are essential for enhancing an organization's ability to detect, analyze, and respond to cyber threats (Skorupka, 2021). Additionally, open-source data plays a crucial role in shaping cybersecurity policies and best practices. By analyzing open-source incident reports and data, policymakers can identify common vulnerabilities and attack vectors, leading to the development of more effective security standards and regulations. Studies have shown that leveraging open-source data in policy formulation helps create adaptive and resilient cybersecurity frameworks that can respond to emerging threats more effectively.

## **Attacker Methods and Tactics**

Cybercrime has become an increasingly prevalent threat in the digital age, with attackers employing a wide range of tactics to compromise computer systems and networks. Understanding the various attacking methods and stages used by cybercriminals is crucial for developing effective countermeasures and enhancing cybersecurity measures.

Notably, the COVID-19 pandemic has led to an exponential growth of cyberattacks and threats as the global economy has been paying much attention to fighting the pandemic. During that time, large corporations, healthcare's industry, and the government have been targets for cyberattacks and threats (Chigada & Madzinga, 2021). In the systematic literature mentioned, while global attention is focused on fighting and combating the spread of COVID-19, another wave of cybercrimes is growing exponentially. Cybercriminals syndicates are well-versed in global trends, have always-up-to-date information, and know very well when to start their operations.

Furthermore, home-based work at this time is the most vulnerable to cyber-risk since individuals are connected through less reliable and unsecured Internet connections. In addition, the new workflows make social engineering tactics against these employees and their families highly efficient (The Growing Cyberthreat to Utilities - and How They Should Respond, 2022). Admittedly, it is evident that technology improves people's lives while also posing new challenges.

As cybersecurity measures become more sophisticated, attackers continually evolve their tactics to bypass detection. One of the biggest challenges nowadays in security is not the evolution of AI technologies that are used in a bad way, but still the human factors of how manipulative a human can be. Social Engineering (SE) often serves as the starting point in

cyberattacks, exploiting psychological principles such as reciprocity, authority, and urgency to manipulate individuals into revealing sensitive information or performing actions to compromise security (Ye et al., 2020).

Additionally, the Advanced Persistent Threats (APTs) provide significant security challenges to organizations due to their sophisticated and persistent nature. (Mat et al., 2024). Conducted a systematic literature review on APT behaviors and detection strategies, highlighting the importance of integrating multi-stage attack-related behaviors with vulnerability assessments to improve detection accuracy. Their review highlights the need for adaptive defense mechanisms to effectively counteract these threats.

The study by Ahmed et al. (2021) outlines the stages of a cyberattack, breaking the process into key steps necessary for a successful attack. Here's a simple breakdown:

1. **Reconnaissance:** gathering information about the target to identify potential vulnerabilities.
2. **Weaponization:** Creating a deliverable payload designed to exploit the identified vulnerabilities.
3. **Delivery (SE):** transmitting the payload to the target through various means to search for an access.
4. **Exploitation:** Executing the malicious payload to take advantage of the target's vulnerabilities.
5. **Installation:** Installing malware to establish a persistent presence on the target's system and cause harm.
6. **Command and Control (C2):** Establishing communication with a command-and-control server to maintain control (Distribution of malicious activity)

**7. Actions on Objectives:** Achieving the attacker's ultimate goal, such as data exfiltration or system disruption.

Understanding these stages helps organizations develop effective defensive strategies. (Ahmed et al., 2021), emphasize the need for continuous monitoring and advanced analytics to identify and respond to sophisticated threats that traditional methods might miss. They propose an enhanced detection strategy leveraging machine learning and behavioral analysis to improve detection accuracy and response times.

Furthermore, (Grigaliūnas et al., 2023), highlights the importance of understanding the scope of cyberattack stages in relation to their impact on cyber-sustainability control over a system. Their study emphasizes the need for a comprehensive approach to cybersecurity that includes identifying the impact of the scope of cyberattack stages on the cyber resilience of information and communication systems. They propose a method for identifying the scope of cyberattack stages based on the aggregation of technical and organizational security metrics and detection sources, finding it 13% more effective in identifying the stage and scope of a cyberattack compared to existing methods. This proves the necessity of staying ahead of attackers by understanding the nature, stages, and scope of upcoming cyberattacks, especially in the context of Industry X.0.

In summary, cybercrime continues to evolve, so understanding the various attacking methods and stages used by cybercriminals is crucial for developing effective countermeasures and enhancing cybersecurity measures. As attackers adapt their tactics to bypass detection, researchers and security professionals must remain vigilant and continue to develop innovative solutions to combat the growing threat of cybercrime.



## **Roles of AI Chatbots in Cybersecurity**

AI chatbots play a crucial role in educating individuals and organizations about cybersecurity risks and safety practices. According to Hamad and Yeferny (2020), these chatbots provide information on common cybersecurity topics, such as password security, data protection, and scam prevention. Because these bots continuously update their knowledge base, users receive the latest insights and recommendations on cybersecurity threats (Hamad & Yeferny, 2020).

Furthermore, AI chatbots can act as first-line cybersecurity responders, offering immediate guidance to users encountering potential cyber threats. He and Xin (2021) highlight that, for example, if a user receives a suspicious email, an AI chatbot can analyze its content and provide insights on whether it might be a phishing attempt. These chatbots help users quickly identify cyber risks and take appropriate action to protect their personal information (He & Xin, 2021).

One of the key roles of AI chatbots is to raise awareness about cybercrime and educate users on how to recognize and avoid online scams. According to NJCCIC (2023), AI-driven chatbots deployed on websites, social media, and mobile apps provide detailed explanations of different types of cyber threats, such as:

- Phishing scams – Fraudulent emails or messages designed to steal user credentials (NJCCIC, 2023).
- Social engineering attacks – Manipulative tactics used by cybercriminals to gain access to personal data (Balbix, 2023).

- Ransomware attacks – Malicious software that locks users' files until a ransom is paid (SecOps Solution, 2023).
- Financial fraud schemes – Cybercrimes such as fake investment platforms and online banking scams (ICIT, 2023).

By offering structured and easy-to-understand information, AI chatbots help reduce the spread of misinformation and ensure users have access to factual cybersecurity knowledge (Balbix, 2023).

## **Cybersecurity Awareness and Education**

### ***Cybersecurity Awareness Among Students***

One significant study conducted at Majmaah University in 2021 evaluated the cybersecurity awareness levels among undergraduate students. The research revealed that while students had some knowledge of cybersecurity concepts, their practical understanding and compliance with security measures were lacking. The study emphasized the need for a combination of passive and proactive educational methods to enhance awareness, suggesting that video-based, text-based, or game-based training could be effective (Alharbi & Tassaddiq, 2021).

### ***Cybersecurity Education in Malaysia***

Another study focused on students at Universiti Teknologi MARA (UiTM) Terengganu, published in 2022, examined the cybersecurity awareness of students during the COVID-19 pandemic. The findings indicated that, despite a reasonable level of awareness regarding cyber threats, students often engaged in risky online behaviors, such as sharing passwords and

accessing unknown websites. The authors called for more structured educational programs to improve students' understanding of cybersecurity and to mitigate risks associated with online activities.

### ***National-Level Initiatives***

Research has also been conducted on national cybersecurity education and awareness initiatives. A 2022 paper assessed the impact of cybersecurity education, awareness raising, and training (CEAT) on internet use at the national level. The authors noted that while there are challenges in implementing effective programs, there is significant promise in using evidence-based strategies to enhance public understanding of cybersecurity threats and safe practices.

### ***CISA Cybersecurity Awareness Program***

The Cybersecurity and Infrastructure Security Agency (CISA) has been actively promoting cybersecurity awareness through national campaigns since 2004. Their initiatives aim to empower the public with knowledge about cyber threats and safe online behavior. The CISA program emphasizes that cybersecurity is a shared responsibility and provides resources to help individuals make informed decisions online. The program's ongoing efforts include promoting Cybersecurity Awareness Month and providing educational materials tailored for various audiences.

### ***EDUCAUSE Resources***

EDUCAUSE has also contributed to the discourse on cybersecurity awareness by offering resources and toolkits for educational institutions. Their focus is on creating a culture of cybersecurity awareness among students and staff, encouraging institutions to implement year-round campaigns and utilize various media to engage the community effectively.

## ***Conclusions and Recommendations***

The literature from 2016 to 2024 indicates that while awareness of cybersecurity issues is growing, significant gaps remain in practical knowledge and behavior among students. Effective cybersecurity education should combine theoretical knowledge with practical applications, utilizing diverse methods to engage learners. Future research should continue to explore the effectiveness of various educational strategies and the long-term impacts of awareness campaigns on behavior change in different populations.

## **Technological Innovations in Cybercrime Detection and Prevention**

According to Dacanay et al. (2024) Cyberattacks have significantly increased in the Philippines in recent years. There were 98.41 thousand cyberattacks in the nation as of June 2021. Online scams virtually tripled during the first half of 2023, as compared to the same period in 2022, while cybercrimes in Metro Manila increased by 152%. The most common kinds of cybercrimes are data breaches, ATM and credit card fraud, and internet scams. Because of its high internet usage, limited cybersecurity knowledge, and inadequate cybersecurity infrastructure, the nation is especially at risk of cyberattacks.

According to Arasa (2024) The Philippines' efforts to become more technologically aware have resulted in improved cybersecurity precautions. To help the public protect themselves, its Cybercrime Investigation Coordinating Center (CICC) has been educating the public about internet scams. The country has welcomed greater foreign investments in cybersecurity, and the CICC has been using the most recent innovations, these are the 3 most recent CICC cybersecurity project in the Philippines:

1. **CitizenWatch Philippines** - is one with the CICC campaign to safeguard our digital

environment.

2. **Consumer Application Monitoring Systems (CAMS)** - A new tool has been developed to ensure the safety of government service apps against cyber threats. The organization developed it on the Zero Defects principle, which is the 9th principle, "Zero Defects Day," which guarantees that businesses have an impact and that everyone gets the same message in the same way.
3. **NCC Group trains future cybersecurity pros** – The Philippines requires local experts to keep advancing cybersecurity in the country. On January 17, 2024, the international cybersecurity company NCC Group opened its first office in Manila. It is also the second office in Southeast Asia for the tech company.

According to Dacanay et al. (2024) Threats to global cybersecurity have increased as a result of cybercriminals taking advantage of networks that were not synchronized during the pandemic. Malware attacks increased by 358% in 2020 over 2019. Cyberattacks then surged by 125% in 2021, continuing to be a threat to people and companies in 2022. These kinds of assaults are common in a number of industries, such as vital infrastructure, government, healthcare, and finance. Phishing, malware, denial-of-service (DoS) attacks, identity-based assaults, supply chain attacks, and Internet of Things (IoT) attacks are among the most prevalent forms of cyberattacks. To defend against potential attacks, it is important that people and organizations keep the latest understanding of the constantly changing cyber threat landscape and have strong cybersecurity measures in place.

In the recent study conducted by Mustapha et al. (2024) it provides a latest innovation in cybersecurity. These cybersecurity innovations are:

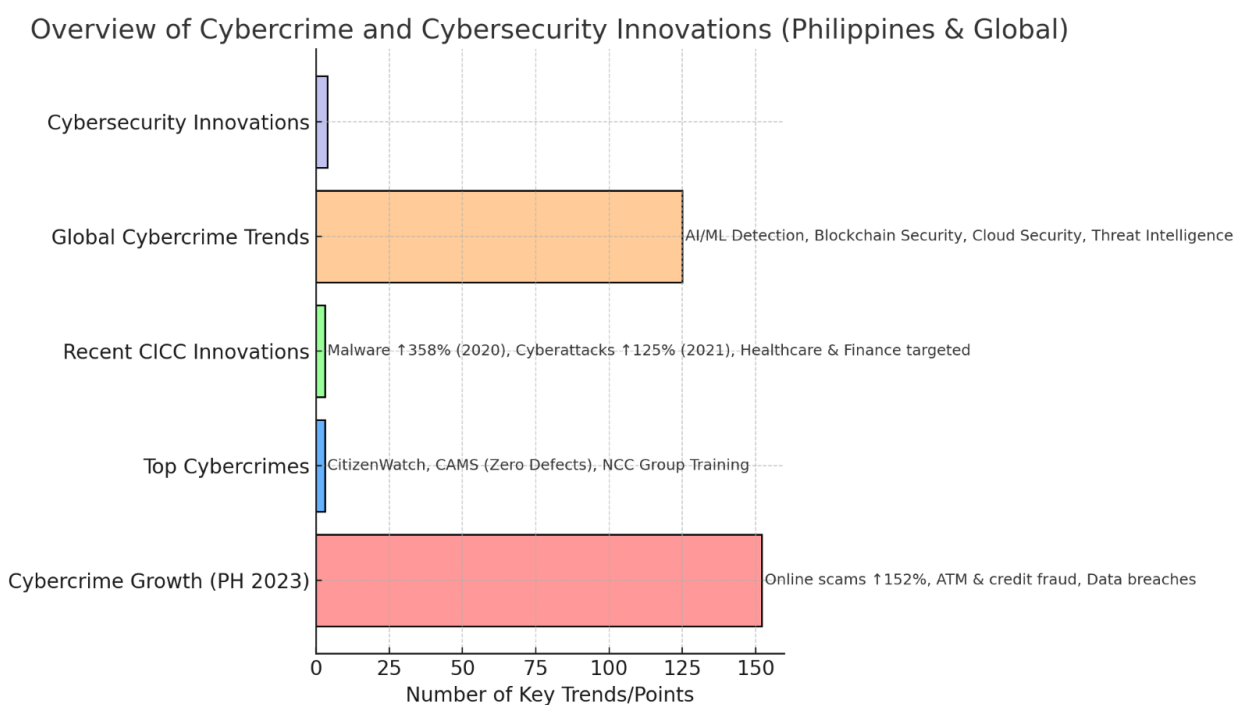
- **Artificial Intelligence and Machine Learning** - Cybersecurity becomes more and

more dependent on AI and ML, which automate threat detection, analysis, and response. Artificial intelligence (AI)-driven systems outperform traditional rule-based solutions in dealing with emerging threats because they can identify patterns in large datasets, spot abnormalities, and anticipate potential attacks. In the fields of proactive threat prevention, malware detection, and network intrusion identification, machine learning is especially useful. These tools convert low-level data into actionable intelligence, enabling quicker and more precise responses to cyber-attacks.

- **Blockchain Technology** – Is a secure, decentralized digital ledger that keeps track of transactions on several computers without the need for a central authority. Every block in the chain includes proof-of-work, transaction data, and a cryptographic hash of the block before it, which keeps the record transparent and unchangeable. By enabling decentralized identity management, enhancing supply chain transparency, and streamlining financial services through real-time transactions and smart contracts, this technology is revolutionizing a number of industries. Blockchain improves cybersecurity by exposing tampering and facilitating safe data transfer. Notwithstanding obstacles such as scalability, interoperability, and certain human-related hazards, blockchain holds great promise for revolutionizing various industries. Current research endeavors to unleash its complete potential.
- **Cloud Security** - It creates new security threats while providing scalable online application, storage, and computing services. Insufficient identity verification, unreliable APIs, and vulnerabilities in web, mobile, and IoT services are major issues. Secure software development processes, robust identity and access management, and improved network defenses designed for cloud environments are all important for effective cloud security. Protecting the privacy and integrity of data requires multi-factor authentication, encryption, and regular surveillance. Resolving these issues is

essential as cloud use rises, particularly in regulated businesses, to guarantee safe and legal operations.

- **Threat Intelligence** - involves gathering and analyzing current information about cyber adversaries' tools, strategies, and goals to proactively defend against threats. TI combines technical signals with open-source data to identify emerging risks, providing a more anticipatory approach than traditional security measures. Key sources of TI include firewall logs, dark web activity, public documents, and social media, while frameworks like MITRE ATT&CK help model adversary behavior for tactical responses.



- Cybercrime Growth (PH 2023): Online scams increased by 152%.
- Top Cybercrimes: Data breaches, ATM/credit fraud, and internet scams dominate.
- Recent CICC Innovations: CitizenWatch, CAMS (Zero Defects principle), and NCC

Group's cybersecurity training.

- **Global Cybercrime Trends:** Malware surged 358% in 2020, attacks rose 125% in 2021, with healthcare and finance frequently targeted.
- **Cybersecurity Innovations:** AI/ML, Blockchain, Cloud Security, and Threat Intelligence play critical roles in protection.

## Gaps in the Literature

The reviewed literature and studies on cybercrime in the Philippines reveal significant gaps and areas for further exploration, particularly in understanding the dynamics of public awareness and the effectiveness of existing educational initiatives. This synthesis aims to highlight these gaps and propose directions for future research, particularly in the context of the development of the "ClickSmart" informative AI chatbot-supported website.

Below are the gaps in the Literature.

1. **Underreporting of Cybercrime:** A recurring theme in the literature is the underreporting of cybercrime incidents, especially in low-income areas. Many victims perceive their losses as too insignificant to warrant reporting, which skews data and hampers effective law enforcement responses. Future studies should focus on qualitative research to understand the psychological and socio-economic factors influencing this underreporting phenomenon.
2. **Public Awareness and Education:** While there are initiatives by agencies like the Philippine National Police (PNP) to raise awareness, studies indicate that a significant portion of the population remains uninformed about cyber threats and protective measures. Research should explore the effectiveness of different



educational strategies, particularly those that utilize digital platforms to reach a broader audience.

