

# CLICKSMART

EMPOWERING FILIPINOS AGAINST  
CYBER THREATS





# About Us

- **Free Online Platform**
- **AI-Powered Chatbot:**
  - Answers FAQs about cyber threats
  - Guides users in reporting incidents to PNP Anti-Cybercrime Group
- **Empowers Users:**
  - Recognize threats like phishing and scams
  - Take proactive measures to safeguard personal and digital lives

# Preventative Measures

- Use Strong Passwords

Create complex passwords that include letters, numbers, and special characters. Avoid using easily guessed information like birthdays.

- Avoid Oversharing on Social Media

Be mindful of the personal information you share online, as it can be used against you in phishing attacks or identity theft.

- Think Before You Click

Always verify the source of links and attachments before interacting with them.



# Recognizing Phishing Emails or Messages

- Unfamiliar Tone or Greeting

Phishing messages often use generic greetings like "Dear Customer" instead of your name. If the tone feels off, it could be a red flag

- Grammar and Spelling Errors

Legitimate organizations typically proofread their communications. Errors can indicate a phishing attempt

- Inconsistencies in Email Addresses

Check the sender's email domain. If it doesn't match the organization's official domain (e.g., @company.com), it's likely a scam



# Recognizing Phishing Emails or Messages

- **Urgent Requests for Action**

Phishing emails often create a sense of urgency, prompting you to act quickly without thinking. Be wary of messages demanding immediate action

- **Suspicious Links or Attachments**

Hover over links to see the actual URL before clicking. If it looks suspicious or doesn't match the claimed source, do not click!



# Signs of a Hacked Device or Account

- **Unfamiliar Transactions**

Unexpected charges on your bank or credit card statements can indicate unauthorized access.

- **Account Lockouts**

Difficulty logging into your accounts, especially if you haven't changed your password, may suggest hacking.

- **Unsolicited Password Reset Requests**

Receiving notifications about password changes that you did not initiate is a strong indicator of a potential breach.



# Indicators That Your Personal Data May Be Compromised

- Increased Spam or Phishing Attempts

A sudden surge in spam emails could signal that your information has been leaked.

- Unrecognized Login Attempts

Alerts from services about logins from unfamiliar locations or devices can indicate that someone else is trying to access your account.



# Steps to Secure Your Accounts After a Breach

- Change Your Passwords

Update passwords for affected accounts and consider using a password manager.

- Enable 2FA:

If not already activated, enable two-factor authentication on all accounts that offer it.

- Monitor Financial Statements

Keep an eye on bank and credit card statements for any unauthorized transactions.



# What to Do After Experiencing a Cybercrime

- Seek Emotional Support

Experiencing cybercrime can be distressing. Reach out to friends, family, or professional counselors for support.

- Report the Incident

Contact local law enforcement and report the crime to relevant organizations (like the PNPACG) for further assistance and guidance on recovery resources.

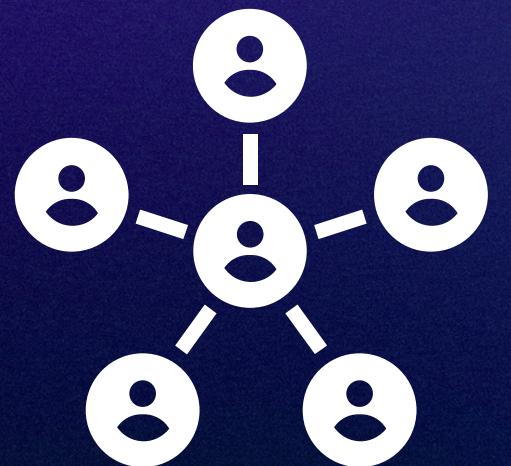


# Types of Cybercriminals



## HACKERS

Individuals who gain unauthorized access to systems for different reasons.



## CYBERCRIMINAL ORGANIZATIONS

Cybercrime groups that work together for large-scale digital crime.



## SCAMMERS & FRAUDSTERS

Cybercriminals who deceive people or businesses to steal money or financial data.



## CYBER EXTORTIONISTS

Cybercriminals who demand money by threatening victims.

# Types of Cybercriminals



## CYBER TERRORISTS

Cybercriminals who attack for ideological, political, or military reasons.



## THE INSIDER THREATS

Cybercriminals who steal trade secrets, manipulate data, or sabotage businesses.



## CYBERBULLIES & HARASSERS

Criminals who harass, intimidate, or exploit others online.



## DARK WEB CRIMINALS

Cybercriminals operating in the dark web, a hidden part of the internet.

