

# CLICKSMART

EMPOWERING FILIPINOS AGAINST  
CYBER THREATS







# Tungkol Sa Amin

- **Libreng Online na Plataporma**
- **Chatbot na pinapagana ng AI:**
  - Sumasagot sa mga karaniwang tanong tungkol sa mga banta sa cyber
  - Nagagabay sa mga gumagamit sa pag-uulat ng mga insidente sa PNP Anti-Cybercrime Group
- **Pinapalakas ang mga Gumagamit:**
  - Kilalanin ang mga banta tulad ng phishing at mga scam
  - Gumawa ng mga proaktibong hakbang upang protektahan ang personal at digital na buhay



# Mga Hakbang sa Pag-iwas

---

- **Gumamit ng Matitibay na Password**

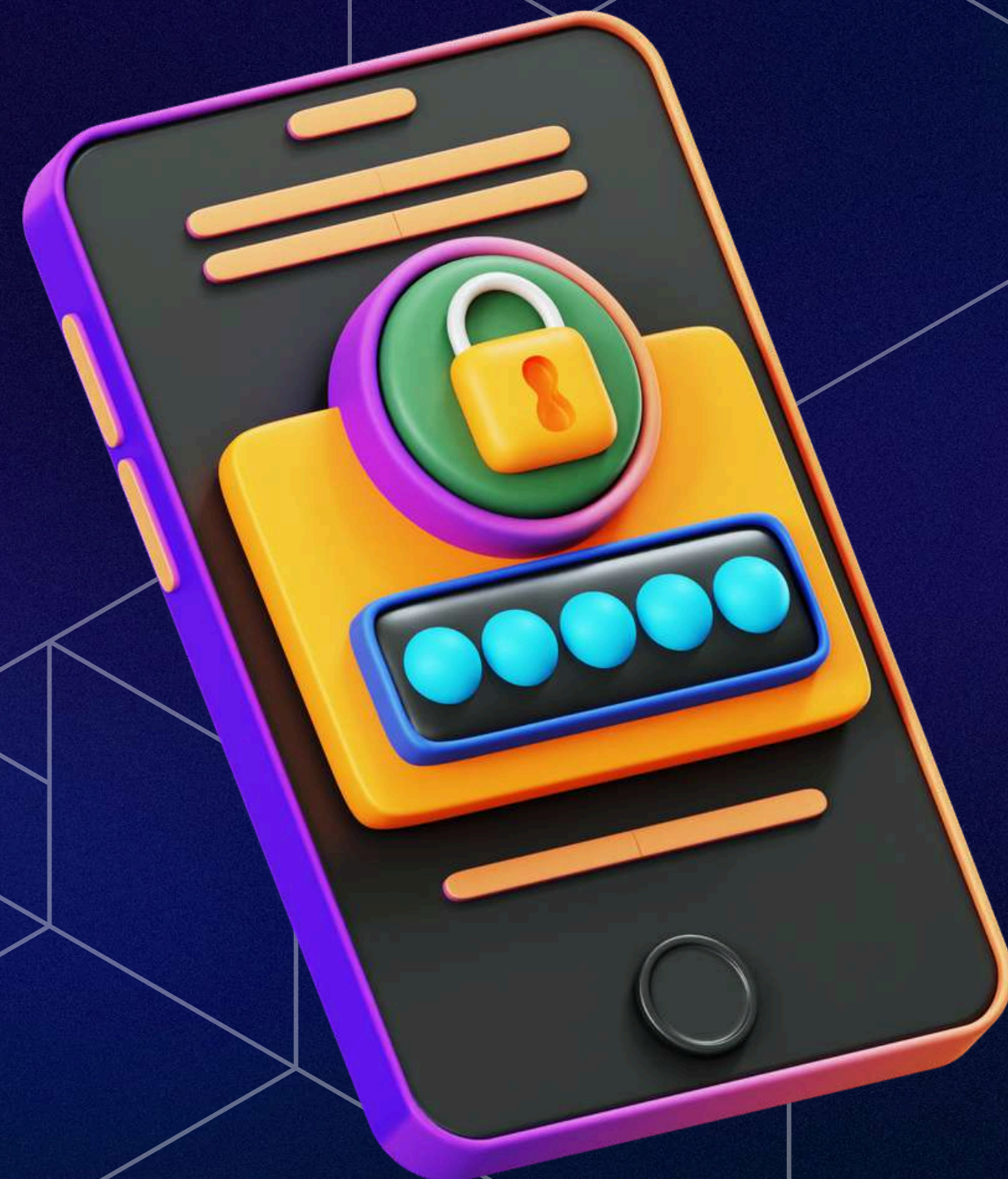
Gumawa ng mga complex na password na may kasamang mga letra, numero, at mga special character. Iwasan ang paggamit ng mga impormasyong madaling hulaan tulad ng mga kaarawan.