3. **Technological Adaptation by Law Enforcement:** The literature suggests that law enforcement agencies are often ill-equipped to handle modern cybercrime due to outdated training and technology. Investigating how technological innovations can be integrated into law enforcement training could provide valuable insights into enhancing their capacity to combat cybercrime effectively.
4. **Demographic Vulnerabilities:** The impact of demographic factors on vulnerability to cybercrime has not been thoroughly examined. Future research should analyze how variables such as age, gender, and socio-economic status correlate with susceptibility to different types of cyber threats.
5. **Evolving Nature of Cyber Threats:** The rapid evolution of cyber threats, including AI-driven attacks and new fraud methods involving cryptocurrencies, necessitates ongoing research into emerging trends. A longitudinal study could help track these changes over time and assess their implications for public safety and policy.

### **Synthesis of the Reviewed Literature and Studies**

The synthesis of existing literature underscores a critical need for enhanced public education regarding cybersecurity practices. The rise in reported cybercrimes correlates strongly with increased internet usage; thus, it is imperative that educational initiatives are tailored to address this growing digital engagement. The "ClickSmart" website aims to bridge this gap by providing accessible resources that simplify complex cybersecurity concepts for users.

### **Key Findings:**

- **Cybercrime Trends:** The increase in online activities during special occasions has been linked to spikes in certain types of scams, highlighting the need for targeted awareness campaigns during these periods.
- **Role of AI Chatbots:** The integration of AI chatbots in educational platforms has shown promise in facilitating immediate user engagement and providing assistance regarding cybersecurity queries.
- **Community-Based Approaches:** Research indicates that localized awareness programs can significantly enhance community resilience against cyber threats. The proposed website will incorporate community-specific data to inform users about prevalent threats in their areas.

### **Proposed Directions for Future Research:**

1. **Effectiveness of informative Learning Tools:** Investigate how informative tools on platforms like ClickSmart can enhance user engagement and retention of cybersecurity knowledge.
2. **Longitudinal Studies on Cybercrime Awareness:** Conduct studies that measure changes in public awareness and reporting behavior before and after implementing educational initiatives.
3. **Cross-Regional Comparisons:** Compare cybercrime trends and public awareness levels across different regions to identify best practices that can be adopted nationwide.

In conclusion, addressing these gaps through targeted research will not only contribute to academic discourse but also provide practical solutions for improving public awareness and response to cybercrime in the Philippines. The development of ClickSmart represents a

proactive step towards fostering a more informed and resilient community against the evolving landscape of cyber threats.

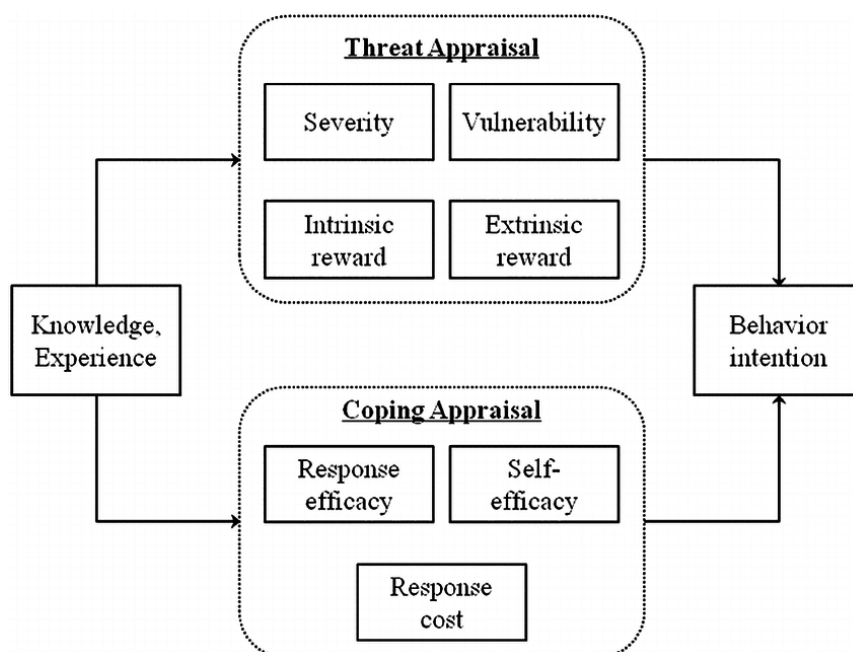
### Chapter 3: Methodology

This chapter explained how the study was conducted and how 'ClickSmart,' an informative website for improving cybersecurity awareness with AI, was developed. It covered the research methods, respondents, instruments, and procedures used in collecting and analyzing data to answer research problems.

#### Frameworks Used

##### *Theoretical Framework: Protection Motivation Theory*

This study is based on Protection Motivation Theory (PMT) by R.W. Rogers in 1975, which helps explain how people decide to protect themselves from threats like cybercrime. PMT suggests that individuals are more likely to take protective actions if they believe cyber threats are serious and think something might happen to them. Also, being aware of what actions helps them to stay safe against these Cybercrime Activities (How can protection motivation theory be used to explain cyber security behaviors?, 2024).



*Figure 1: PMT Diagram*

**PMT has two main parts:**

1. **Threat Appraisal:** This is when people think about how serious a threat is. They consider how bad cybercrime can be and whether they might become a victim. If they believe cybercrime is a big risk, they are more likely to take steps to protect themselves.

- Severity: How bad do you think the threat is? For example, how harmful could a cyberattack be?
- Vulnerability: How likely do you think it is that the threat will affect you personally?
- Intrinsic Reward: What benefits or convenience do you get by not doing anything to protect yourself (e.g., saving time or effort)?
- Extrinsic Reward: What outside benefits (like saving money or getting things done faster) do you get by ignoring protection?

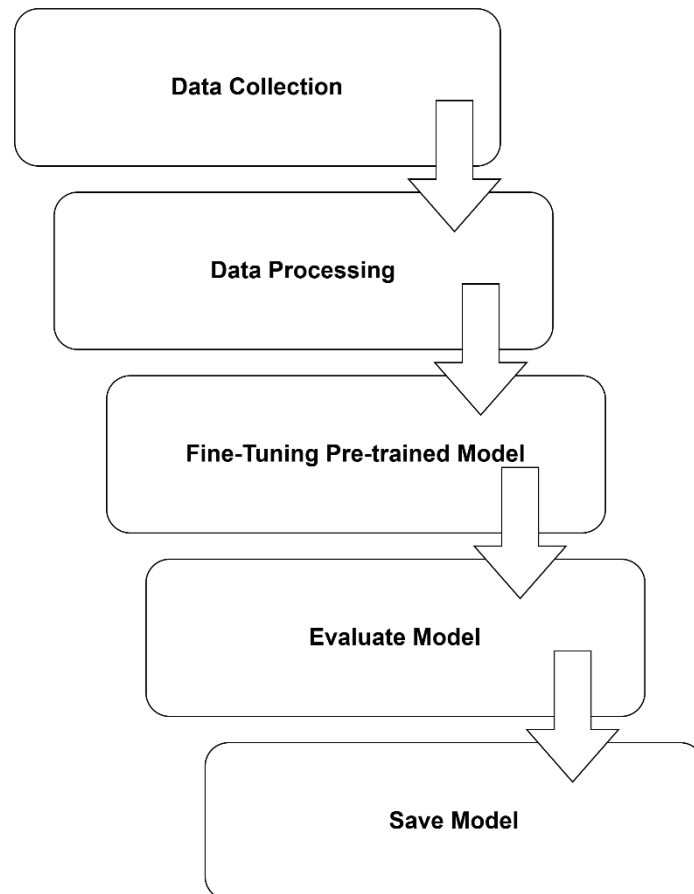
2. **Coping Appraisal:** In this part, people think about how they can handle the threat. They look at ways to protect themselves, like creating strong passwords or recognizing phishing scams, and how sure they feel about using these methods. If they think they can effectively keep themselves safe, they are more likely to act.

- Response Efficacy: Do you think the protective action (e.g., using strong passwords) will actually work?
- Self-Efficacy: Do you feel confident in your ability to take protective steps (like spotting a scam)?

- **Response Cost:** What does it "cost" you to take action? This could be time, effort, or money involved in protecting yourself.

This model explains why some people take steps to protect themselves online while others do not. It depends on how serious they perceive the threat to be and whether they feel capable of taking the necessary actions to stay safe. By raising awareness about the severity of cybercrime and educating people on protective measures, individuals can become more engaged and proactive in safeguarding themselves and reporting incidents.

### ***Framework for Chatbot Model***



*Figure 2: Model Workflow*

## Data collection

The first step in chatbot development is data collection; the researcher collects cybercrime-related information to train the model. This step is crucial because gathering relevant and reliable data helps the model generate accurate and informative responses for users.

The primary source of the dataset includes public websites, official government portals (such as the PNP Anti-Cybercrime Group and NBI Cybercrime Division and other law government offices), and online platforms of cybersecurity agencies, including their official websites and verified Facebook pages. These sources were chosen to ensure that the dataset consists of authentic, up-to-date, and credible information on cybercrime prevention, online scams, and digital security measures.

The researcher will store the collected data in a CSV (Comma-Separated Values) file, creating a structured and organized dataset for efficient processing and training. The dataset consists of three key columns:

- Question: The cybercrime-related query users might ask.
- Answer: The chatbot's expected response is based on factual information.
- Source: The reference for the answer, ensuring transparency and reliability.

This structured format allows the chatbot to accurately retrieve information, match user queries with appropriate responses, and ensure the credibility of provided answers by citing reliable sources.

## Data Processing

After the data collection phase, the dataset undergoes preprocessing to ensure it is structured, cleaned, and optimized for training the chatbot. The key steps in data processing include:

- **Rephrasing the Questions** – Since users may phrase the same question in different ways, the researchers manually rephrased select questions while retaining the same corresponding answers. This process enhances the model's ability to recognize variations of the same query, thereby improving its response accuracy.
- **Cleaning and Preprocessing the Dataset** – The dataset was cleaned and process by:
  - Correcting grammatical errors and spelling inconsistencies to enhance data quality.
  - Manually removing duplicate questions to prevent redundancy.
  - Manually filtering out irrelevant or unrelated information that could negatively affect the model's training.
  - Converting all questions to lowercase using the `str.lower()` method from the pandas library to maintain uniform formatting.
  - Dropping the "Source" column using the `drop()` method from the pandas, as it is not required for training the model.
- **Tokenizing the Dataset** – After cleaning and preprocessing, the dataset is tokenized to prepare it for model training. Tokenization is an essential step which the text is converted into numerical tokens (IDs) that the model can process. Padding is also applied to ensure that all inputs have the same length, preventing shape mismatches during training.



- **Splitting the Dataset into Training and Validation Sets** – To ensure effective model evaluation, the dataset was divided into two subsets:
  - Train dataset – Used to fine-tune the model and optimize its performance.
  - Validation dataset – Saved separately and used to evaluate the chatbot's responses after training.

### **Fine-Tune the Pre-trained Model**

Fine-tuning is the process of adapting a pretrained model to a specific dataset to improve its performance for a particular task. For this study, the researcher will use GPT-2 (Generative Pretrained Transformer 2) as the language model. GPT-2 is a large-scale transformer-based model developed by OpenAI, designed to generate human-like text using deep learning. It is highly effective in natural language generation (NLG), text completion, summarization, and question-answering tasks after being pretrained on a diverse set of online text data. GPT-2 is widely utilized in chatbots, automated content generation, and conversational AI systems. The objective of fine-tuning is to enhance the chatbot's ability to generate accurate, informative, and contextually relevant responses to cybercrime-related queries.

To fine-tune the model, the researcher will use the `TrainingArguments` class from the `transformers` library to define hyperparameters that optimize learning efficiency while preventing overfitting.

After defining the training arguments, the dataset was processed and passed to the `Trainer` class, which automates the training loop and evaluation. The `Trainer` object was initialized with the fine-tuned GPT-2 model, training parameters, and dataset. The fine-tuning

process was executed using the `train ()` method, enabling the model to learn patterns from the dataset and improve its ability to generate accurate and contextually relevant responses.

The following hyperparameters were used for this study:

Hyperparameter	Value	Why we chose this Hyperparameter	Why we chose this value
num_train_epochs	3	Determines how many samples are processed per training step.	Three epochs strike a balance between learning and overfitting; more epochs could lead to memorization instead of generalization.
per_device_train_batch_size	2	The number of samples processed per training step.	A small batch size prevents memory overload on the GPU while maintaining stable training.
per_device_eval_batch_size	1	Defines how many samples are used per evaluation step.	Using batch size 1 mimics real-world chatbot interactions, where a single query is processed at a time.
warmup_steps	500	Gradually increases the learning rate at the start of training.	Prevents sudden jumps in learning rate, allowing smoother convergence and reducing instability.
weight_decay	0.01	Applies regularization to reduce overfitting.	A value of 0.01 is commonly used in NLP models to maintain generalization without excessive constraint.
evaluation_strategy	"epoch"	Defines when the model should be evaluated.	Evaluating at the end of each epoch provides structured performance tracking without interrupting training too often.
save_strategy	"epoch"	Specifies when to save model checkpoints.	Saving after every epoch ensures that the best-performing model version is available for retrieval.
load_best_model_at_end	True	Ensures that the best-performing checkpoint is used after training.	Prevents the risk of using the last-trained checkpoint, which may not be the most optimal version of the model.

*Table 1: Hyperparameter Selection for Fine-Tuning*

## Evaluate Model

After fine-tuning the model, it is necessary to evaluate its performance to ensure that it generates accurate, relevant, and contextually appropriate responses to cybercrime-related queries. The evaluation process involves testing the chatbot using a separate validation dataset and measuring its performance using evaluation metrics.

- Evaluation Method
  - The model is evaluated by comparing its generated responses to ground-truth answers from the dataset. The evaluation dataset consists of questions that were not included in the training phase, ensuring that the model is tested on previously unseen data to measure its generalization capability.
  - To ensure consistency in its responses, the fine-tuned GPT-2 model is set to evaluation mode (`model.eval()`) before generating answers. For each question in the validation dataset, the chatbot produces a response, which is then compared against the correct answer using evaluation metrics.
- Evaluation Metrics
  - Exact Match (EM): Measures whether the chatbot's response exactly matches the correct answer. This is a strict metric, where even small variations in wording can affect the score. EM is useful for measuring word-for-word accuracy, but it does not account for cases where the chatbot provides a paraphrased yet correct response.
  - BERTScore: Uses transformer-based embeddings to evaluate the semantic similarity between the chatbot's response and the ground-truth answer. Unlike EM, BERTScore considers synonyms, paraphrasing, and contextual meaning, making it a more flexible evaluation metric for chatbots.

Since chatbots require a conversational and context-aware evaluation, BLEU, ROUGE, and METEOR were not prioritized, as they are primarily used for machine translation and text summarization tasks. EM and BERTScore were chosen because they provide a balanced evaluation of both exact correctness (EM) and semantic similarity (BERTScore).

### **Save Model**

Once training was completed, the fine-tuned model and tokenizer were saved for deployment and future use. This step ensures that the model is stored in a manner that allows it to be easily loaded and used to generate responses in real-world applications. The Hugging Face transformers library provides a straightforward method for saving both components.

The tokenizer was saved using the `save_pretrained()` method, and the fine-tuned GPT-2 model was also saved using `save_pretrained()`. Both were stored in the "fine\_tuned\_gpt2" directory, ensuring accessibility for further evaluation, testing, or integration into the chatbot system.

### **Research Design**

This study used an exploratory research design with a mixed-methods approach, combining both qualitative and quantitative methods to provide an understanding of cybercrime trends and user behavior regarding cybersecurity. This design aimed to:

- Analyze the types of cybercrime incidents reported in Quezon City, based on data from the Philippine National Police Anti-Cybercrime Group (PNP ACG).
- Examine how often different types of cybercrime cases occur in various districts from January to June 2024.

- Assess the number of reported cybercrime victims from the 4th quarter of 2023 and 1st quarter of 2024.

### **Research Locale**

This study focused on Quezon City, specifically examining cybercrime activities reported in Districts 3-6. The data and information were collected through interviews at two police stations: QCPD Kamuning and the QCPD Headquarters, where the Anti-Cybercrime Group (ACG) team operated. These locations served as the main sites for gathering insights from police officers about local cybercrime issues and trends.

### **Data Gathering Procedure**

Data collection was conducted in collaboration with the National University and the Philippine National Police Anti-Cybercrime Group (PNP ACG). The methods used for collecting data included:

- **Formal Request:** A formal request letter was written and signed by the thesis adviser to obtain permission from the PNP for interviews and access to data.
- **Interviews:** Semi-structured interviews were conducted with local law enforcement personnel. This provided the researchers with an opportunity to clarify issues and questions that arose during the interview process. The interviews were recorded (with the interviewees' consent) using a smartphone to ensure accuracy and create verifiable documentation for the study. The researcher then manually transcribed the recordings to capture all relevant information and insights from the interviews.
- **Cybercrime Data:** Quantitative data was gathered from PNP ACG reports on cybercrime incidents in Quezon City, focusing on the nature of cybercrime cases and

the number of incidents reported between January and June 2024, as well as information on the number of victims from the 4th quarter of 2023 to the 1st quarter of 2024.

### **Research Instrument**

The research instrument included a semi-structured interview guide aimed at collecting detailed responses regarding cybercrime issues and trends in Quezon City. The questionnaire was developed based on the study's objectives and consisted of eleven (11) questions in total. The first part included four (4) questions focused on seminars, the second part contained two (2) questions related to the inquiry process, and the third part consisted of six (6) questions concerning statistical data on cybercrime incidents.

### **Respondents of the Study**

The study focused on districts within Quezon City that were identified in the data provided by the PNP ACG. Purposive sampling was used as a non-probability sampling technique in which researchers intentionally selected participants who possessed specific characteristics or knowledge relevant to the study, ensuring that the data gathered was insightful and applicable to the research objectives.