# Types of Cybercriminals



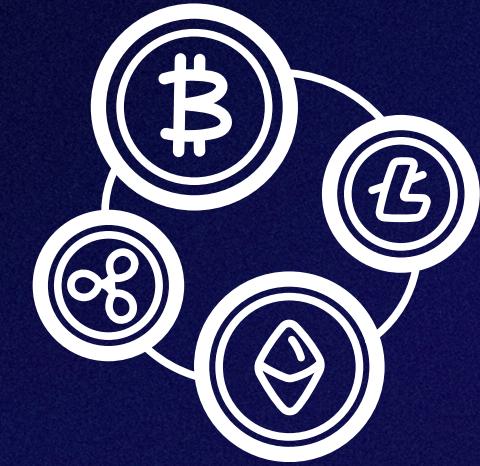
## AI CYBERCRIMINALS

Cybercriminals using artificial intelligence (AI) for digital crime.



## IOT HACKERS

Cybercriminals who target Internet of Things (IoT) devices.



## NFT & CRYPTO SCAMMERS

Cybercriminals who exploit NFTs, blockchain, and cryptocurrency platforms.

# CLICKSMART

WEBSITE MANUAL

Home About Contacts ::



# Homepage

**CLICKSMART**

Cybercrime Guide   Cybercrime Statistics   About Us   Resources Hub

**Experiencing a cybercrime from a careless click can cost you, but a smart click can save you. ClickSmart!**

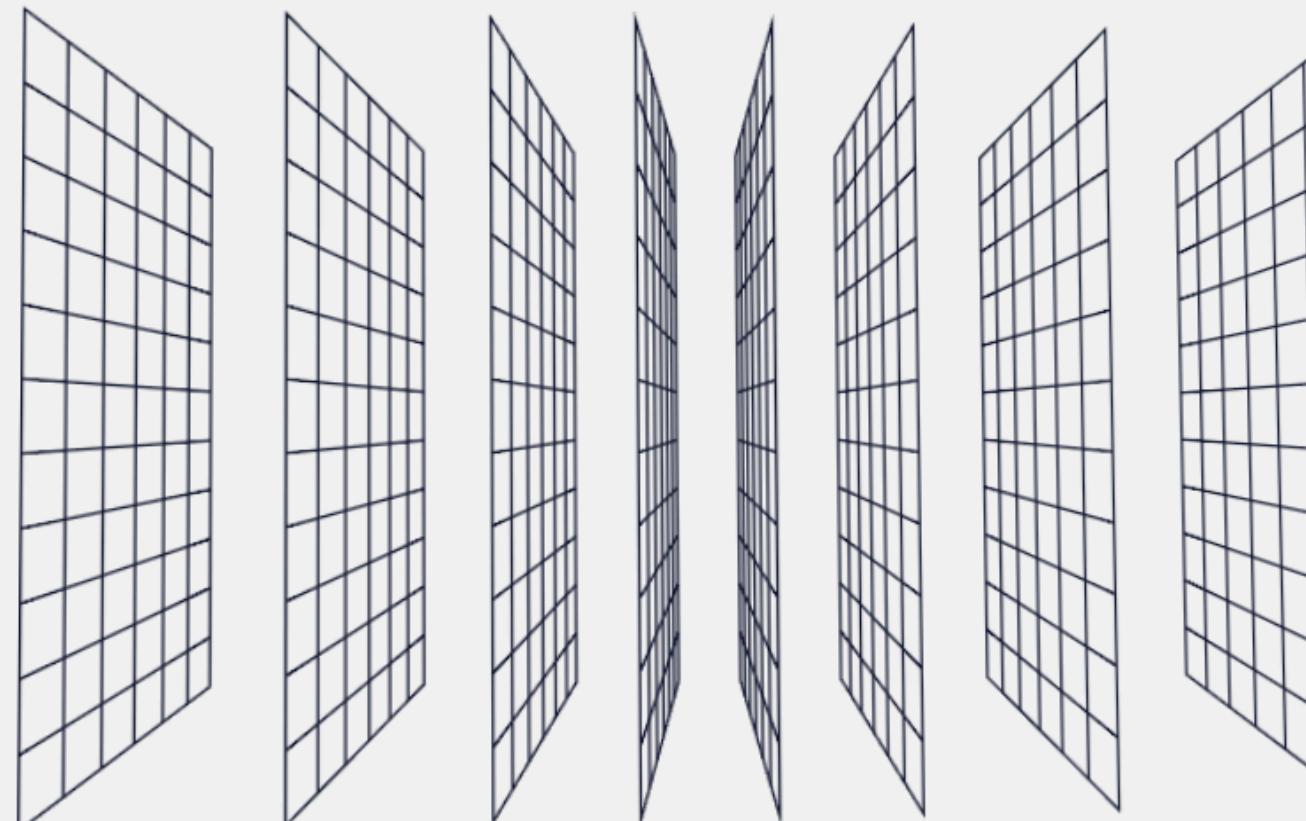
ClickSmart is here to empower you by providing tools, knowledge, and guidance to help you protect yourself and stay one step ahead of cybercriminals. Awareness and vigilance are our best defenses against this growing threat.