- **Iwasan ang Labis na Pagbabahagi sa Social Media**

Maging maingat sa mga personal na impormasyong ibinabahagi mo online, dahil maaaring gamitin ito laban sa iyo sa mga pag-atake ng phishing o pagnanakaw ng pagkakakilanlan

- **Mag-isip Bago Mag-Click**

Palaging beripikahin ang pinagmulan ng mga link at attachment bago makipag-ugnayan sa mga ito.





# Pagganap sa mga Phishing Emails o Mga Mensahe

- **Hindi Kilalang Tono o Pagbati**

Ang mga mensahe ng phishing ay madalas na gumagamit ng mga pangkalahatang pagbati tulad ng "Dear Customer" sa halip na ang iyong pangalan. Kung ang tono ay hindi parang karaniwan, ito ay maaaring isang babala

- **Mga Kamalian sa Gramatika at Pagbaybay**

Ang mga lehitimong organisasyon ay karaniwang nagpapatunay ng kanilang mga komunikasyon. Ang mga kamalian ay maaaring indikasyon ng isang pagtatangka sa phishing

- **Mga Hindi Pagkakatatugma sa mga Email Address**

Tingnan ang domain ng email ng nagpadala. Kung hindi ito tumutugma sa opisyal na domain ng organisasyon (halimbawa, @company.com), malamang ito ay isang scam.





# Pagganap sa mga Phishing Emails o Mga Mensahe

- **Mga Kahilingan na Nangangailangan ng Agad na Aksyon**

Ang mga email ng phishing ay madalas na lumilikha ng isang pakiramdam ng kagipitan, na hinihikayat ka na kumilos nang mabilis nang walang pag-iisip. Mag-ingat sa mga mensahe na nangangailangan ng agad na aksyon

- **Mga Kahina-hinalang mga Link o mga Nakalakip**

Itaas ang mouse sa ibabaw ng mga link upang makita ang tunay na URL bago mag-click. Kung ito ay tila kahina-hinala o hindi tumutugma sa pinag-aangkin na pinagmulan, huwag mag-click!





# Mga Senyas ng Isang Hacked na Device o Account

- Mga Hindi Kilalang Transaksyon

Ang mga diinaasahang mga singil sa iyong mga statement ng bangko o credit card ay maaaring indikasyon ng hindi awtorisadong pag-access.

- Pagkalock ng Account

Ang kahirapan sa pag-login sa iyong mga account, lalo na kung hindi mo pa nagbago ang iyong password, ay maaaring magpahiwatig ng hacking.

- Mga Hindi Inaasahang Kahilingan para sa Pagpapalit ng Password

Ang pagtanggap ng mga abiso tungkol sa mga pagbabago ng password na hindi mo sinimulan ay isang malakas na indikasyon ng posibleng paglabag.





# Mga Indikasyon na ang Iyong Personal na Data ay Maaaring Nakompromisa

- Pagtaas ng Spam o mga Pagtatangka sa Phishing

Ang biglaang pagtaas ng mga spam na email ay maaaring magpahiwatig na ang iyong impormasyon ay na-leak.

- Mga Hindi Kilalang Pagtatangka sa Pag-login

Ang mga abiso mula sa mga serbisyo tungkol sa mga pag-login mula sa hindi kilalang mga lokasyon o mga device ay maaaring magpahiwatig na may ibang tao na nagtatangka na mag-access sa iyong account.