Using this approach, researchers selected respondents based on their knowledge of local cybercrime issues and their willingness to participate in the study. However, the researcher also employed convenience sampling, which involved selecting participants who were available and willing to take part in the study at that time.

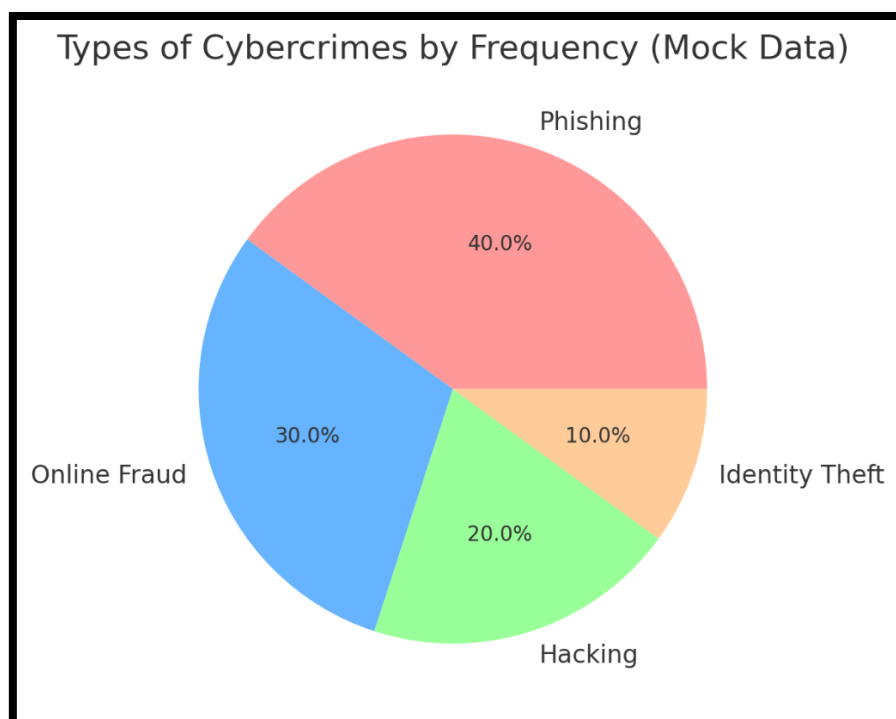
This was important because PNP officers had busy schedules and many responsibilities during work hours. Therefore, while the researcher intended to gather information from PNP officers, whichever officer was available for the interviews was accepted. This approach

allowed the researcher to gather a variety of perspectives while still concentrating on the appropriate group.

### Data Analysis

Data analysis involved both qualitative and quantitative methods:

- **Qualitative Analysis:** Data from interviews with law enforcement and cybersecurity experts were transcribed and analyzed to identify common themes and insights related to cybercrime in Quezon City.
- **Quantitative Analysis:** Statistical analysis of cybercrime data from PNP ACG reports was conducted to identify trends, patterns, and the frequency of cybercrime incidents in the districts covered in the study.



This pie chart categorizes different types of cybercrimes and their relative occurrences. It offers insights into which types of offenses are most prevalent, helping users become more aware of common threats.

The following charts represent sample visualizations that utilizes during the analysis phase of this research. They serve as examples of how real data once collected from PNP ACG reports analyzes and presents on the website.

### **Ethical Considerations**

Before the study was conducted, the PNP officers of the Quezon City Police District (QCPD) and the Quezon City Anti-Cybercrime Group (QC ACG) received a briefing detailing the purpose of the research. Informed consent will be obtained, allowing the officers to voluntarily decide whether to participate in the study.

To ensure ethical integrity, all information gathered from the PNP officers was treated with the highest level of confidentiality. This includes protecting the anonymity of participants and the information provided is for project purposes only. No identifying details will be disclosed in the study findings. The research complied with the provisions of Republic Act No. 10173, known as the Data Privacy Act, to prevent any potential harm to the respondents and to uphold their right to privacy.



## Chapter 4: Results and Discussion

This chapter presented an analysis of cybercrime data collected from interviews and data from Districts 3-6 in Quezon City, focusing on the nature and frequency of reported cases. It also included the evaluation of the classification of the training dataset for the AI chatbot.

**Note:** It is important to understand that the insights drawn from the data showed relationships between certain factors, but they did not prove that one factor directly caused another. The analysis was based on the numbers provided, and while these patterns appeared to be logical, they were not definitive conclusions. Therefore, these insights should be viewed as possible explanations based on the data rather than absolute facts.

### Comparative Analysis of Cybercrime Cases: Q4 2023 vs. Q1 2024

Nature of Cybercrime Cases	4th Quarter of 2023	1st Quarter of 2024
Art. 315 of RPC - Swindling / Estafa (Online Scam)	188	255
Sec. 4(a)1 of R.A. 10175 (Illegal access)	113	128
R.A 8484 (ATM Credit Card Fraud)	26	53
Sec. 4(b)3 of R.A. 10175 (Computer Related Identity Theft)	28	42
Sec. 4(c) of R.A. 10175 (Online Libel)	16	17
Art. 282 of RPC (Online Threat) in rel. to Sec. 6 of R.A. 10175	8	14
Art. 286 of RPC (Grave Coercion) in rel. to Sec. 6 of R.A. 10175	3	6
TOTAL CASES	382	515

*Table 2: Data Count*

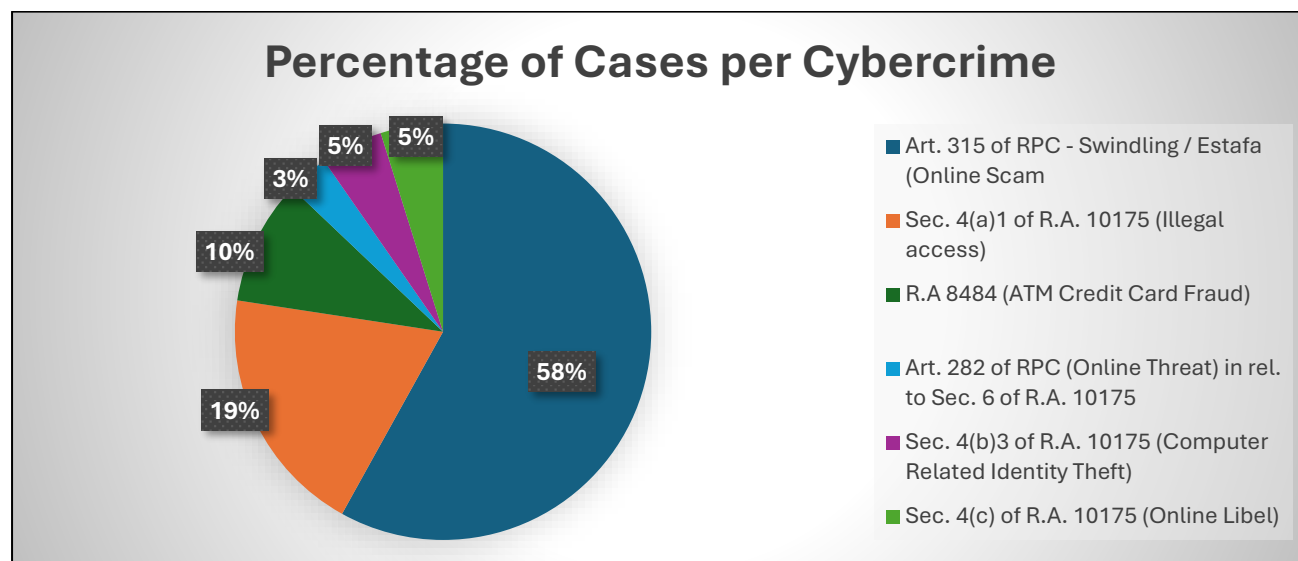
From the data, the total number of reported cybercrime cases in Quezon City increased by 38.4 from Q4 2023 to Q1 2024.

Nature of Cybercrime Cases	Increased By
Art. 315 of RPC - Swindling / Estafa (Online Scam)	+67
Sec. 4(a)1 of R.A. 10175 (Illegal access)	+15
R.A 8484 (ATM Credit Card Fraud)	+27
Sec. 4(b)3 of R.A. 10175 (Computer Related Identity Theft)	+14
Sec. 4(c) of R.A. 10175 (Online Libel)	+1
Art. 282 of RPC (Online Threat) in rel. to Sec. 6 of R.A. 10175	+6
Art. 286 of RPC (Grave Coercion) in rel. to Sec. 6 of R.A. 10175	+3
TOTAL CASES	+133

*Table 3: Data Count Increased*

Table 3 shows that **online scams (Swindling/Estafa)** had the biggest increase in cases, rising from **188 in Q4 2023 to 255 in Q1 2024**, an increase of **67 cases**.

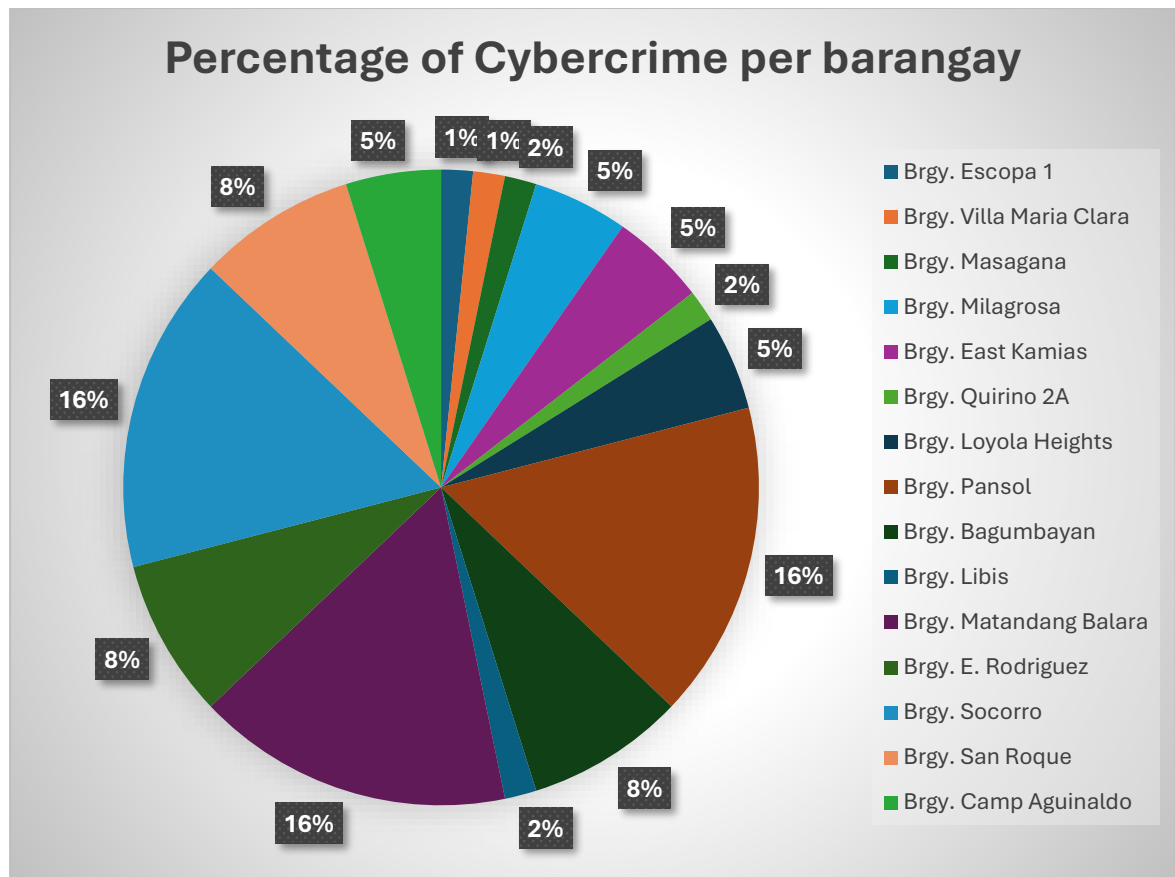
#### Cybercrime Analysis of District 3 in Quezon City (January to June of 2024)



*Chart 1: Percentage of Total Cybercrime Cases in District 3*

Chart 1 shows that **online scams** made up 58% of the total reported cybercrime cases in District 3, making them the most common in the area. This was followed by **illegal access** at 19% and credit card theft at 10%. The high percentage of online scams suggests the growing

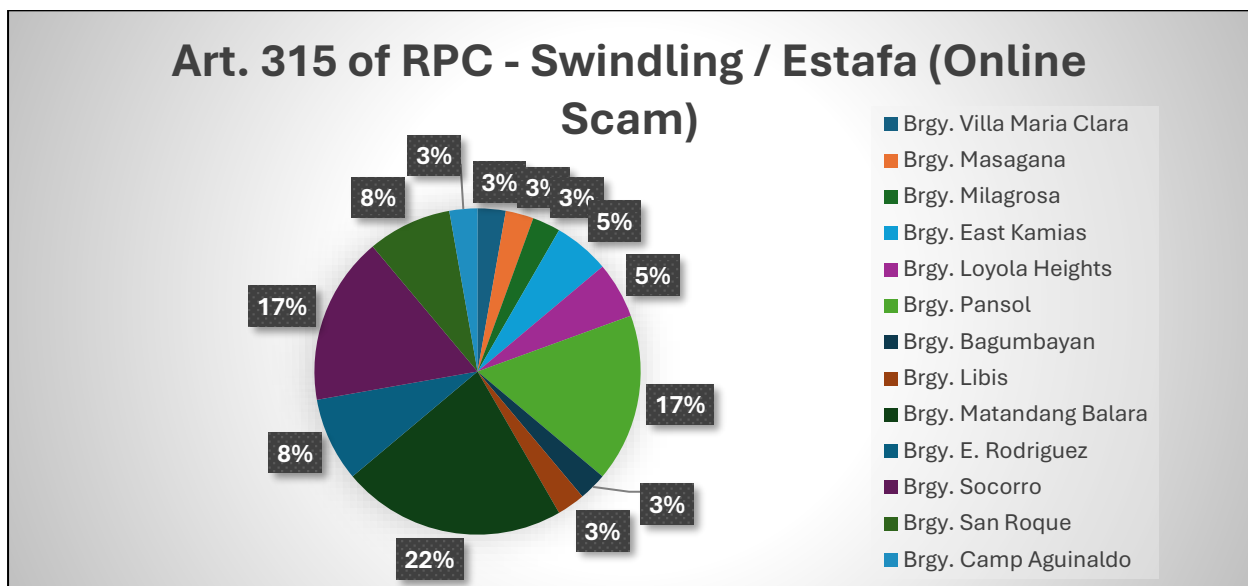
use of social media and online marketplaces, which cybercriminals frequently take advantage of to deceive people.



*Chart 2: Percentage of cybercrime cases per barangay in District 3*

Chart 2 illustrates the percentage of cybercrime per barangay. In this case it shows that three (3) barangays in district 3 have the same number of cases. **Barangay Socorro, Matandang Balara and Loyola Heights** with a 16% percent cases.

---

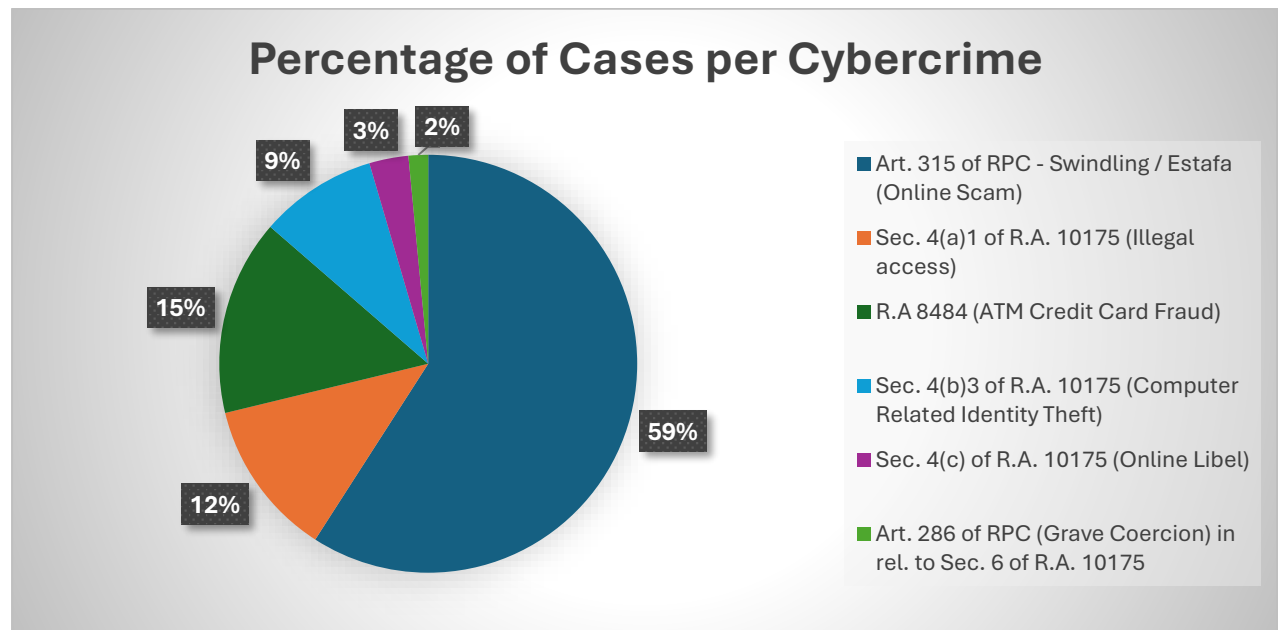


*Chart 3: Percentage of online scam cases per barangay in District 3*

Chart 3 shows that **Barangay Matandang Balara** has the most online scam cases in District 3, making up 22% of all the cases. This means online scams are more common in this barangay compared to the others in the district.