# Homepage

**CLICKSMART**

Cybercrime Guide Cybercrime Statistics About Us Resources Hub



## What is ClickSmart?

ClickSmart is your **free online ally** against cybercrime, designed specifically for Filipinos. Our platform features an **AI-powered chatbot** that answers your questions about cyber threats and guides you on reporting incidents to the Philippine National Police (PNP) Anti-Cybercrime Group.

Cybercrime can affect anyone, but with ClickSmart's resources, you can stay informed and protected. Join us today and take charge of your digital safety!



# Homepage (News and Articles)

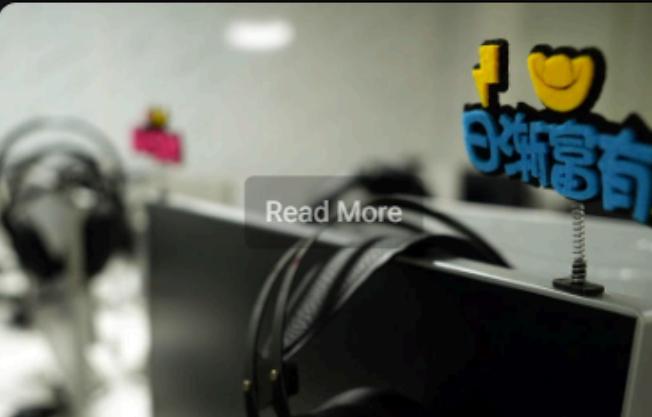
**CLICKSMART**

Cybercrime Guide Cybercrime Statistics About Us Resources Hub

## News and Articles



PHILIPPINE AUTHORITIES DETAIN MORE THAN 160 PEOPLE OVER SUSPECTED CYBERCRIME OPERATION  
09/01/2024, 07:00 AM, +0000 UTC



MAKING THE DIGITAL AND PHYSICAL WORLD SAFER:  
WHY THE CONVENTION AGAINST CYBERCRIME MATTERS  
12/24/2024, 08:00 AM, +0000 UTC