# Mga Hakbang para Seguruhin ang Iyong mga Account Matapos ang Paglabag

---

- **Magpapalit ng mga Password**

Agad na magpapalit ng mga password sa lahat ng mga account, lalo na sa mga sensitibong impormasyon tulad ng bangko at mga account ng social media.

- **Mag-enable ng Two-Factor Authentication (2FA)**

I-enable ang 2FA sa lahat ng mga account na suportado nito.

- **Bantayan ang mga Pahayag ng Pinansyal**

Mahalagang bantayan ang iyong mga pahayag ng pinansyal, tulad ng mga statement ng bangko at credit card, para sa mga hindi inaasahang mga transaksyon.





# Anong Gawin Matapos Makaranas ng Cybercrime

- Seek Emotional Support

Mahalagang hanapin ang suporta emosyonal mula sa mga kaibigan, pamilya, o mga propesyonal na makakatulong sa iyo na makitungo sa mga emosyonal na epekto ng paglabag.

- Iulat ang Insidente

Mahalagang iulat ang insidente ng cybercrime sa mga kaugnay na partido at awtoridad kagaya ng PNP ACG.





# Mga Uri ng Cybercrime



## PERSONAL

Tumutukoy sa mga digital na krimen na direktang nagtutuon sa mga indibidwal, na nakakaapekto sa kanilang pinansyal, personal na seguridad, pribasiya, o reputasyon.



## KORPORATIBO/ NEGOSYO

Mga Cybercrime na Nakakaapekto sa mga Negosyo, Organisasyon, at mga Enterprise



## MGA BAGONG PELIGRO

Habang umaangat ang teknolohiya, nagbabago rin ang mga banta ng cybercrime upang mapahamak ang mga biktima sa mga bagong paraan.



## GOBYERNO AT KRITIKAL NA INFRAESTRUKTURA

Ang mga cybercrime na ito ay nagtutuon sa mga sistema ng gobyerno, mga serbisyo publiko, at seguridad ng bansa, sa halip na sa mga indibidwal o negosyo.

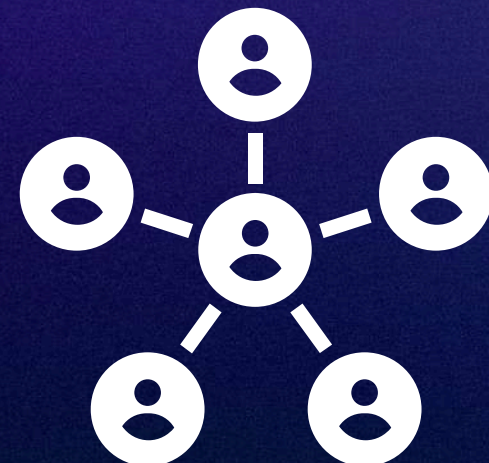


# Types of Cybercriminals



## MGA HACKER

Ang mga hacker ay mga indibidwal na nagkakamit ng hindi awtorisadong access sa mga sistema para sa iba't ibang mga dahilan.



## MGA ORGANISASYON NG CYBERCRIME

Ang mga grupo ng cybercrime ay mga samahan ng mga indibidwal na nagtatrabaho magkakasama para sa malawakang mga digital na krimen.



## MGA MANLOLOKO AT MGA MANDARAYA

Ang mga cybercriminal na ito ay mga taong nagpapaloko sa mga tao o negosyo upang magnakaw ng pera o mga datos ng pinansyal.



## MGA CYBER EXTORTIONISTA

Ang mga cyber extortionista ay mga cybercriminal na nagpapalit ng pera sa pamamagitan ng pagbanta sa mga biktima.



# Types of Cybercriminals



## MGA CYBER TERRORISTA

Ang mga cyber terrorist ay mga cybercriminal na nag-atake sa mga sistema at mga network para sa mga ideolohikal, pampolitika, o pangmilitar na mga dahilan.