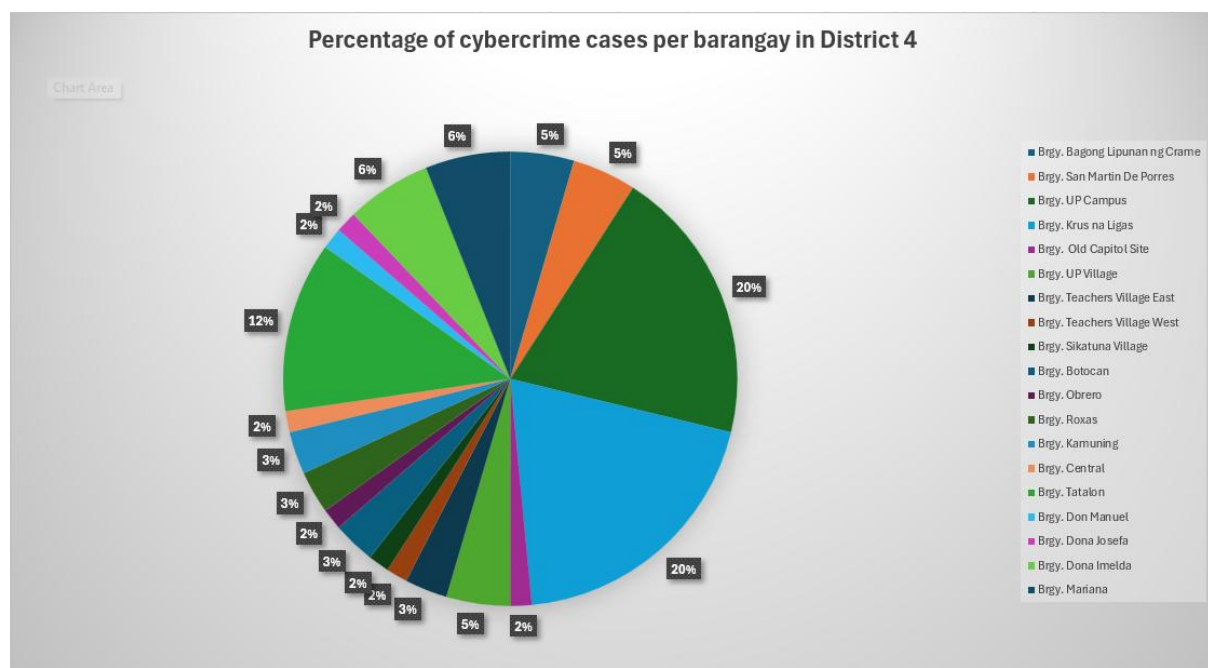
---

### Cybercrime Analysis of District 4 in Quezon City (January to June of 2024)



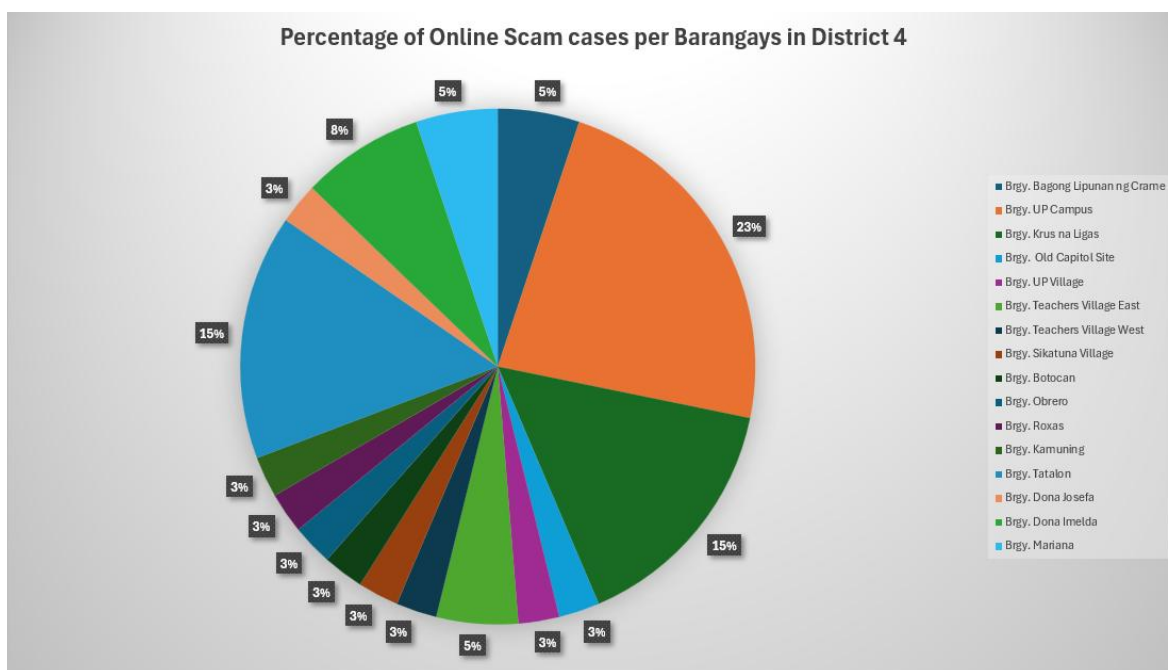
*Chart 4: Percentage of Total Cases per Cybercrime in District 4*

Chart 4 illustrates the percentage cases of cybercrime per barangay based on active cybercrime in the district 4. In this case, it shows that **Swindling/Estafa(Online Scam)** is the most prevalent cybercrime for district 4 in Quezon City with a percentage of 59% and **Grave Coercion** is the least prevalent with a 3% percentage.



*Chart 5: Percentage of cybercrime cases per barangay in District 4*

Chart 5 illustrates the percentage of cybercrime per barangay. In this case it shows that two (2) barangays in district 4 have the same number of cases. **Barangay UP Campus** and **Krus na Ligas** with a 20% percent cases.

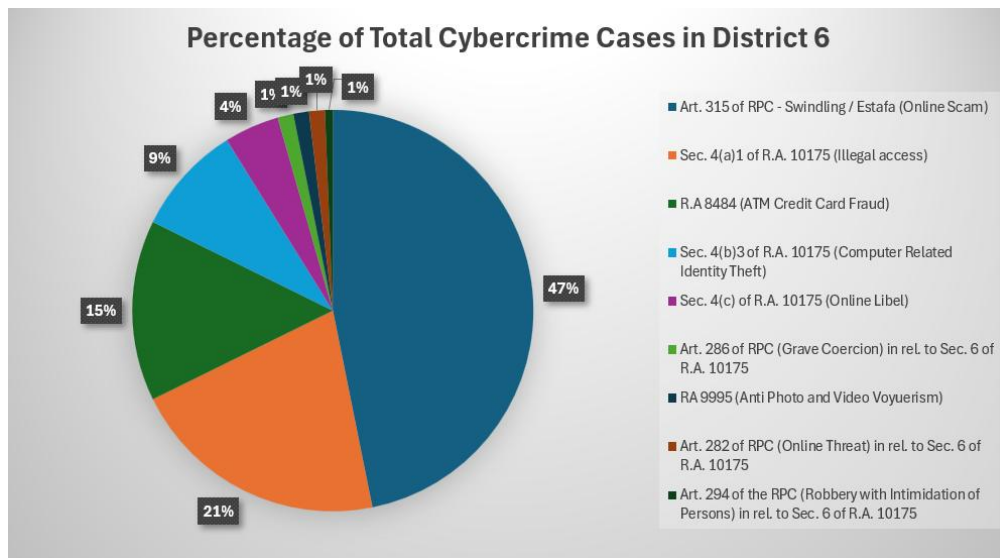


*Chart 6: Percentage of Online Scam cases per Barangays in District 4*

Chart 6 illustrates the percentage of cybercrime per barangay. In this case it shows that **Barangay UP Campus (23%)** has the most cases of online scam within the district 4 of Quezon City. Followed by **Barangay Krus na Ligas** that has 15% cases

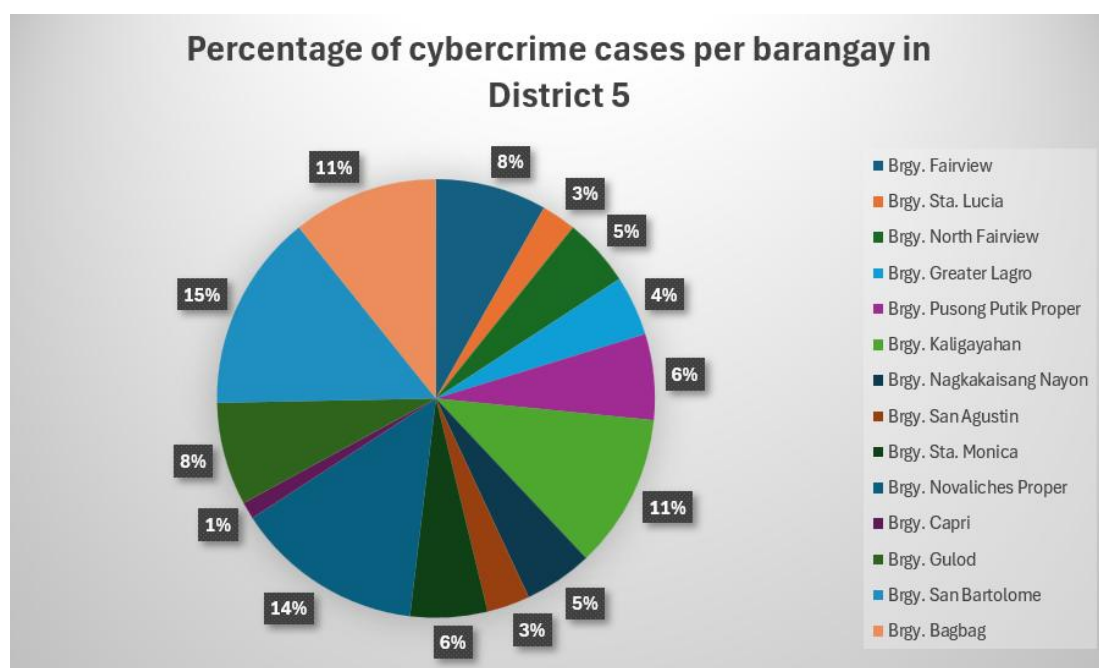
---

### Cybercrime Analysis of District 5 in Quezon City (January to June of 2024)



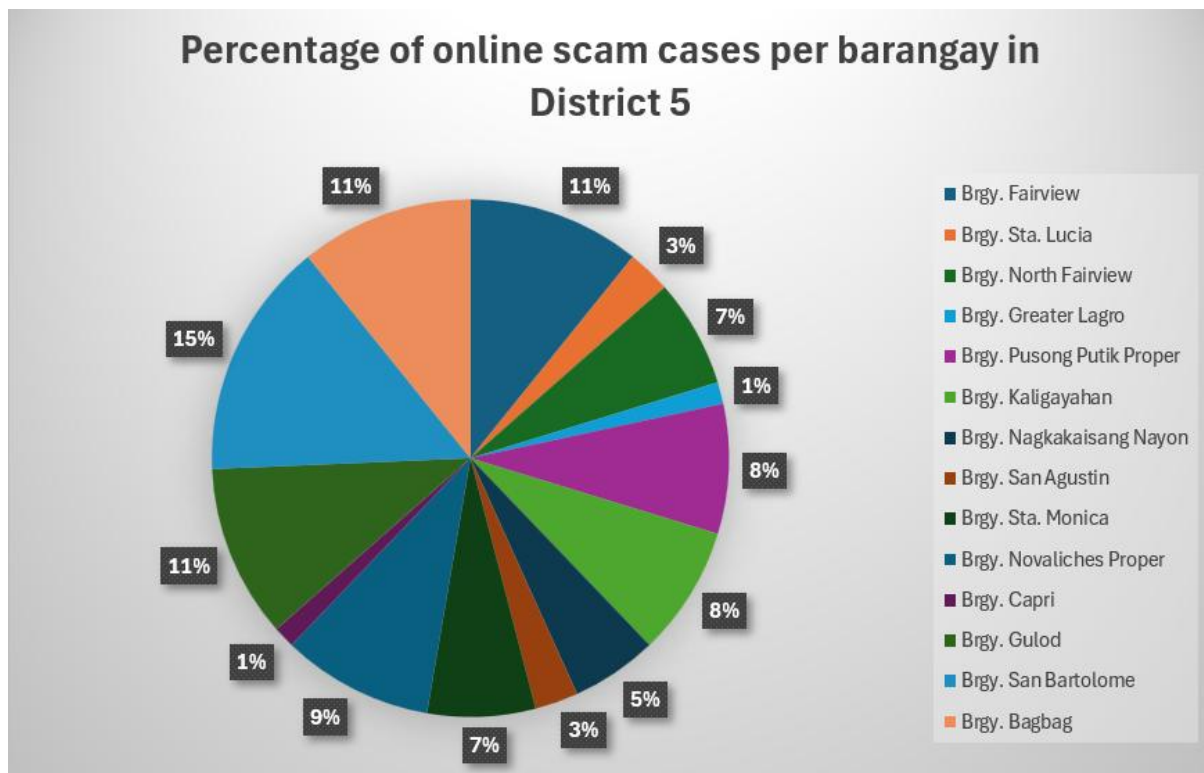
*Chart 7: Percentage of Total Cybercrime Cases in District 5*

Chart 7 illustrates the percentage cases of cybercrime per barangay based on active cybercrime in the district 5. In this case, it shows that **Swindling/Estafa(Online Scam)** is the most prevalent cybercrime for district 5 in Quezon City with a percentage of 47% and both **Grave Coercion, Video Voyuerism and Online Threat** are the least prevalent with a 1%.



*Chart 8: Percentage of cybercrime cases per barangay in District 5*

Chart 8 illustrates the percentage of cybercrime per barangay. In this case it shows that **Barangay San Bartolome (15%)** has the highest cybercrime cases in district 5 followed by **barangay Novaliches Proper (14%)**.



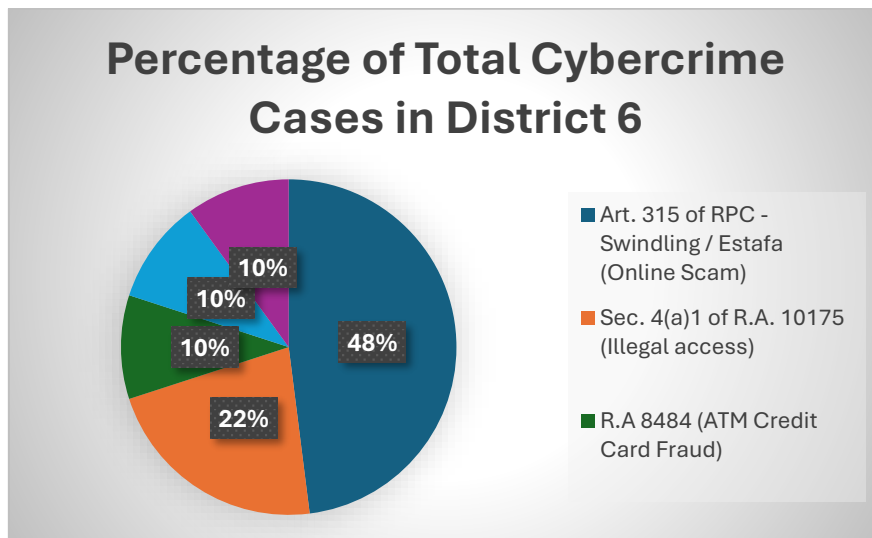
*Chart 9: Percentage of online scam cases per barangay in District 5*

Chart 9 illustrates the percentage of cybercrime per barangay. In this case it shows that **Barangay San Bartolome (15%)** has the most cases of online scam within the district 4 of Quezon City. On the other hand, **both barangay Greater Lagro and Capri** has the least of online scam with a 1% case.