THE LATEST ON SOUTHEAST ASIA'S TRANSNATIONAL CYBERCRIME CRISIS  
10/30/2024, 07:00 AM, +0000 UTC



HOW IS SOUTHEAST ASIA TACKLING CYBERATTACKS ON THE UNDERRANKED?  
10/15/2024, 07:00 AM, +0000 UTC

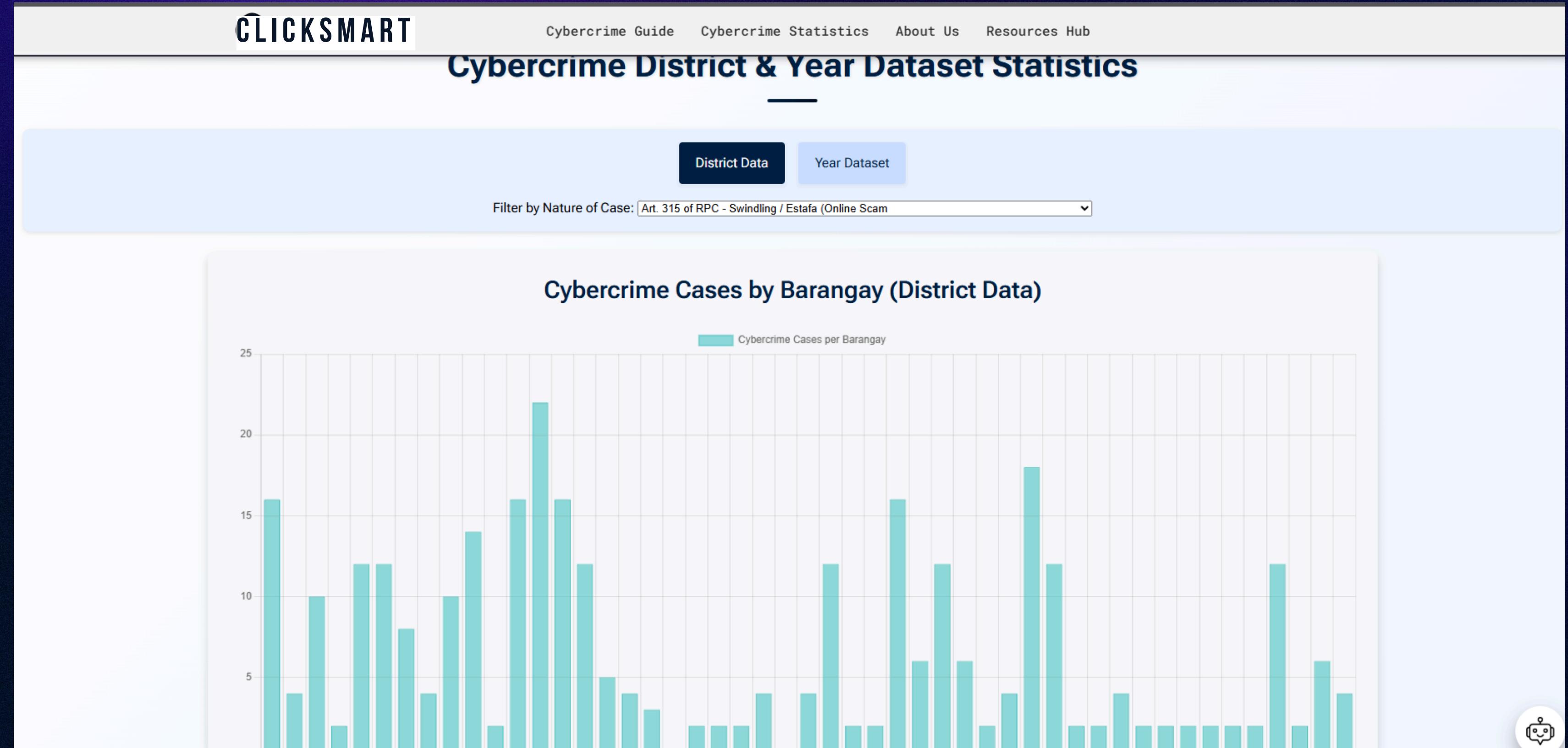
< Previous      Next >

Here's how ClickSmart works:

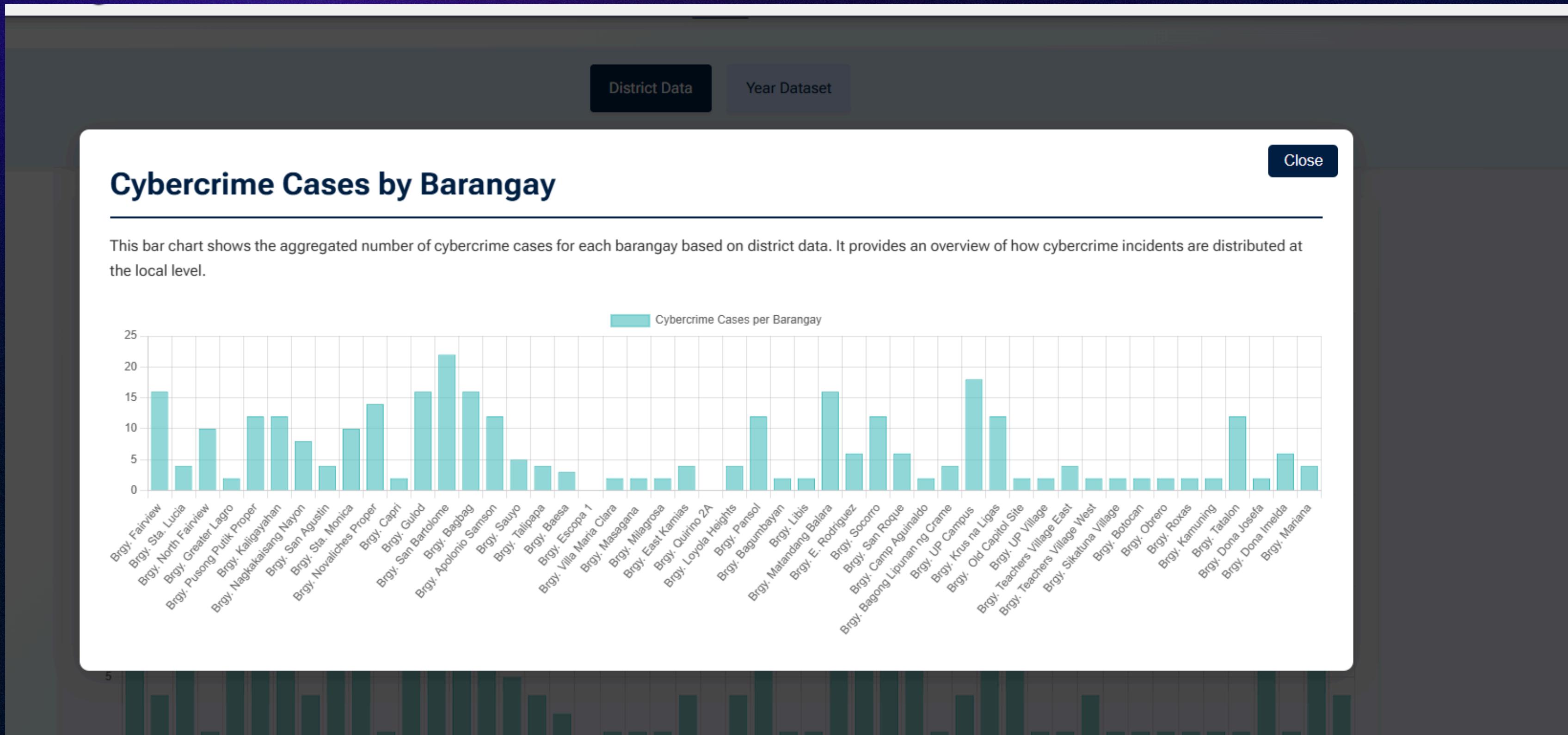
 LEARN:  
<https://news.un.org/en/story/2024/12/1158526>