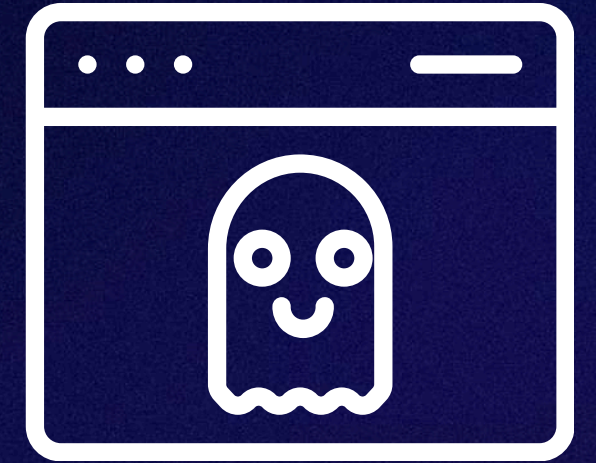
## MGA BANTA NG INSIDER

Ang mga insider threat ay mga cybercriminal na nasa loob ng isang organisasyon at gumagamit ng kanilang mga access upang magnakaw ng mga trade secret, manipulahin ang mga datos, o sabotahin ang mga negosyo.



## MGA CYBERBULLY AT MGA MANLULUPIT

Ang mga cyberbully at mga manlulupit ay mga taong nagpapalupit, nagpapakita ng karahasan, o nagpapaloko sa iba online.



## MGA KRIMINAL SA DARK WEB

Ang mga kriminal sa dark web ay mga cybercriminal na nag-oopera sa dark web, isang tagong bahagi ng internet na hindi madaling makita ng mga awtoridad.



# Types of Cybercriminals



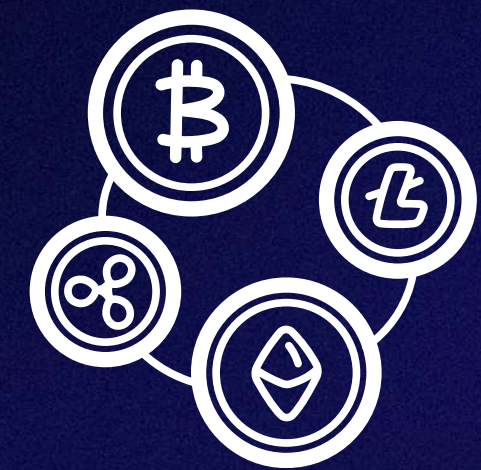
## MGA KRIMINAL NG AI SA CYBERCRIME

Ang mga kriminal ng AI sa cybercrime ay mga cybercriminal na gumagamit ng artificial intelligence (AI) upang magawa ang mga digital na krimen.



## MGA HACKER NG IOT

Ang mga hacker ng IoT ay mga cybercriminal na nagtutuon sa mga device ng Internet of Things (IoT), tulad ng mga smart home devices, mga smart TV, mga router, at iba pang mga device na konektado sa internet.



## MGA MANLULUKO NG NFT AT CRYPTO

Ang mga manluluko ng NFT at crypto ay mga cybercriminal na nagpapaloko sa mga platform ng NFT, blockchain, at cryptocurrency upang magnakaw ng pera o mga sensitibong impormasyon.