---

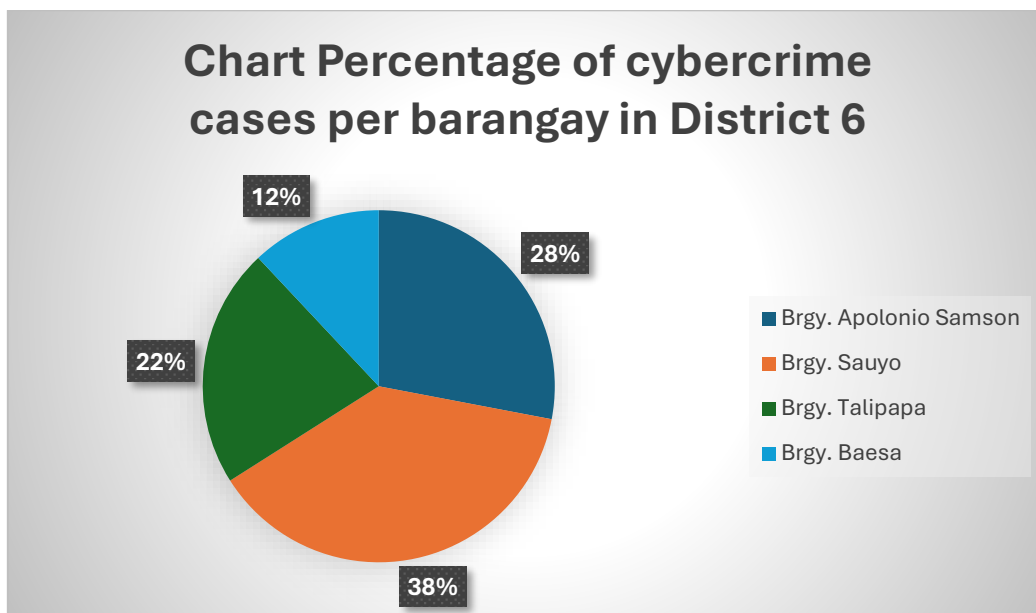


### Cybercrime Analysis of District 6 in Quezon City (January to June of 2024)



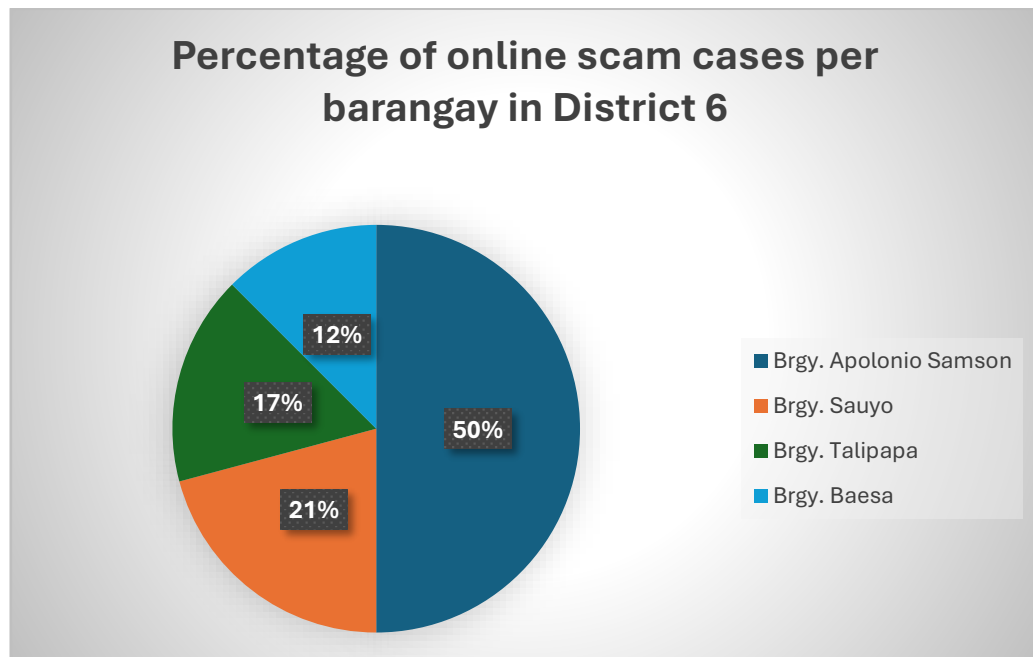
*Chart 10: Percentage of Total Cybercrime Cases in District 6*

Chart 10 illustrates the percentage cases of cybercrime per barangay based on active cybercrime in the district 6. In this case, it shows that **Swindling/Estafa(Online Scam)** is the most prevalent cybercrime for district 10 in Quezon City with a percentage of 48%.



*Chart 11: Percentage of cybercrime cases per barangay in District 6*

Chart 11 illustrates the percentage of cybercrime per barangay. In this case it shows that **Barangay Sauyo (38%)** has the highest cybercrime cases in district 6 followed by barangay **Apolonio Samson (28%)**.



*Chart 12: Percentage of online scam cases per barangay in District 6*

Chart 12 illustrates the percentage of cybercrime per barangay. In this case it shows that **Barangay Apolonio Samson (50%)** has the most cases of online scam within the district 6 of Quezon City. On the other hand, **barangay Baesa (12%)** has the least cases of online scam.

---

### **Summary of Data Across Districts in Quezon City (January–June 2024)**

Across all four districts analyzed (Districts 3 to 6), online scams consistently account for the highest percentage of reported cybercrime cases. On average, online scams make up over 50% of total cybercrime reports, indicating that fraudsters frequently exploit digital platforms to deceive victims.

District	Online Scam Cases (%)	Barangay with Highest Cybercrime Cases	Actual Number of Online Scam Cases	Total Cybercrime Cases
District 3	58%	Matandang Balara (16%) Barangay Socorro (16%) Barangay Loyola Heights (16%)	36	62
District 4	59%	UP Campus (20%) Krus na Ligas (20%)	39	66
District 5	47%	San Bartolome (15%)	74	158
District 6	48%	Barangay Sauyo (38%)	36	50

*Table 4: Online Scam Cases Across Districts*

**Observations:**

District 5 had the highest number of cybercrime cases (158) and the most online scam cases (74), even though online scams made up only 47% of all cases. This meant that while online scams were the most common, other crimes like identity theft and illegal access also occurred frequently in this district. Barangay San Bartolome (15%) had the most cybercrime cases in District 5, making it one of the areas most affected by online fraud.

In District 4, online scams accounted for the largest percentage (59%) of cybercrime cases, but the total number of cases (66) was much lower than in District 5. This meant that while online scams were the most reported crime, overall cybercrime in this district was not as high as in others. The barangay with the most online scam cases was UP Campus (23%), likely because it had many students who frequently used online shopping and digital platforms, making them easy targets for scammers and Krus na Ligas (23%).

Districts 3 and 6 had the same number of online scam cases (36 each), but District 6 had fewer total cybercrime cases (50) compared to District 3 (62). In District 3, Matandang Balara (22%) had the most online scam cases, possibly because many people in the area bought

and sold items online also for both barangay Socorro and Loyola Heights (22%). In District 6, Apolonio Samson (15%) recorded the highest online scam cases, showing that online scams were a major issue in this barangay.

Finally, District 6 had the lowest total number of cybercrime cases (50), but online scams still made up a large portion (48%). This showed that even in areas where cybercrime was less frequent, online scams remained a major problem.

Cybercrime Type	District 3	District 4	District 5	District 6
Art. 315 of RPC - Swindling / Estafa (Online Scam)	36	39	74	24
Sec. 4(a)1 of R.A. 10175 (Illegal access)	12	8	33	11
R.A 8484 (ATM Credit Card Fraud)	6	10	23	5
Art. 282 of RPC (Online Threat) in rel. to Sec. 6 of R.A. 10175	2	0	2	5
Sec. 4(b)3 of R.A. 10175 (Computer Related Identity Theft)	3	6	14	5
Sec. 4(c) of R.A. 10175 (Online Libel)	3	2	7	0
Art. 286 of RPC (Grave Coercion) in rel. to Sec. 6 of R.A. 10175	0	1	2	0

RA 9995 (Anti Photo and Video Voyuerism)	0	0	2	0
Art. 294 of the RPC (Robbery with Intimidation of Persons) in rel. to Sec. 6 of R.A. 10175	0	0	1	0

*Table 5: Breakdown of Cybercrime Cases Across Districts*

### **Qualitative Analysis of Cybercrime Trends Based on Interviews**

To better understand the data gathered from the Philippine National Police – Anti-Cybercrime Group (PNP-ACG), interviews were conducted with PNP officers. These interviews helped explain the patterns found in the data and supported the researchers' goal of raising public awareness. By gathering insights directly from experts, this section provided a deeper look into the causes of cybercrime, challenges in reporting, and possible solutions.

#### ***How Does the PNP Handle Cybercrime Reports, and Why Do Many Cases Go Unreported?***

Data from **PNP-ACG records** indicate that online scams (**Swindling/Estafa**) increased from **188 to 255 cases (+67)** between **Q4 2023** and **Q1 2024**, making them the most frequently reported cybercrime. However, despite the increasing number of reports, law enforcement suggests that many cases remain unreported, particularly lower-value scams.

According to **Colonel June Paolo Abrazado (Kamuning Police Station)**, cybercrime is **one of the most underreported crimes** due to **victim hesitancy, inconvenience in the reporting process, and perceived insignificance of losses**:

*“Cybercrime is heavily underreported. Victims losing ₱500 to ₱2,000 often choose not to report because the process is too inconvenient. The cost of transportation to the police station alone discourages them.” (Abrazado, 2024).*

Moreover, a similar observation was made by an **ACG officer from the Quezon City Anti-Cybercrime Unit**, who noted that many victims prefer to report incidents informally via **social media** rather than filing official complaints:

*“We have a 24/7 Facebook page where people can send inquiries or report scams, but many do not proceed with formal cases. They just want to warn others, not go through legal proceedings.” (ACG Officer, 2024).*

---

### ***Why Are Online Scams the Most Prevalent Cybercrime?***

Online scams accounted for 58-59% of total cybercrime cases in all districts, making them the most frequently reported type of cybercrime.

Both **Col. Abrazado** and the **ACG officer** highlighted **social engineering tactics** and **seasonal trends** as reasons for the dominance of online scams:

- **Evolving Scam Methods:** Scammers adapt their tactics to popular trends, such as fake e-commerce deals, phishing messages, and social media promotions.
  - *“During Christmas, we see an increase in holiday scams. Similarly, platforms like Lazada and Shopee introduced more phishing scams when they became popular.” (Abrazado, 2024).*
- **Psychological Manipulation:** Scammers exploit **emotional triggers** like **greed** or **fear**, making victims more likely to fall for fake offers.
  - *“Scammers take advantage of victims’ desire for discounts or quick earnings, which is why these scams are so common.” (ACG Officer, 2024).*

---

### ***What Factors Make Certain Barangays High-Risk for Cybercrime?***

The data analysis of cybercrime reports revealed that **Barangays San Bartolome, Matandang Balara, and UP Campus** had the highest cybercrime cases, particularly **online scams and identity theft**.

According to the **ACG officer**, barangays are classified as **high-risk cybercrime areas** based on the **number of victim complaints** rather than the presence of cybercriminal operations:

*“Barangays are categorized as high-risk based on where the victims are located, not where the scammers operate. We track reports to see which areas have the most affected individuals.” (ACG Officer, 2024).*

The officer also noted that **high-risk barangays often have higher digital activity, making residents more susceptible to scams**. For instance:

- **UP Campus (District 4)** has a large student population, making it a target for phishing attacks and fake job scams.
- **Barangays Matandang Balara and San Bartolome** have many residents engaged in online selling and digital transactions, making them **vulnerable to fraudulent buyers and online financial scams**.

#### **Correlation with SOP:**

One of the research problems identified in the **Statement of the Problem (SOP)** is how **PNP determines high-risk areas for cybercrime**. The officer’s insights confirm that **victim density, rather than scammer location, defines high-risk barangays**.

---

*Does Age, Gender, and Occupation Influence Cybercrime Victimization?*

Based on the interview data from **PNP-ACG reports** indicate that while **anyone can be a victim of cybercrime**, certain demographics are more vulnerable due to **behavioral tendencies and psychological factors**.

#### **A. Categorization of Cybercrime Victims (Kamuning Police Station)**

Col. Abrazado identified **three common types of victims**:

1. **Unaware Victims** – Often elderly, unaware of online threats, and easily manipulated (e.g., romance scams).
  - Example: A **senior citizen was tricked into sending ₱300,000** to a scammer pretending to be a foreigner stuck at NAIA airport. The victim **believed they were helping a friend in need**, only to find out they had been scammed.
  - *“Marami sa matatanda ang nabibiktima ng romance scam o investment fraud kasi hindi nila alam na may ganito palang klaseng panloloko.”*
2. **Greedy or Overconfident Victims** – Individuals who suspect fraud but **continue engaging due to promises of high returns** (e.g., Ponzi schemes).
  - Example: Investment scams frequently **use fake testimonials and social proof** to make scams appear legitimate. Victims **keep investing, even taking out loans, in hopes of massive returns**.
  - *“Kahit obvious na scam na, may mga willing victims pa rin dahil iniisip nila na baka may chance pa silang kumita.”*



3. **Highly Skilled Victims** – Even cybersecurity experts can fall for **AI-generated scams and social engineering attacks**.

- Example: **Advanced cybercriminals, including state-sponsored hackers from China and Malaysia**, use AI-generated phishing scams and complex social engineering tactics.
- *“Kahit may OTP ka, kahit may security measures ka, kung magaling talaga ang hacker, may paraan sila.”*

**B. Demographic Factors in Cybercrime (ACG Interview)**

The **ACG officer** confirmed that certain age groups and occupations are more frequently targeted.

1. **Teenagers and students** – More likely to fall for **phishing scams and fake job offers**.
2. **Elderly individuals** – Common victims of **romance scams and financial fraud**.
3. **Investment seekers** – High risk for **Ponzi schemes and cryptocurrency fraud**.
  - *“Marami sa atin ngayon, lalo na teenagers, engaged sa online activities. Pero marami rin sa matatanda naghahanap ng investment opportunities, kaya sila ang madalas na biktima.”*

**Correlation with SOP:**

One of the research problems identified in the **Statement of the Problem (SOP)** is whether **demographic factors influence cybercrime vulnerability**. Both interviews confirm that **specific groups** are targeted based on psychological tendencies and financial behavior.

---

***Why Are Certain Cybercrime Types Less Common (e.g., Identity Theft, Credit Card Fraud)?***

While online scams dominate, crimes like **identity theft** (6-10% of total cases) and **credit card fraud** (10-15%) are less frequently reported. According to the **ACG officer**, these cybercrimes are often **underreported due to complexity and victim hesitation**:

*“Victims of identity theft often don’t realize they’ve been compromised until much later, making it harder for them to report incidents.” (ACG Officer, 2024).*

Similarly, **Col. Abrazado** noted that **victims of credit card fraud often contact their banks** rather than filing police reports:

*“Most victims of credit card scams resolve the issue with their bank instead of going through the legal process with the police.” (ACG Officer, 2024).*

The interviews confirm that **awareness, time delays, and alternative resolution channels** affect reporting rates for these crimes.

---

***Why Do Certain Districts Have More Cybercrime Cases?***

The comparative analysis revealed that **District 5 reported the highest number of total cybercrime cases (158 cases) and online scams (74 cases)**, while **District 6 reported the fewest total cases (50 cases)**. s

As mentioned by **Col. June Paolo Abrazado (Kamuning Police Station)**, population density, accessibility to digital platforms, and accessibility to reporting stations are key factors contributing to the disparity in cybercrime cases across districts:

*“Cybercrime cases are higher in more populated barangays and areas where residents are actively using online platforms like e-commerce and digital wallets.” (Abrazado, 2024).*

In contrast, areas with **fewer accessible police stations or cybercrime units** often report fewer cases, not necessarily due to lower incidents, but because **victims are less likely to report crimes**:

*“We’ve observed that areas closer to our regional or provincial offices report more cases simply because victims find it easier to lodge complaints.” (Abrazado, 2024).*

*“Barangays with active awareness campaigns tend to report more incidents, while those with little outreach often have underreported cases.” (ACG Officer, 2024).*

The **Quezon City ACG officer** also explained that **awareness levels vary across districts**, influencing reporting behavior:

---

### Evaluation of Pre-Trained and Post-Trained Chatbot Model

This chapter presents the training and evaluation results of the AI-powered chatbot developed for the **ClickSmart** website. It includes the chatbot's **training performance**, showing how well it learned from the dataset, and the **evaluation loss**, which measures its accuracy in understanding and responding to user inputs.

The chapter also explains the **evaluation scores** and what they mean for the chatbot's effectiveness. By analyzing these results, the study identifies areas where the chatbot performs well and where improvements may be needed to better assist users in understanding and reporting cybercrime.

## **Training Results**

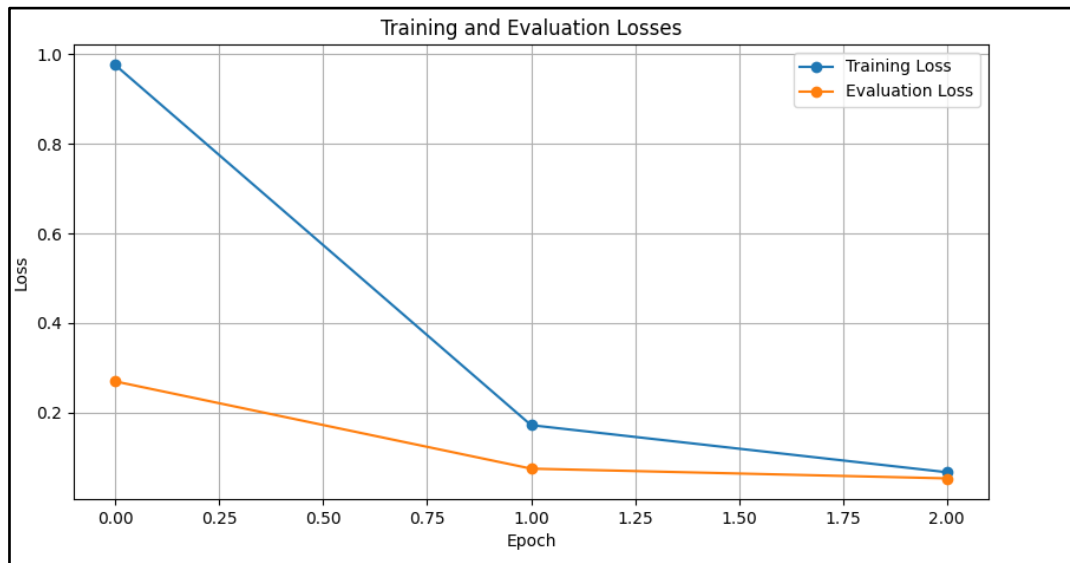
The model was trained using supervised fine-tuning (SFT) with GPT-2-medium, adjusting the pretrained weights based on the cybercrime dataset. The training process aimed to minimize the loss function, which measures how well the model learns from the dataset.

### **1. Training and Evaluation Loss**

The training and evaluation loss trends provide insights into the model's learning process. The loss curve (Figure X) shows how both training loss and evaluation loss evolved over epochs.

- **Training Loss:** Initially high but gradually decreased, indicating that the model successfully learned patterns from the dataset.
- **Evaluation Loss:** Also showed a decreasing trend, suggesting that the model generalizes well to unseen data rather than overfitting.