# CYBERCRIME STATISTICS



# CYBERCRIME STATISTICS



# CYBERCRIME STATISTICS

**CLICKSMART**

Cybercrime Guide   Cybercrime Statistics   About Us   Resources Hub

ART. 315 OF RPC - SWINDLING / ESTAFA (ONLINE SCAM)   ART. 315 OF RPC - SWINDLING / ESTAFA (ONLINE SCAM)

## Crime Type Distribution

This pie chart displays the distribution of different types of cybercrime cases based on district data, helping you understand which crimes are more prevalent.

ART. 315 OF RPC - SWINDLING / ESTAFA (ONLINE SCAM)   ART. 315 OF RPC - SWINDLING / ESTAFA (ONLINE SCAM)

# ABOUT PAGE

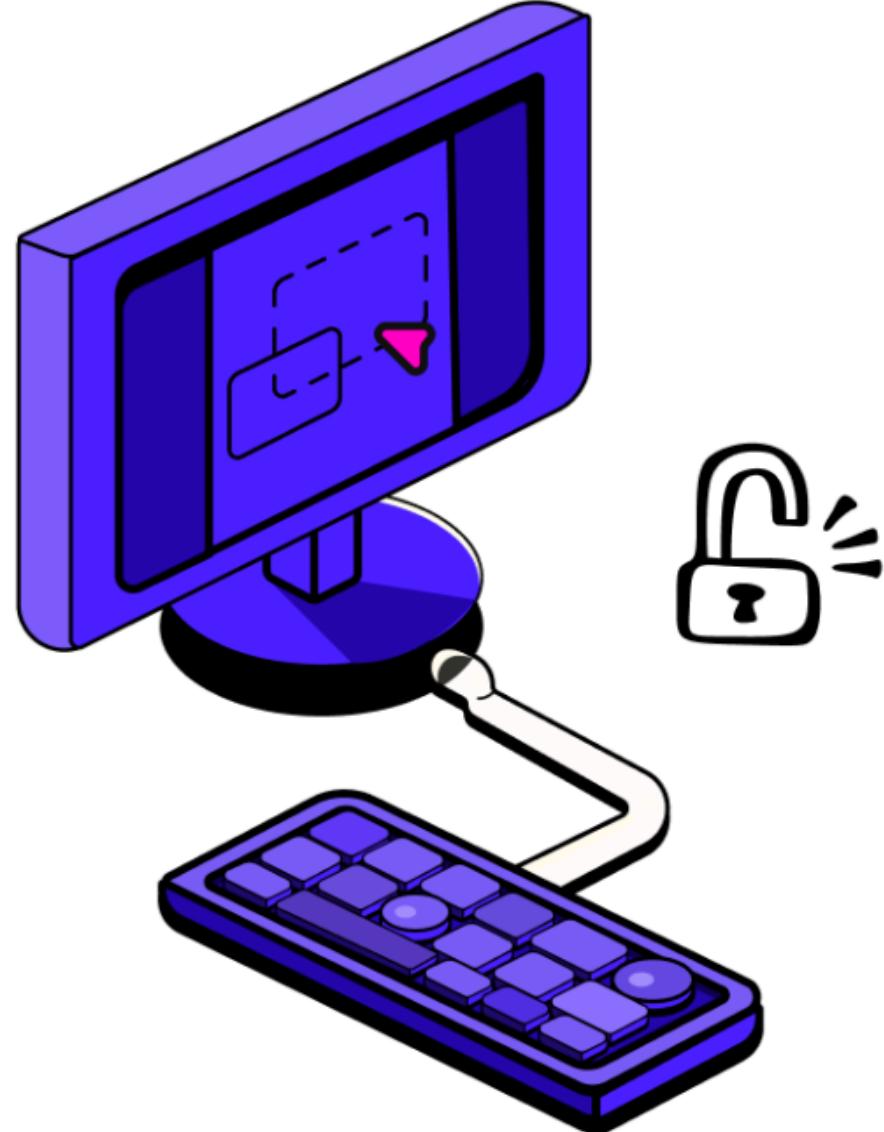
**CLICKSMART**

Cybercrime Guide   Cybercrime Statistics   About Us   Resources Hub

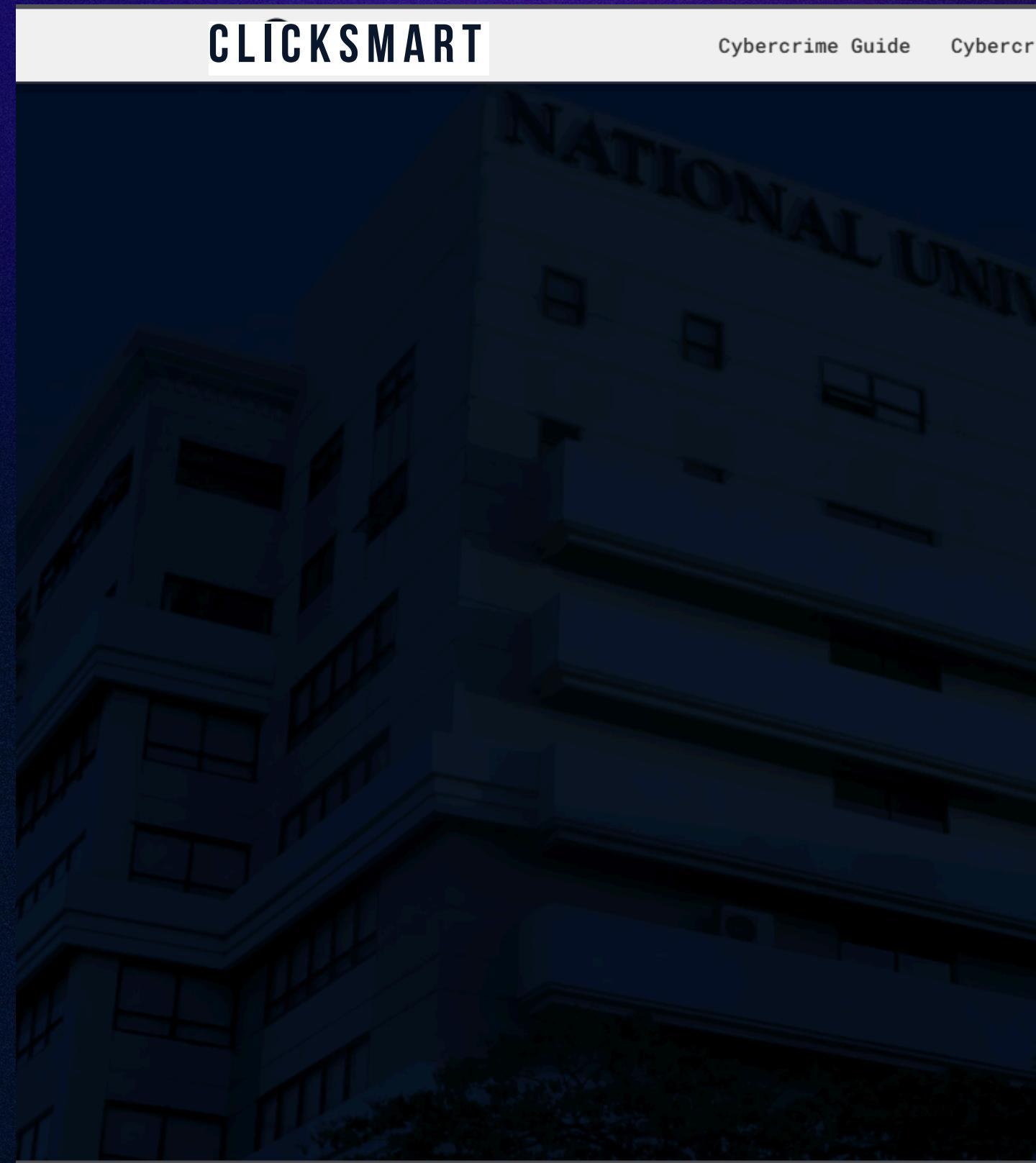
## About ClickSmart

ClickSmart is a free online platform dedicated to helping Filipinos stay informed and cautious online. With an **AI-powered chatbot** and **educational resources**, ClickSmart makes it easier to understand cyber threats, recognize scams, and learn how to report cybercrime to the Philippines authorities.