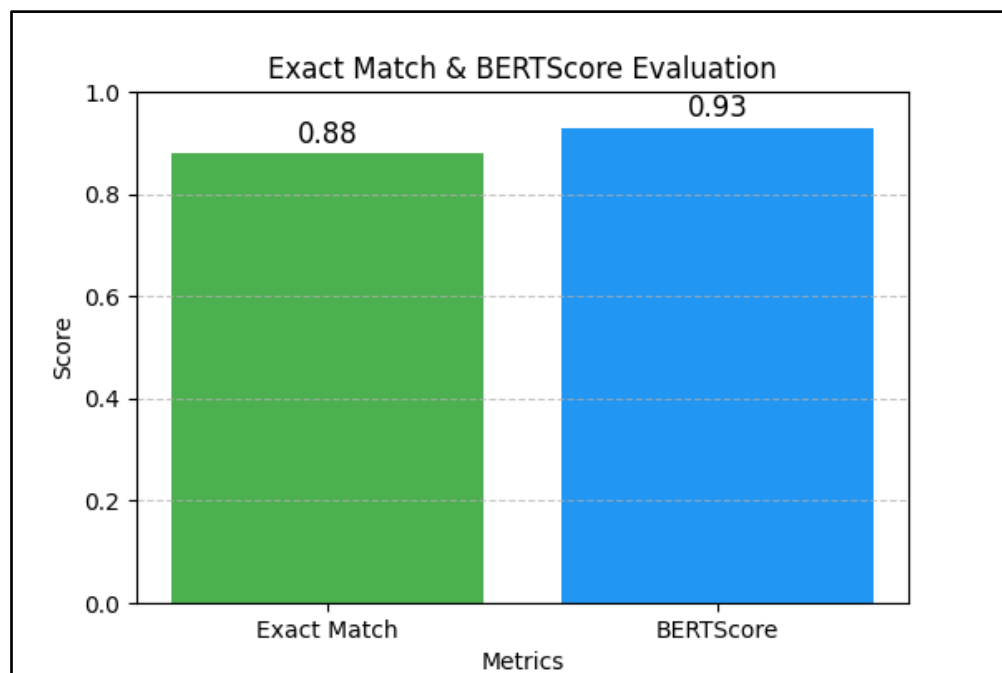
These trends confirm that the fine-tuning process improved the chatbot's ability to generate relevant responses while maintaining its effectiveness on previously unseen questions.



*Figure 3: Training and Evaluation of Losses*

## 2. Evaluation Results

After fine-tuning, the chatbot was evaluated to measure its response accuracy. The results are presented in Figure X.1, showing Exact Match (EM) and BERTScore as the key evaluation metrics.



*Figure 4: Exact Match & BERTScore Evaluation*

After fine-tuning, the chatbot was evaluated to measure its response accuracy. The results are presented in Figure X.1, showing Exact Match (EM) and BERTScore as the key evaluation metrics.

## 2.1 Interpretation of Evaluation Scores

The chatbot achieved an Exact Match (EM) score of 0.88, meaning 88% of generated responses were word-for-word matches with the reference answers. However, the BERTScore of 0.93 suggests that even when responses were not exact matches, they still conveyed high semantic similarity to the correct answers.

This difference highlights a key limitation of Exact Match (EM): it does not account for valid paraphrased responses that differ slightly in phrasing. For example, if the chatbot generates a shorter or longer version of the answer, or replaces words with synonyms, EM will assign a score of 0, even though the response is accurate.

On the other hand, BERTScore effectively captures these variations by analyzing contextual embeddings rather than exact words, making it a more robust metric for chatbot evaluation in real-world applications.

---

## Rule-Based Chatbot Integration for ClickSmart

To enhance the efficiency of the AI-model-based chatbot, a rule-based component was integrated into ClickSmart to handle non-cybercrime-related queries. This system addresses frequent and predefined inquiries, ensuring users receive quick and accurate responses without requiring complex natural language processing.

Unlike the AI chatbot, which generates responses dynamically based on trained datasets, the rule-based system follows a predefined set of rules and patterns. It specifically manages:

- **Common User Interactions** – Handles greetings, casual conversations, and engagement-based queries (e.g., “Hi,” “How are you?”).
- **FAQs About ClickSmart** – Provides general information about the platform’s purpose, features, and functionality.
- **Handling Typos and Query Variations** – Uses fuzzy matching technique to recognize common misspellings, synonyms, and reworded questions, improving response accuracy.
- **Filtering Unrelated or Off-Topic Queries** – Redirects users back to cybersecurity topics when queries fall outside the chatbot’s intended scope.

Feature	Rule-Based Chatbot	AI Chatbot (Model-Based)
Best For	FAQs, greetings, reporting guidance	Cybercrime-related queries
Handling Typos	Corrects common errors	Learns from dataset patterns
Response Time	Instant	Slight delay for processing
Flexibility	Limited to preset questions	Can generate diverse responses

Figure 5: *Comparison of Rule-Based and AI Chatbot Functionality*

By integrating rule-based logic with fuzzy matching technique, the chatbot effectively filters, redirects, and structures responses, ensuring that unrelated or ambiguous queries do not interfere with the AI chatbot’s accuracy. This hybrid approach allows the AI model to focus on generating contextual cybercrime-related responses, while the rule-based system improves user engagement, response efficiency, and overall conversational flow within ClickSmart.

## **Chapter 5: Summary of Findings, Conclusions and Recommendations**

This chapter presents the summary of findings, conclusions, and recommendations offered.

### **Summary of Findings**

From a thorough analysis of the data collected and results obtained, the following significant findings are summarized:

**1. Current level of public awareness regarding cybersecurity measures among residents of high-risk areas in Quezon City based on the data from the Quezon City Kamuning Police Station and the Quezon City Police District Headquarters Camp Tomas Caringal.**

1.1 With respect to common cyberthreats, the officer's insights confirmed that the public lack of awareness when it comes to identifying cyberthreats.

1.2 With respect to awareness of protective measures, the officer's insights confirmed that victims don't know how to protect themselves from cybercrime especially for seasonal scams.

1.3 With respect to familiarity with the reporting process and available reporting channels (e.g., Facebook pages, official hotlines), the officer's insights confirmed that the public have very low understanding on how to report a cybercrime case and where to report.

**2. Philippine National Police (PNP) categorize barangays as high-risk for cybercrime, and criteria used for this classification.**



2.1 With respect to categorize barangays as high-risk for cybercrime, the officer's insights confirmed that victim density, rather than scammer location, defines high-risk barangays.

2.2 With respect to criteria used for this classification, the officers' insights confirmed that the classification of high-risk cases was based on the location where the incident occurred, and the LGU provided information based on the statistics or volume of cases in each area.

### **3. Demographic factors (e.g., age, gender, occupation) affect vulnerability to cybercrime.**

3.1 With respect to demographic factors, both interviews from separate PNP branch confirmed that specific groups are targeted based on psychological tendencies and financial behavior.

### **4. Chatbot Development and Evaluation Results**

4.1 The ClickSmart website was successfully developed, featuring a GPT-2-based chatbot trained on a cybercrime-specific dataset.

4.2 The chatbot achieved high accuracy in responding to cybercrime-related queries, with an Exact Match (EM) score of 0.88 and a BERTScore of 0.93.

4.3 A rule-based system was integrated to handle non-cybercrime queries, such as FAQs about ClickSmart, greetings, reporting guidance, and government contact information, ensuring structured and user-friendly interactions.

## **Conclusions**

Based on the findings of the study, the following conclusions are drawn:

1. Increasing cybersecurity awareness through simple and accessible campaigns could help residents in high-risk areas recognize threats, protect themselves, and report cybercrimes more effectively.
2. Improving public awareness and reporting practices may influence how the PNP classifies high-risk areas and enhance law enforcement responses to cybercrime.
3. Personalized cybersecurity education programs could help protect vulnerable groups by addressing specific risks based on age, occupation, and financial behavior.
4. The ClickSmart chatbot effectively provides cybercrime-related information with high accuracy, as demonstrated by its Exact Match (EM) score of 0.88 and BERTScore of 0.93. Its integration with a rule-based system for FAQs and reporting guidance further enhances user experience.
5. The combination of AI and rule-based systems improves user engagement and accessibility. By addressing both cybercrime-related queries and general questions (FAQs, greetings, and reporting guidance), the chatbot ensures structured, reliable, and informative interactions.

## **Recommendations**

Based on the results and the conclusions of the study, the following recommendations are offered:

1. It is hoped that public awareness campaigns will be developed to educate residents in high-risk areas about common cyber threats, protective measures, and proper reporting processes. These campaigns are encouraged to be delivered through social media, community seminars, and informative online resources.

2. It is encouraged that platforms for cybercrime systems be improved by making them more accessible and user-friendly. Strengthening collaboration between law enforcement with local government units (LGUs), NGOs and other government organizations is hoped to streamline reporting procedures and enhance response strategies.
3. It is recommended that targeted cybersecurity education programs be implemented for vulnerable groups, such as students, seniors, and small business owners. These programs are expected to focus on specific risks they face and provide practical strategies to prevent cyber fraud.
4. It is recommended that the ClickSmart chatbot be further enhanced and expanded to improve its effectiveness as a cybercrime awareness tool. The chatbot, which demonstrated strong performance with an Exact Match (EM) score of 0.88 and a BERTScore of 0.93, could be further developed by:
  - Expanding its dataset to cover emerging cybercrime trends.
  - Enhancing its ability to process mixed-language (Taglish) inputs for better accessibility.
  - Collaborating with law enforcement and cybersecurity experts to improve response accuracy and credibility.

# APPENDICES

## APPENDIX - A

### Letters & Chart

#### A. Advisory Request Letter

August 21, 2024

Armida P. Salazar  
Computer Science Department

Dear Prof. Salazar

Good day.


We, the undersigned, are fourth-year students at National University pursuing a degree in Bachelor of Science in Computer Science with a specialization in Digital Forensics and currently enrolled in Thesis 1.

After thorough consideration and exploration of various research areas within our field, we have developed a strong interest in Cybersecurity Landscape. We followed your lessons and tips to improve our research during defense in Method of Research, which are a great help to us, and have reviewed your extensive body of work and found your expertise and contributions in this field.


We understand that you may have a busy schedule, but we would greatly appreciate the opportunity to have you as our adviser and are confident that your guidance and support will play a pivotal role in shaping our academic and professional journey.


Once again, thank you for your time and consideration. We look forward to the possibility of working with you as our adviser.

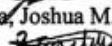
Sincerely,

Researcher 1:  Abalos, Hanst Diether B.

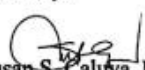
Researcher 2:  Montalban, Farrah V.

Researcher 3:  So, Vlademer Zane A.

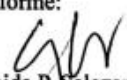
Researcher 4:  Diaz, Joshua M.

Researcher 5:  Castillo, John Russell M.

Noted by:

  
Susan S. Caluya, MSc  
Thesis Professor

Conforme:

  
Armida P. Salazar  
Professor

## B. Request Letter to Interview PNP Officials

September 27, 2024

Quezon City Police District Headquarters  
Camp Tomas Caringal  
21 Makadios, Diliman,  
Lungsod Quezon,  
1101 Kalakhang Maynila

**Subject:** Request for Interview and Data Access for Research Project

**To Whom It May Concern,**

Good day.

We, the undersigned, are fourth-year students at National University pursuing a Bachelor of Science in Computer Science with a specialization in Digital Forensics, currently enrolled in Thesis 1.

Our group is conducting a research project titled "ClickSmart: An Interactive Website Guide to Cybercrime Awareness with AI Capability." This project aims to develop an interactive and informative website to raise public awareness about cybercrime by analyzing data on the top five high-risk cybercrime activities in barangays within Quezon City.

To support our research, we respectfully request:

1. An interview with a representative from your department to gain insights into the context and trends of cybercrime in these areas. This interview will be recorded and used solely for academic purposes.
2. Data on the top five high-risk cybercrime activities in barangays within Quezon City, including:
  - o Statistical data on cybercrime incidents in these areas.
  - o Information on the types and nature of these high-risk cybercrimes.
  - o Victim demographics, including age, gender, and occupation.

We believe that the insights and data you provide will be valuable in helping us achieve the objectives of our research. If you have any questions, please feel free to contact us via email of our research leader [abaloshb@students.national-u.edu.ph](mailto:abaloshb@students.national-u.edu.ph).

Thank you for considering our request. We look forward to your positive response.

Respectfully,

Hanst Diether B. Abalos

Vlademer Zane A. So

Farrah V. Montalban

John Russell M. Castillo

Joshua M. Dia

Noted by:

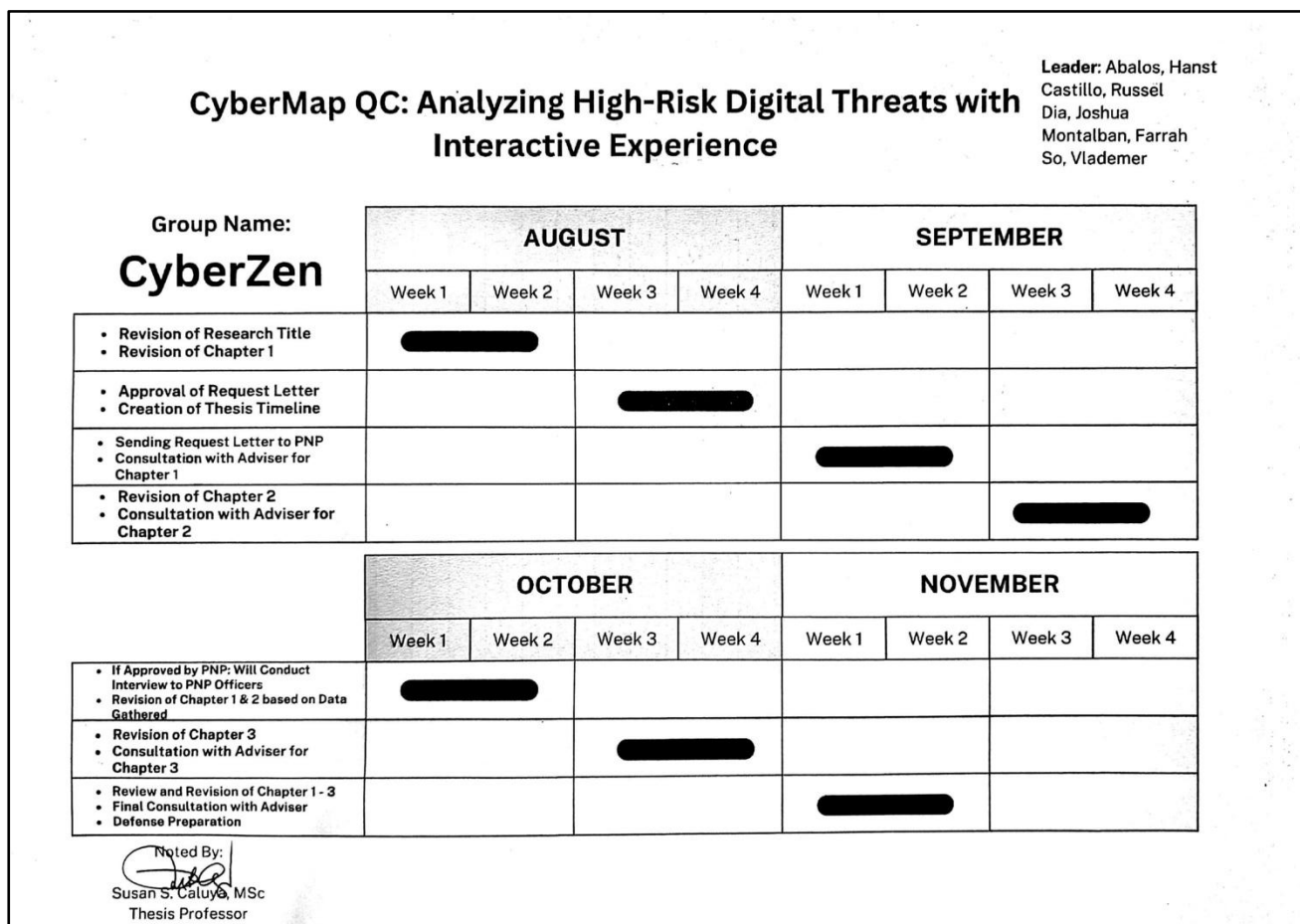
Armida P. Salazar

Thesis Adviser

Susan S. Caluya, MSc

Professor, Thesis I

## C. Gantt Chart





APPENDIX - B  
Research Instrument

INTERVIEW QUESTIONNAIRE FOR THE RESPONDENTS

CLICKSMART: AN INTERACTIVE WEBSITE GUIDE TO CYBERCRIME AWARENESS  
WITH AI CAPABILITY

Researchers

Abalos, Hanst Diether B.

Castillo, John Russell M.

Dia, Joshua M.

Montalban, Farrah V.

So, Vlademer Zane A.

**Introduction**

The following interview questionnaire was developed as part of the research for “*ClickSmart*”, a project aimed at enhancing public awareness of cybercrime through an interactive website with AI capability. The objective of this interview is to gather detailed insights from Philippine National Police (PNP) officials regarding the current trends, challenges, and strategies associated with cybercrime in Quezon City.

This semi-structured interview guide consists of twelve (12) questions. It is divided into three parts: the first part focuses on the effectiveness of seminars, the second part addresses the inquiry and reporting process, and the third part seeks statistical data and trends on cybercrime incidents in high-risk areas of Quezon City.

We fully recognize the sensitivity of the information that may be discussed and are committed to upholding the highest standards of confidentiality and data security. Your

participation will help us understand how existing efforts can be strengthened to improve public cybercrime awareness.

## **Interview Questionnaire**

### ***I. Seminar Focus***

1. Are the seminars conducted by the PNP exclusively for police personnel, or do they also include the general public?
2. What is the primary objective of these seminars, and how do they contribute to cybercrime awareness?
3. What challenges have you encountered when organizing seminars related to cybercrime?
4. How do you evaluate the effectiveness of these seminars in terms of public engagement and awareness?

### ***II. Inquiry Process***

1. What channels are available for individuals to inquire about cybercrime incidents or report cybercrime to the PNP?
2. Are there any public campaigns or advocacy efforts to inform the citizens about these platforms where they can report cybercrime?

### ***III. Statistical Data on Cybercrime Incidents***

1. Can you provide statistical data on cybercrime incidents reported in high-risk barangays in Quezon City for the past year?
2. How does the PNP categorize these barangays as high-risk, and what criteria are used?
3. What types of cybercrimes are most prevalent in these high-risk areas?

4. Are there specific trends or patterns observed in the nature of cybercrimes reported in Quezon City?
5. What demographic information is available regarding the victims of cybercrime in these barangays, specifically concerning age, gender, and occupation?
6. How does the PNP collect and analyze this demographic data, and how is it used to improve prevention efforts?

## APPENDIX – C

### Interview Transcripts

#### A. Interview at Kamuning Police Station

**Interview Date:** September 18, 2024

**Interviewee:** Colonel June Paolo Abrazado

**Interviewers:** Abalos, Hanst Diether  
Dia, Joshua  
So, Vlademer Zane

---

**[00:10] COLONEL (COL):** Sige, let's start, how do we ano..., mag rerecord ba kayo?

**[00:15] INTERVIEWERS (INT):** Opo.

**[00:41] INT:** Sir about seminar focus yung pong pinaka unang tanong. Are the seminars conducted by the PNP exclusively for police personnel or they also include the general public? How does the PNP engage with the community to educate them about preventing cybercrime?

**[00:57] COL:** Okay so this about cybercrime? Uh, concerns, uh, ang ACG, first of all, ACG, the authorized, uh, PNP unit to handle cybercrime cases. Is the anti-crime group activated on March 13, 2013. And then ngayon for how many years now? 11 years with the ACG. Ang awareness namin sa ACG ng PNP as a whole, ay targeting the PNP, the General Public, and the Government Officials. So, hindi lang talaga sa public kasi even PNP members, government officials lalo na ang mga politicians ay nabibiktima ng cybercrimes kaya no one is really immune to cybercrimes. Kaya ang awareness campaign ng PNP ay the general public, government offices, and it's personnels.

**[01:56] INT:** Next po, what is the primary objective of these seminars, and how do they contribute to cybercrime awareness?

**[02:01] COL:** Pag sa PNP, sinisingit namin ang awareness sa mga cyber related courses. For example, sa PNP, may module kami for cybercrime investigation. For example, basic cybercrime investigation for police officers, kasi kung ang ACG ang mag hahandle ng crimes, cybercrimes, wala nang matutulog sa ACG dahil maraming uri 'yang cybercrimes hindi ba...

And mostly, sa investigations sa local police stations such as Kamuning, pag naka rinig ka nang “Sir, naloko po ako sa Facebook”, ituturo agad ‘yan sa cybercrime group without delegating the details na pwede naman nilang i-handle sa police station

**[02:38] COL:** Ang batas natin sa cybercrime ay ma-mandate ng PNP-ACG ang primary unit to handle, but it does not deprive the local units to handle cybercrime cases. So pwede silang mag-file lalo na kung identified ang suspect, pwedeng may witnesses na they can handle that para hindi ma-overwhelm ang ACG.

Hopefully ‘yung ACG ang mag handle ng mga highly technical cases na kailangan natin i-investigate. So kaya kina-capacitate namin yung local investigators na mag-handle ng basic cybercrime cases. Also, sinisingitan na namin ng awareness ‘yun.

**[04:03] COL:** So meron kaming PNP module, basic cybercrime investigation and awareness. Para sa public naman, yun talaga ang need na full package ng awareness. ‘Yung sa most common cybercrimes, modules, most prevalent crimes, anong ginagamit ng mga mostly money service businesses, gcash, union bank, anong mga mostly ginagamit, and anong mga genders or ages ang mostly affected. So, that kind of statistics, and ano yung mga emerging na naman.

**[04:15] COL:** Kasi iba-iba ang modus natin, akala natin may bago ang modus, pero the bottomline is pare-pareho pa rin na niloloko nila ang victims nila, so iba-iba lang talaga ‘yung cases story. and sinasabay nila talga nila sa latest trends. For example, valentines diba? Pag valentines, nandiyan naman yung Valentines Scam. Pag Christmas, nandiyan naman yung Christmas Holiday scam. So, sumasabay sa trend. So noong lumutang yung mga Lazada, at Shopee na ‘yan, dumami nanaman yung cases ng phishing, which is sumasabay talaga sila sa trend.

**[04:37] INT:** What specific information drives does the PNP implement to raise awareness about cybercrime among individuals?

**[04:55] COL:** Ang pinaka-effective sa amin is yung lecturing, kasi nandiyan ‘yong audience, and may presentation ka, makikita nila first-hand ‘yung mga nangyari. For example, yung mga case studies kung bakit siya na biktima. Meron din kami yung distribution of flyers, ‘yung mga traditional na kahit sa mga nag-aantay ng bus, binibigyan namin ng flyers, which is makikita nila yung mga top modus, like, may mga text pala na

ipapakitang nanalo ka ng lotto, kahit hindi ka naman tumataya. So we do, traditional flyers, radio and media guestings.

[05:30] INT: More parang traditional pa rin talaga yung pag-aano. yung sa awareness

[05:33] COL: And yung mga publication is sa official social media page ng PNP at ACG.

[05:34] INT2: Yung lecturing po, saan po yung lecturing? Paano po nangyayari?

[05:42] COL: Pag sa mga school, kami ang nag-volunteer na pumunta para mag-lecture. But, also, sa lahat na nag-request, nag-se-look sa PNP ng awareness lecture, pinupuntahan namin. It works in both ways.

[05:53] INT3: Yung sa flyers po, how often po nyo ginagawa yan?

[05:57] COL: More often, kasi mayroon kaming compliance. I think the ACG can give you data. Kasi mayroon silang report every week about it.

[06:15] INT1: How does the PNP assist individuals who may not realize they have experienced cybercrime? Yung mga unaware, paano niyo pinapakita, pinapaalam na yung mga individuals na 'di sila aware na naka-experience na pala sila ng ganito. Mostly nangyayari ito sa mga scam, hindi po ba?

[06:33] COL: Yes scam, usually kasi.. may tatlong klase. Number 1, wala talagang alam which mostly mga matatanda, kasi hindi naman nila alam na may ganyan, like na pag may nakita silang panging lalaki tapos kinokompliment siya, tapos etong si nanay, na fall sa lalaking yun tapos hinihingan na siya ng kung ano-ano, like suddenly may investment, kasi nasa-satisfy siya sa companionship, yun pala scam na. So wala talagang silang alam.

To the point na minsan may sumugod na matanda diyan sa NAIA, kasi may nag pakilala sa kanya na foreigner na nangloloko, ang sabi "Nandito na ako sa Pilipinas, na-trap ako sa airport, 'yung mga padala ko sa iyong diamond,

kinonfiscate, na dapat daw aregluhin ko ng P300,000” Tapos ayon, ngayon, nagpadala si Senior Citizen ng P300,000 para ma-aregulo, tapos na-trap nanaman daw yung package sa isa namang unit, so, padala naman siya hanggang sa...

**[07:42]COL:** Sumugod yung matanda sa NAIA, at nag sisigaw nang “Mga walang hiya kayo Custom! Mga walang hiya kayo! I-release niyo yung ano ko... bakit mo hindi niyo pinapalaya?”. So, naging kahiya-hiya siya. Nakak-awa kasi wala talaga silang alam totally.

**[8:10]COL:** Number 2, alam nilang pwedeng scam pero nanaig yung pagiging greedy. So, invest, invest, pinakitaan ng isang positive results sa investment. So, si victim, sige invest, invest, then nangutang na, nangutang. Ang dami ng na-scam, kasi may nag-tetestify na ano eh. May nag-tetestify na marami silang nakuha from the investment. May mga picture-picture pa, pero itong si victim, sige lang sa pag-papaloko.

**[8:20]INT1:** Akala po totoo.

**[8:21]COL:** Despite it is overwhelming na ang daming scam sa paligid, nag eexist tong si willing or or greedy victims. Pangatlo is yung talagang mga high level na despite kahit ako, I cannot guarantee na hindi ako mag-bibiktima ng any forms of cybercrimes. Kasi may mga bihasa at magaling talaga na cybercriminals. Even so, na may OTP password ka or whatsoever. Eh magaling talaga eh. So may mga high-level talaga, even state-sponsored na hackers, Malaysia, and China. So, overall, may mga certain levels ang basic scamming. May mga high level, at national level cyber security concern.

**[9:19]INT1:** Next question po. May mga partnerships mo ba kayo with private sectors, NGOs, or educational institutions na nagpo-focus sa cybercrime prevention?

**[9:31]COL:** Sa amin [Kamuning Police Station] meron kaming ACG (Anti-Cybercrime Group). Dapat talaga ACG yung na interview inyo. Kasi sa ACG talaga ang may focus sa mga ganyang klase ng awareness. Meron ang ACG na specific group na tinaawag naming advisory group, from different cyber security and business industries involving cybercrimes and cyber security. Merong mga groups na mga cyber security

professionals na nag-advise sa amin kung ano ang magandang gawin to address cybercrimes. So yan lang yung masashare kong mga partners namin. Advisory groups.

[10:31]INT1: Pag statistical data naman po, sinong magandang kausapin?

[10:36]COL: For cybercrime sa amin [Kamuning Police Station], wala kaming data ng cybercrime dito. Meron yan is sa QCPD Camp Caringal - ACG, hindi pwedeng mawalan yan doon. Kaya lang pag dating sa data, medyo kailangan niyong mag ingat, or you can search their Facebook pages na mag-represent ng ACG kasi baka nag-ppresent sila dyan ng data trends.

[10:56]INT1: So, 'yong next question po about statistical, hindi niyo po masasagot?

[11:02]COL: I have no authority, not in my jurisdiction

[11:11]INT1: Sir ayun lang naman mostly yung question namin. Nakausap din po namin si miss secretary. Sabi niya po sa amin na baka sa Camp Caringal din po kami makahingi ng statistical data.

[11:43]COL: Sa QC area lang?

[11:47]INT: QC area lang po

[11:50] COL: So, okay, yung data kasi namin dito in cybercrime is just the basic information of Quezon City. I recommend na you guys shall visit to Camp Caringal para sa data na sineseek niyo, I think, ma pprovide nila 'yun.

[13:07]INT1: Sir, lastly, yung reporting talaga ng mga cybercrime incidents, paano po nangyayari? Pupunta talaga sa station? Magco-complain?



[13:18]COL: Yan ang isang problem talaga, kasi cybercrime is one of the most under-reported I believe. Kasi sa ilang victims na nawawalan ng 500 or 2000 pesos, hindi o tinatamad na sila mag report.

[13:53] COL: Like, itong si nanay nong na-scam sa ganong halaga, tapos tinanong siya ng anak niya na kung pupunta pa ba siya ACG para mag-report? Kung ang pamasahé mo palang eh luge kana. So ilan ang hindi nag-rreport ng ganon? Minsan nga yung pinaka lowest losses ng cybercrime na na-handle ko is 2,000 pesos. So it doesn't matter. Minsan meron lang ako na-encounter na gamer na nawalan ng 200,000 pesos. Isa siya sa sikat na vlogger at gamer, then nawalan siya ng 200,000 pesos. Nagpa-police record lang siya pero hindi siya proceed to file sa court ng case. Siguro kasi mababa pa sa kanya ang 200,000 na yan at mapapagod lang siya sa due process.

[14:39]INT1: So sir, sa tingin nyo, what's on your take kung may mga parang website na madali. Di ba? Mostly tatawag ka pa? What's your take kapag mayroong sariling system yung PNP na dito na nga lang ako para hindi na ako ma-hassle. Tapos may magiging katulungan talaga ito dito kahit sa QC area kapag mayroong system na ganon.

[15:01]COL: Na-address na namin yan, na ako pa nag-author niyan yung ano "CyberCrimeWatch". Meron kami sa CyberWeb, may central database ng internal yung PNP ACG para kapag may nag-complainant, na ito yung number na nang-text sa atin, in-encode na pala yung number, then mag-aalert na yung number na yan na ito ay nakakapangloko. Meron 'yung CyberCrimeWatch na pwede kang mag-search kung itong cellphone number na ito ay flagged as a scammer, lalabas doon na this number is already reported. So alam mo na-scammer yun kasi may nag-report ng iba. Up and running na yun, maraming na accomplishment na doon. Pero unfortunately tinakedown 'yun ng PNP, and I don't know the reason why.

[16:00]INT: Anong year yan sir, na-establish?

[16:04]COL: Na-establish ko yun, nasa ACG pa ako noon, 2021. CyberCrimeWatch, CyberWeb. Nandyan pa yung third instruction, na-establish sa study niyo. Impact niya sana yung study ko sa masteral ko, kaya lang nagpang-e-study ko, then tinake down, hanggang ngayon sa ACG, ini-invite ako as subject matter expert. Nag-present ako sa kanila.

Lahat ng katanungan nila na at problema, yun na ang sagot. Oh, yan, sama niyo sa study niyo, yung CyberWeb and CyberCrimeWatch.

[18:22]INT: Ayun po yung pinaka-coverage po. Parang barangay po.

[18:28] COL: Ito yung mga sinabi ko pang background. Ang assessment ko dyan sa barangay mostly most populated saka pinakabalapit sa office Kasi maraming natamad na eh. Dumami yung cybercrimes. Ang problem siya dyan is yung convenience sa pag-report Saka yung ano, yung may malapit na... Dati ang ACC, Central Headquarters lang. And then nagkaroon kami ng regional offices nationwide. Hanggang sa nagkaroon kami ng provincial offices. O di dumami na ang report namin kasi maraming nang nakabalik. So isa sa factor yun kung bakit namasin yung cybercrimes. Kasi maraming nang accessible na cybercrime offices na pwede mag-handle.

[19:29]INT: Ah okay po sir, again po, ano pong name sasabihin namin pag punta po sa Camp Caringal?

[19:32] COL: Si Erick, hanapin niyo si Erick Casabal.

[19:40]INT: Sir, yung contact number po ba is okay lang din po makuha?

[19:42] COL: Ah, sige. I-ano ko sa inyo, ibigay ko, at iforward ko sa kanila.

[19:44]INT: Sige po. Thank you so much po and for your time.

## B. Interview at Quezon City Police District Headquarters Camp Caringal.

**[00:00]INT:** For the inquiry process, number one, what channels are available for individuals to inquire about cybercrime incidents or report cybercrime to the PNP?

**[0:14]COL:** The PNP ACG itself together with its respective RACOs, Regional Anti-Cybercrime and Anti-Cybercrime Unit to include National Capital Region Cybercrime Unit. As a whole we have our facebook page, respected facebook page to contact us in terms of inquiry or lodging their complaints or concerns. So we have our own Facebook account. This facebook account are approved by the higher headquarters doon sa main office namin.

**[01:16 0]INT:** and its open 24 hours?

**[1:18]COL:** yes, The Facebook page can cater their concerns for 24 hours or any time the complaint is sent to that page. We have respected facebook page or they can contact us to our cellphone numbers of office phone numbers so sa ACG, yun ang approach through Facebook page. in case the complainant or the victim address the issue, the NHQ will inform you of the concerned unit where to address and where to report. the NHQ or the ACG headquarters will endorse you to the concerned district team or to the concerned PCRT or RACO.

**[02:33]INT:** May advocacy po ba or campaign na yung purpose po is to the community know kung paano mag report po ng mga cybercrime incident?

**[02:47]COL:** yes we have existing policies regarding that so to include our PCR activities the police community division we have our own PCR or now PCADG the Police Community Affairs Division Group where in each offices include the PNP ACG also its PCR PCADG so the PCADG has their kung baga yung condote to inform the community so we have also our way so we conduct lectures, seminars, and, infographic materials we to inform the public of their rights their guide as a guide for them not to be a victim of any cybercrime. We conduct lectures on respective barangays not only respective barangays but also schools schools can ask us any SME or subject matter expert

**[04:46] INT:** additional question po, how often nag ka-campaign?

**[04:51]COL:** we cater di kami mismo yung nag a-ano.. depending on the request of the concern office, institution but we also have our kung baga kami yung nag i-initiate we also initiate effort. Kami ang nakikipag-communicate sa barangay. Very often naman yan. Usually, sa isang quarter we conduct at least four or less than ten depending on our situation considering that we only have limited resources. So, through infographics materials naman So daily nagpo-post kami in our Facebook page for them to be aware, for the community to be aware. So we also conduct outreach program where in they are informed of the update cybercrime or any cybercrime related incidents so for them to be aware

**[06:11]INT:** Question lang po. Sino po or paano po kayong makacontact if ever, halimbawa sa org namin sa NU tapos gusto namin magkaroon ng seminar or talk about cybercrime?

**[06:26]COL:** you can prepare a letter, submit a letter to us, address it to the team leader or to the nearest concerned team where NU is located.

**[06:41]INT:** sampaloc

**[06:43]**You can also ask manila anti-cybercrime team for them to be art of that program or part of that advocacy for them to be included as subject matter expert. Just request to them, submit a letter of what would be the purpose of that letter, communicating, requesting to them as subject matter expert

**[07:14]INT:** then sa may ano naman po paano po kina-categorized nung PNP yung barangay na to is high risked cybercrime activity compared po sa ibang barangay?