We believe that knowledge is the first line of defense — but ultimately, it is up to the individual to decide how to **respond, react, and act upon the information they acquire**. This project is based on the **Protection Motivation Theory (PMT)**, which says that people are more likely to protect themselves from cyber threats when they **understand the risks, see how serious the threat is, and believe that safety measures work**.



# ABOUT PAGE



**CLICKSMART**

Cybercrime Guide   Cybercrime Statistics   About Us   Resources Hub

## Made by Students

ClickSmart is a **thesis project by students of National University Philippines**, created to help raise awareness and educate Filipinos about online threats.

**Cybercrime** can happen to anyone, anywhere—no one is immune. But **awareness** is the first step toward staying safe. Our **goal** is to make cybersecurity information more accessible and easier to understand.



# RESOURCE HUB

**CLICKSMART**

Cybercrime Guide Cybercrime Statistics About Us Resources Hub

**RESOURCE HUB**

- [PNP-ACG Branches](#)
- [Developer Team Contacts](#)
- [Offline Resource](#)
- [Projects](#)

## PNP-ACG Branches

Find Philippine National Police Anti-Cybercrime Group branches near you.

### PNP-ACG Contact List (NCR)

**Quezon City District Anti-Cybercrime Team (QCDACT)**

**Contact:** 0968-873-5132 / 0927-142-9620

**Email:** operations.dact@gmail.com / qcpd.act2018@gmail.com / 2018dact@gmail.com

**Address:** Makarios Street, Corner Maginhawa, Brgy. Sikatuna Village, Quezon City

**Manila District Anti-Cybercrime Team (MDACT)**

**Contact:** 0995-973-2432 / 0968-875-1396

**Email:** mdact2022@gmail.com

**Address:** Ground Floor, Manila Police District HQ, UN Ave, Ermita, Manila

**Eastern District Anti-Cybercrime Team (EDACT)**

**Contact:** 0968-859-3183

**Email:** edact2020@gmail.com

**Address:** Romulo Building, Sta. Rosa Street, Brgy. Kapitolyo, Pasig City

**Northern District Anti-Cybercrime Team (NDACT)**

**Contact:** +82-888811-15 local 2217 / +63 928 512 8074

**Email:** ndact.pnpacg@gmail.com

**Address:** Northern Police District HQ, Tanigue St, Cor Dagat-Dagatan Ave, Caloocan City

**Southern District Anti-Cybercrime Team (SDACT)**

**Contact:** +63 956 344 0075 / +63 968-858-9836

**Email:** pnp.sdact@gmail.com

**Address:** 2nd Floor, SPD Building, Fort Bonifacio, Taguig City



# RESOURCE HUB

**CLICKSMART**

Cybercrime Guide   Cybercrime Statistics   About Us   Resources Hub

## PNP-ACG Regional Contact List

<b>PNP-ACG Region 1</b> <b>Address:</b> San Fernando, La Union <b>Contact:</b> (072) 607-6586 / acgregion1@pnp.gov.ph	<b>PNP-ACG Region 2</b> <b>Address:</b> Tuguegarao City, Cagayan <b>Contact:</b> (078) 304-1860 / acgregion2@pnp.gov.ph	<b>PNP-ACG Region 3</b> <b>Address:</b> Camp Olivas, Pampanga <b>Contact:</b> (045) 963-7753 / acgregion3@pnp.gov.ph	<b>PNP-ACG Region 4A</b> <b>Address:</b> Calamba City, Laguna <b>Contact:</b> (049) 545-2223 / acgregion4a@pnp.gov.ph
<b>PNP-ACG MIMAROPA</b> <b>Address:</b> Calapan City, Oriental Mindoro <b>Contact:</b> (043) 288-2329 / acgregion4b@pnp.gov.ph	<b>PNP-ACG Region 5</b> <b>Address:</b> Legazpi City, Albay <b>Contact:</b> (052) 742-8155 / acgregion5@pnp.gov.ph	<b>PNP-ACG Region 6</b> <b>Address:</b> Iloilo City, Iloilo <b>Contact:</b> (033) 329-9955 / acgregion6@pnp.gov.ph	<b>PNP-ACG Region 7</b> <b>Address:</b> Cebu City, Cebu <b>Contact:</b> (032) 254-7417 / acgregion7@pnp.gov.ph
<b>PNP-ACG Region 8</b> <b>Address:</b> Tacloban City, Leyte <b>Contact:</b> (053) 832-0405 / acgregion8@pnp.gov.ph	<b>PNP-ACG Region 9</b> <b>Address:</b> Pagadian City, Zamboanga del Sur <b>Contact:</b> (062) 215-3677 / acgregion9@pnp.gov.ph	<b>PNP-ACG Region 10</b> <b>Address:</b> Cagayan de Oro City, Misamis Oriental <b>Contact:</b> (088) 857-2955 / acgregion10@pnp.gov.ph	<b>PNP-ACG Region 11</b> <b>Address:</b> Davao City, Davao del Sur <b>Contact:</b> (082) 224-1625 / acgregion11@pnp.gov.ph
<b>PNP-ACG Region 12</b> <b>Address:</b> General Santos City, South Cotabato <b>Contact:</b> (083) 552-9735 / acgregion12@pnp.gov.ph	<b>PNP-ACG CAR</b> <b>Address:</b> Baguio City, Benguet <b>Contact:</b> (074) 422-5515 / acgcar@pnp.gov.ph	<b>PNP-ACG ARMM</b> <b>Address:</b> Cotabato City, Maguindanao <b>Contact:</b> (064) 421-2552 / acgarmm@pnp.gov.ph	<b>PNP-ACG CARAGA</b> <b>Address:</b> Butuan City, Agusan del Norte <b>Contact:</b> (085) 342-6177 / acgcaraga@pnp.gov.ph