**[07:30]COL:** In particular hindi naman siya activity. We usually categorize them as victim or based on the reports kung saan nangyari, kung saan nila nalaman, kung saan nila napag-alaman, kung saan nila nalaman, kung saan napag-alaman na iyon nga ay scam or any possible cybercrime-related incident. So based sa complaints ng victim kung saan sila located, doon namin malalaman na iyon ay high-risk area or possibly high-risk area for them to be victimized.

**[08:30]INT:** And ito naman, what specific proactive measure naman ang ginagawa ng PNP to implement for example para ma-prevent na lumalala na iyong high-risk ng cybercrime dito sa barangay?

**[08:47]COL:** Sa QC we have existing ugnayan sa mga barangay so per ugnayan sa district together with the or in collaboration with the LGU, the district command or district staffs together with us. Doon kami bumababa for them to be informed of the crime statistics or crime volume doon sa district na iyon. So they are aware, and We also inform them of the precautions or proactive measures para the community within that district will be informed. Kung ma-enlighten sila of the existing trends, kung ano mga trends ba yan.

Kasi nag-iiba-iba ang trends. They are unaware na trend na iyon pala, iyon na ang ngayon nangyayari. So ganun ang ginagawa dito. Nakikipag-ugnayan kami sa QC police District Command or the staffs invite us to inform the community

**[10:38]INT:** next po is factor po ba yung age, gender, and, occupation nung victim kung bakit sila na-scam or naging victim ng cybercrime

**[10:43]COL:** so demographic yan diba? Sa demographic naman. Big factor. May factor din yan. Actually, based kasi sa natin wala sa edad, wala kung sino ka walang pinipili ang cybercrime. As long as clinic mo yan diba clinic mo yan nag bigay ka information you can be victimized kung di ka aware although in some manner there is consideration sa age mo Sa community ngayon marami sa atin ang nag-i-engage usually teenagers, usually mayroon din mga matatanda na naghahanap ng kalinga online, naghahanap ng other investment kapag kukuhaanan ng ano. Doon kasi siya, depende sa situation.

**[12:25]INT:** then yung last po is paano po kinocollect ng PNP and inanalyze ang data?

**[12:32]COL:** we have crime incident reporting and analysis system, meron kaming CIRAS, based on the blatter ini-encode namin yun ganon din sa local police diba pag na blatter ka may report na binibigay sa inyo ini-incode name nyun through online we have existing system to us to determine and analyze yung crime volume crime statistics kung anon yung mataas yung crime incident So yung system na yun, yun ang nag-i-gather sa akin.

[13:25]INT: about po sa website namin yung sa thesis po namin Yung gagawin po namin is informative to gain awareness sa public. And then about si significance po namin to the local government office which is yung PNP po Ano pong opinion or idea niyo about sa website namin?

[13:50]COL: you can post, lalagay mo doon yung mga informative materials. And then basta huwag mo lang kakalimutan ilagay sa kung saan mo kinakinuha yung credit back, yung source.

[14:16]INT: yung ability po to report sa website namin mag redirect po

[14:20]COL: I-link nyo yung page

[14:26]INT: pag may nagreport pong user dun directa po sa mapupunta sa email sa inyo sir

[14:33]COL: email no siguro hyperlink mo lang yung page, kasi kung magcreate ka other page sa system nyo it is very risky for you and to the PNP. Di nyo sa pwedeng kuhain na feature kasi makikipag collaborate ka dyan may agreement.



APPENDIX – D  
Photos of Data Gathering

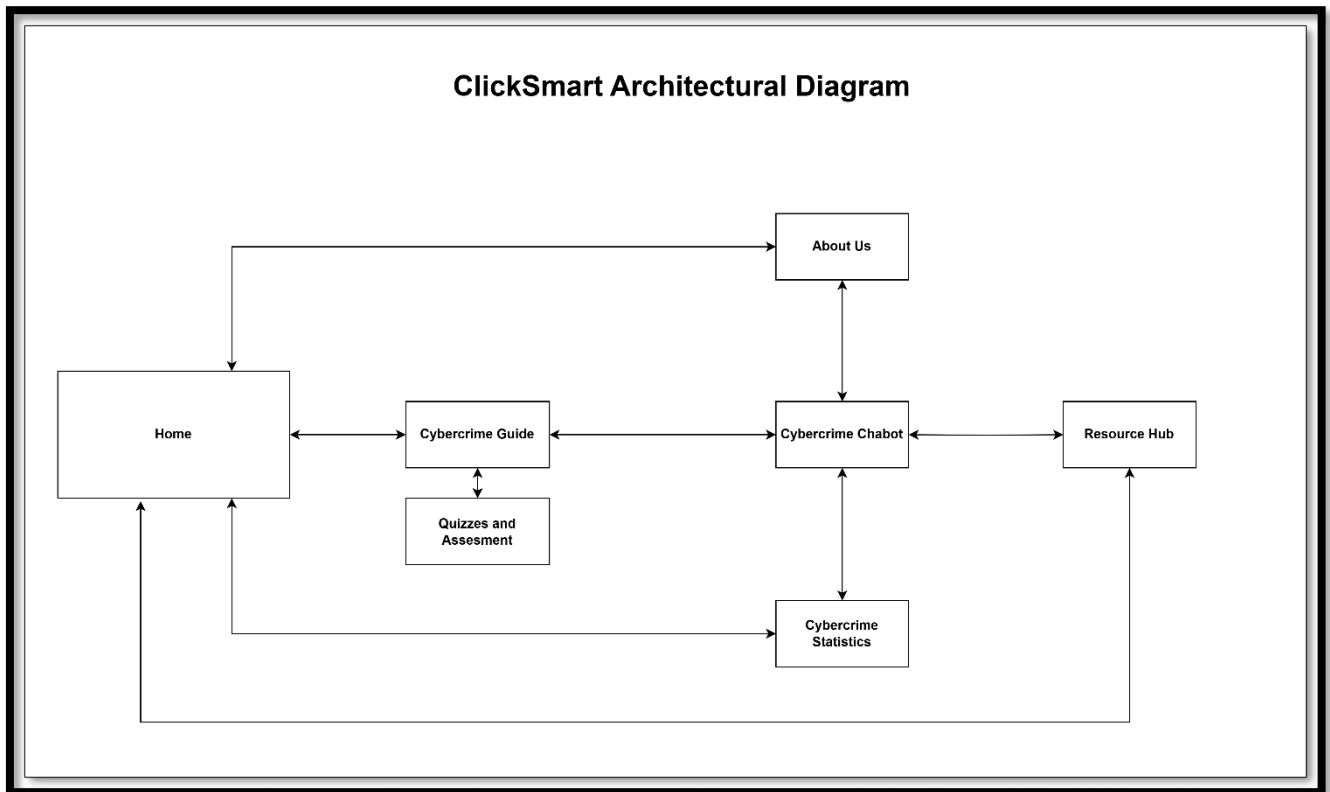
A. Photos at Quezon City Kamuning Police Station



B. Photos at Quezon City Police District Headquarters Camp Caringal.



APPENDIX – E  
Photos of Data Gathering





## REFERENCES

- Gonzales, C. (2019, October 16). \*Cybercrime on the rise over the last 6 years\*. INQUIRER.net. <https://newsinfo.inquirer.net/1177832/cybercrime-on-the-rise-over-the-last-6-years>
- Esmeralda, R. (2022, April 7). \*The cybersecurity threat landscape in the Philippines 2022 (Infographic)\*. \*MEC Networks Corporation\*. <https://mec.ph/infographics/cybersecurity-threat-landscape-2022/>
- Presidential Communications Office. (2024, February 15). PBBM orders PNP to intensify anti-cybercrime efforts and strengthen communication capabilities. [https://pco.gov.ph/news\\_releases/pbbm-orders-pnp-to-intensify-anti-cybercrime-efforts-astrngthen-communication-capabilities/](https://pco.gov.ph/news_releases/pbbm-orders-pnp-to-intensify-anti-cybercrime-efforts-astrngthen-communication-capabilities/)
- Lalu, G. P. (2023, July 11). Cybercrimes in Metro Manila up 152% in 1st half of 2023 — CICC. INQUIRER.net. <https://newsinfo.inquirer.net/1798786/cybercrimes-in-ncr-rose-by-152-in-1st-half-of-2023-vs-same-period-in-2022-cicc>
- Cabalza, D. (2023, July 14). Cybercrimes still up despite SIM registration law – police data. INQUIRER.net. <https://newsinfo.inquirer.net/1800395/cybercrimes-still-up-despite-sim-registration-law-police-data>
- Cabalza, D. (2023, July 19). Crime rate dips by 10% in first half of 2023 – PNP. INQUIRER.net. <https://newsinfo.inquirer.net/1803658/crime-rate-dips-by-10-in-first-half-of-2023-pnp>
- Laqui, I. (2024, February 6). Swindling tops list of cybercrimes in Philippines — PNP chief. Philstar.com. <https://www.philstar.com/headlines/2024/02/06/2331392/swindling-tops-list-cybercrimes-philippines-pnp-chief>
- Tupas, E. (2024, April 9). Cybercrime cases continue to rise, up 21.84 percent in Q1. Philstar.com. <https://www.philstar.com/headlines/2024/04/10/2346516/cybercrime-cases-continue-rise-2184-percent-q1>
- Cybercrime cases fall by 40.79% in the final week of March 2024 | ACG. (2024, April 24). ACG. <https://acg.pnp.gov.ph/cybercrime-cases-fall-by-40-79-in-the-final-week-of-march-2024-2/>
- Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. <https://www.semanticscholar.org/paper/Cyberattacks-and-threats-during-COVID-19%3A-A-review-Chigada-Madzinga/a20f6aef4325aa00854fe6eeac66ff20789d41f2>

The growing cyberthreat to utilities - and how they should respond. (2022, May 20). World Economic Forum. <https://www.weforum.org/agenda/2020/01/are-utilities-doing-enough-to-protect-themselves-from-cyberattack/>

Ye, Z., Guo, Y., Ju, A., Wei, F., Zhang, R., & Ma, J. (2020). A risk analysis framework for a social engineering attack based on user profiling. *Journal of Organizational and End User Computing*, 32(3), 37–49. <https://doi.org/10.4018/joeuc.2020070104>

Mat, N. I. C., Jamil, N., Yusoff, Y., & Kiah, M. L. M. (2024). A systematic literature review on advanced persistent threat behaviors and its detection strategy. <https://www.semanticscholar.org/paper/A-systematic-literature-review-on-advanced-threat-mat-Jamil/a96405c934160861223afbc212056fddadfla67b>

Ahmed, Y., Asyhari, A., & Rahman, M. A. (2021). A cyber kill chain approach for detecting advanced persistent threats. *Computers, Materials & Continua*, 67(2), 2497–2513. <https://doi.org/10.32604/cmc.2021.014223>

Grigaliūnas, Š., Brūzgienė, R., & Venčkauskas, A. (2023). The method for identifying the scope of cyberattack stages in relation to their impact on cyber-sustainability control over a system. *Electronics*, 12(3), 591. <https://doi.org/10.3390/electronics12030591>

The ultimate guide to open-source data [2023 update]. (2023). Lido. <https://www.lido.app/post/open-source-data>

The pros and cons of open data. (2021, September 30). The official MERL open source community. <https://merlcenter.org/guides/pros-and-cons-of-open-data/>

Cybercops apprehended online seller of registered SIM cards. (2024, June 5). ACG. <https://acg.pnp.gov.ph/cybercops-apprehended-online-seller-of-registered-sim-cards/>

Broken trust, two friends torn apart by investment scam. (2024, May 27). ACG. <https://acg.pnp.gov.ph/broken-trust-two-friends-torn-apart-by-investment-scam/>

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, 5(2), 23. <https://doi.org/10.3390/bdcc5020023>

Rama, P., & Keevy, M. (2023). Public cybersecurity awareness good practices on government-led websites. *International Journal of Research in Business and Social Science*, 12(7), 94–104. <https://doi.org/10.20525/ijrbs.v12i7.2840>

National Defense College of the Philippines. (2023, March 28). Philippine cybersecurity in retrospect (2016-2021). NDCP. <https://www.ndcp.edu.ph/philippine-cybersecurity-in-retrospect-2016-2021/>

CT Link Systems, Inc. (2022, January 11). Cybersecurity awareness in the Philippines. CT Link. <https://www.ctlink.com.ph/cybersecurity-awareness-philippines/>

ABS-CBN News. (2023, September 19). PH needs 180,000 cybersecurity professionals—group. <https://news.abs-cbn.com/business/09/19/23/ph-needs-180000-cybersecurity-professionals-group>

International Journal of Computing Sciences Research. (2018). Internet security awareness of Filipinos: A survey paper. *International Journal of Computing Sciences Research*, 1(4), 14-26. <https://www.stepacademic.net/ijcsr/article/view/56>

WCCPU arrests male suspect for exploiting a minor. (2024, June 10). ACG. <https://acg.pnp.gov.ph/wccpu-arrests-male-suspect-for-exploiting-a-minor/>

Hernandez, S. S., Lacsina, A. C., Ylade, M. C., Aldaba, J., Lam, H., Estacio, L. R., Jr, & Lopez, A. (2018). Sexual exploitation and abuse of children online in the Philippines: A review of online news and articles. <https://www.semanticscholar.org/paper/Sexual-Exploitation-and-Abuse-of-Children-Online-in-Hernandez-Lacsina/8486de57c7b68fbe9190e71778b282688d95ed75>

Skorupka, C. S. J. M. L. B. D., & W. J. S. C. (2021, May 4). Guide to cyber threat information sharing. NIST. <https://www.nist.gov/publications/guide-cyber-threat-information-sharing>

News and announcements. (2024). AMLC. <http://www.amlc.gov.ph/index.php>

Arasa, D. (2024, January 23). Philippine cybersecurity: How the country beats digital threats. INQUIRER.net. <https://technology.inquirer.net/131336/philippine-cybersecurity-how-the-country-beats-digital-threats>

Dacanay, D. J., Quinto, M., Parayno, J., & Fajutagana, J. (2024). A comparative study of the Philippines in a global cybersecurity context and its implications on local cybersecurity practices. <https://doi.org/10.13140/RG.2.2.30104.00008>

Mustapha, A., Alhassan, R., & Ashi, T. (2024). Current trends and innovations in cybersecurity technologies: A comprehensive review. <https://doi.org/10.13140/RG.2.2.10471.05288>

Sunnexdesk. (2023, September 14). PNP probes 16,297 cybercrime cases in 2023; 397 arrested, 4,092 rescued. \*SunStar Publishing Inc.\* <https://www.sunstar.com.ph/davao/local-news/pnp-probes-16297-cybercrime-cases-in-2023-397-arrested-4092-rescued>

Cisco. (2024, August 27). Hackers think in all directions. End-to-end security is the answer. \*Cisco\*. <https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybercrime.html>

How can protection motivation theory be used to explain cyber security behaviors? | 5 Answers from Research papers. (2024). SciSpace - Question. <https://typeset.io/questions/how-can-protection-motivation-theory-be-used-to-explain-fnyqrf0b3f>

- Identity Theft Resource Center. (2022, January 24). 2021 data breach report. [https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124\\_ITRC-2021-Data-Breach-Report.pdf](https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf)
- Caliwan, C. (2024). PNP faces challenges in cybercrime investigations due to lack of training and equipment. \*Philippine News Agency\*. <https://www.pna.gov.ph/articles/1218444>
- Caliwan, C. (2024). PNP notes a rise in cybercrime cases and arrests. \*Philippine News Agency\*. <https://www.pna.gov.ph/articles/1222307>
- Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. *Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency* (pp. 149-159). <https://doi.org/10.1145/3287560.3287600>
- Bada, A., Gunapala, S. R., & Dehghantarnha, A. (2019). Cyber security awareness: A comparative study. *IEEE Access*, 7, 161051-161065. <https://doi.org/10.1109/ACCESS.2019.2952970>
- Evans, S. (2024, July 12). Microsoft launches AI chatbot for cybersecurity. <https://www.iotworldtoday.com/security/microsoft-launches-ai-chatbot-for-cybersecurity>
- Malwarebytes. (2024, July 16). What is ChatGPT? ChatGPT Security Risks | AI Chatbots. <https://www.malwarebytes.com/cybersecurity/basics/chatgpt-ai-security>
- Figure 1. Schematic presentation of the Protection Motivation Theory. . . (2023). ResearchGate. [https://www.researchgate.net/figure/Schematic-presentation-of-the-Protection-Motivation-Theory-PMT-and-its-seven\\_fig1\\_267102412](https://www.researchgate.net/figure/Schematic-presentation-of-the-Protection-Motivation-Theory-PMT-and-its-seven_fig1_267102412)
- [https://assets.publishing.service.gov.uk/media/605a1679d3bf7f2f112f0f1b/Cyber\\_Security\\_Breaches\\_Survey\\_2021\\_Statistical\\_Release.pdf](https://assets.publishing.service.gov.uk/media/605a1679d3bf7f2f112f0f1b/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf)
- Hamad, S., & Yeferny, T. (2020). A Chatbot for Information Security. Retrieved from ResearchGate
- He, J., & Xin, C. (2021). Developing an AI-Powered Chatbot to Support the Administration of Middle and High School Cybersecurity Camps. *Journal of Cybersecurity Education, Research and Practice*. Retrieved from Cybersecurity Journal
- NJCCIC (New Jersey Cybersecurity & Communications Integration Cell). (2023). ChatGPT and Its Impact on Cybersecurity. Retrieved from NJCCIC
- Balbix. (2023). What To Know About Generative AI Chatbots and Cybersecurity Risks. Retrieved from Balbix