Source: PNP-ACG Official Website

# RESOURCE HUB

The screenshot shows a webpage titled "Other Cybercrime-Related Agencies in the Philippines". The page includes a header with navigation links and a source attribution. Below the title, five agency profiles are listed in boxes:

- NBI Cybercrime Division**  
Contact: (632) 8523-8231  
Email: ccd@nbi.gov.ph  
Address: NBI Headquarters, 3rd Floor, JDC Center Building, No. 571 Engracia Cruz-Reyes Street, Ermita, Manila, Philippines 1000
- DOJ Office of Cybercrime**  
Contact: (632) 8523-8481  
Email: cybercrime@doj.gov.ph  
Address: DOJ Main Building, Padre Faura St, Ermita, Manila
- CICC (Cybercrime Investigation & Coordination Center)**  
Contact: 1326  
Email: complaints@cicc.gov.ph  
Address: DICT Complex, C.P. Garcia Avenue, Diliman, Quezon City
- National Privacy Commission (NPC)**  
Contact: (632) 8234-2228  
Email: info@privacy.gov.ph  
Address: 5th Floor, Delegation Building, PICC Complex, Pasay City
- DICT Cybersecurity Bureau**  
Contact: (632) 8920-0101  
Email: cybersecurity@dict.gov.ph  
Address: DICT Central Office, C.P. Garcia Ave, Diliman, Quezon City

At the bottom of the page, there are "Quick Links" and "Support" sections.

# RESOURCE HUB

**CLICKSMART**

Cybercrime Guide   Cybercrime Statistics   About Us   Resources Hub

**RESOURCE HUB**

PNP-ACG Branches  
Developer Team Contacts  
**Offline Resource**  
Projects

## Downloadable Materials

Access and download offline resources here.

 [Cybercrime Awareness Infographic](#)

 [ClickSmart Research Thesis](#)



# ASSESSMENT FORM

**CLICKSMART**

Cybercrime Guide Cybercrime Statistics About Us Resources Hub

## Cybercrime Assessment Form

This Cybercrime Assessment Form is designed to evaluate your knowledge and awareness of cybercrime, its various forms, and the appropriate actions to prevent and report incidents. Through this quiz, we aim to assess your understanding of the Philippine laws, key cybercrime concepts, and best practices for staying safe online.

• • • • •

Page 1 of 5

### Section 1: General Knowledge on Cybercrime

What is considered a cybercrime under Philippine law? \*

Unauthorized access to computer systems  
 Cyberbullying  
 Online scams or phishing  
 All of the above

What is the name of the Philippine law that addresses cybercrime? \*

Data Privacy Act of 2012  
 Cybercrime Prevention Act of 2012

# Emergency Hotlines



For urgent cases, contact:

- PNP-ACG: (632) 723-0401 local 7491 / 0961-731-9256
- NBI Cybercrime Division: (632) 8523-8231
- CICC-DICT: 1326
- DTI Consumer Hotline: 1-384
- BSP Consumer Affairs: (632) 8708-7087

# Our Team

For support or collaboration, contact the development team.

---

01

**Hanst Diether B. Abalos**

Team Leader / Researcher

abaloshb@students.national-u.edu.ph

03

**Joshua M. Dia**

Frontend / Backend Developer

dajm@students.national-u.edu.ph

05

**Vlademer Zane A. So**

Main Frontend Developer / Designer

sova@students.national-u.edu.ph

02

**John Russell M. Castillo**

AI Chatbot Model Developer

castillojm@students.national-u.edu.ph

04

**Farrah V. Montalban**

Main UI/UX Designer

montalbanfv@students.national-u.edu.ph