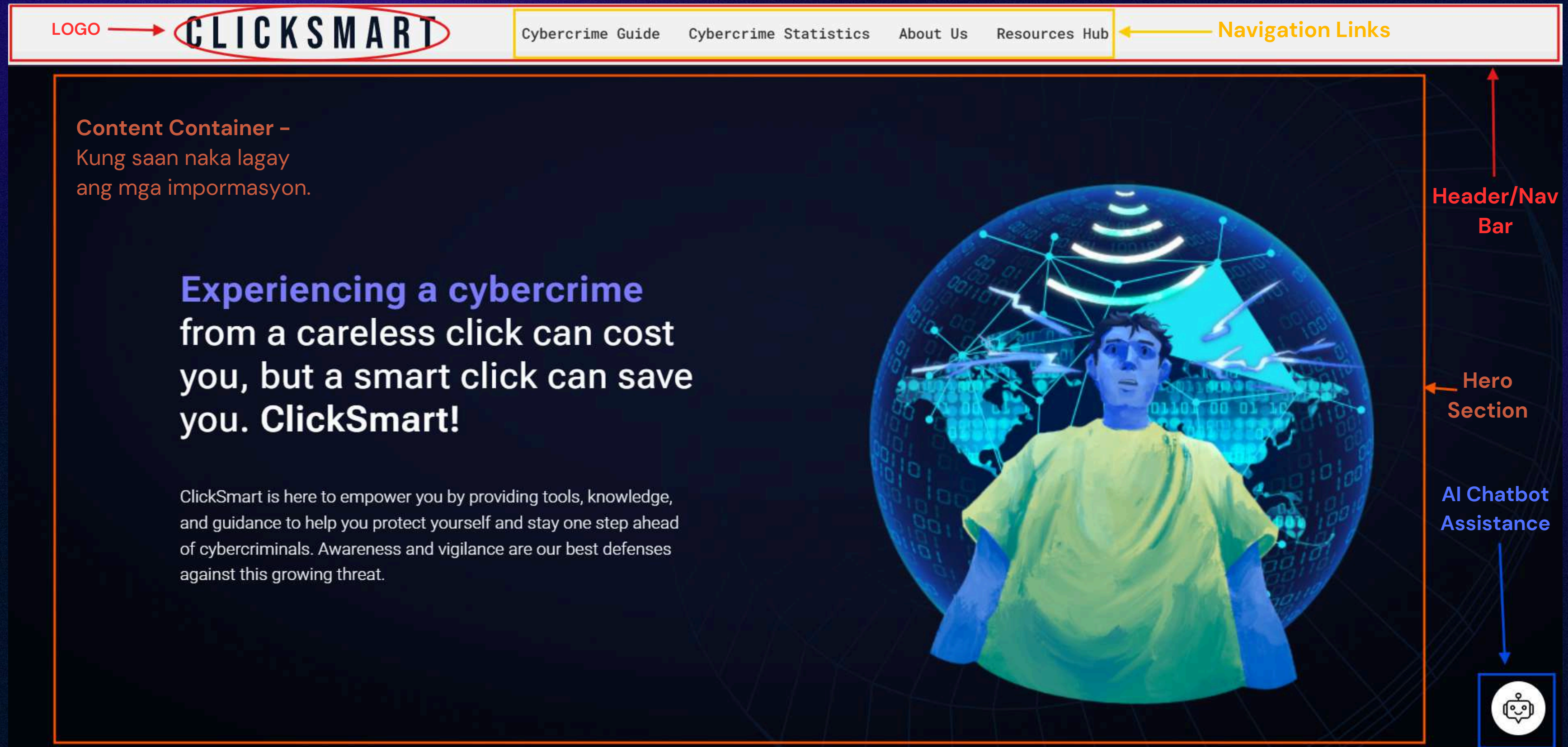
# CLICKSMART

MANWAL NG WEBSITE





# HOMEPAGE





# HOMEPAGE

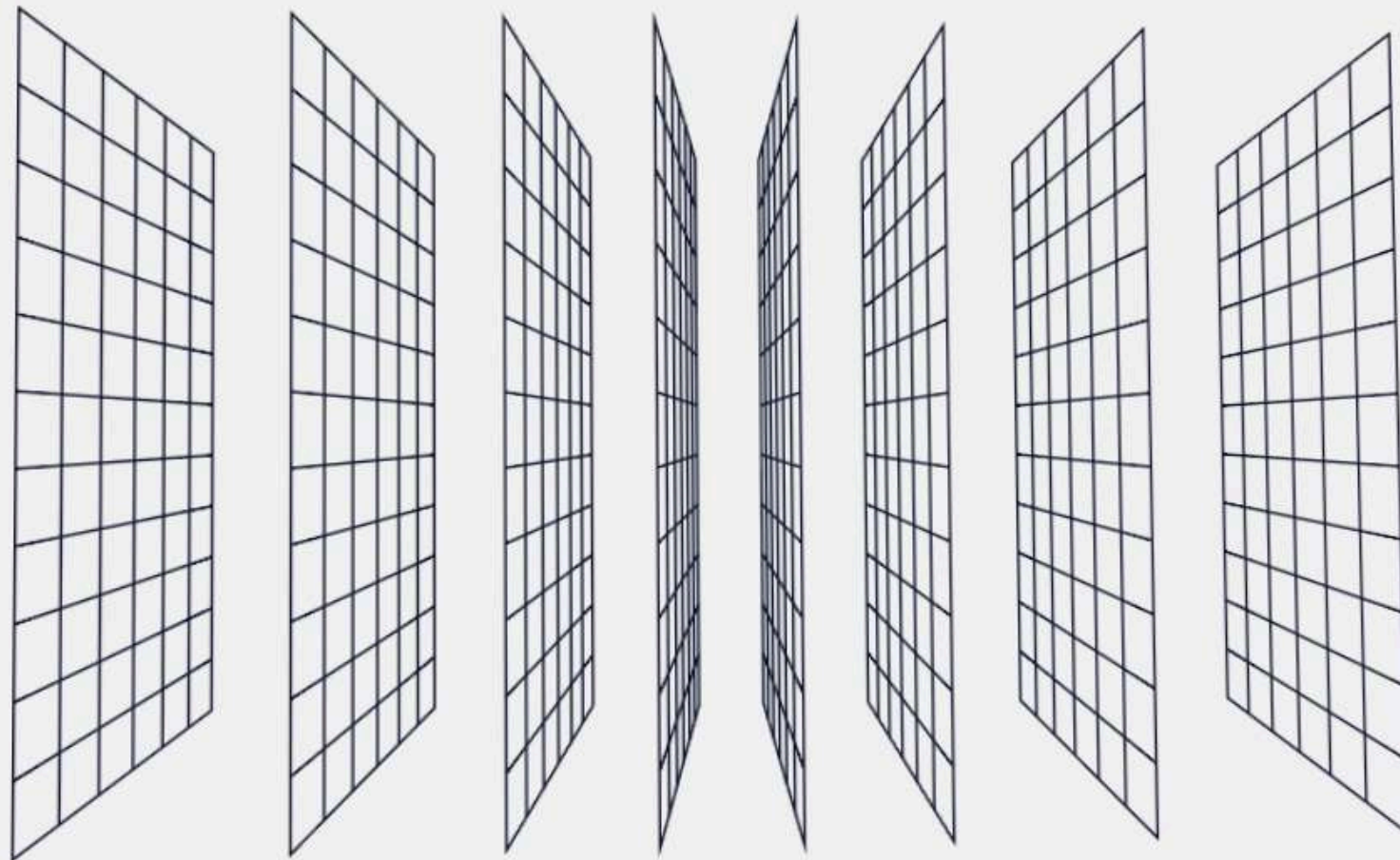
CLICKSMART

[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 GuideCybercrime StatisticsAbout UsResources Hub


Linked Content Container

News and Articles



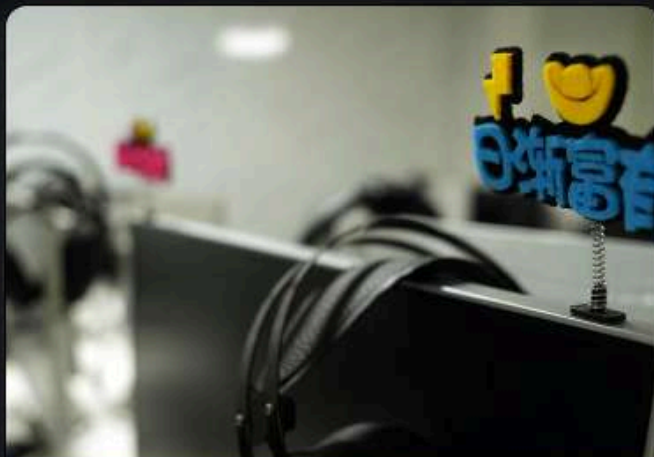
PHILIPPINE AUTHORITIES DETAIN MORE THAN 160 PEOPLE OVER SUSPECTED CYBERCRIME OPERATION

09/01/2024, 07:00 AM, +0000 UTC




THE LATEST ON SOUTHEAST ASIA'S TRANSNATIONAL CYBERCRIME CRISIS

10/30/2024, 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



HOW IS SOUTHEAST ASIA TACKLING CYBERATTACKS ON THE UNDERBANKED?

10/15/2024, 07:00 AM, +0000 UTC

< Previous

Next >

Pindutan para sa kasunod na pahina

Ang nilalaman at imahe ng balita

Pangunahin nilalaman ng balita

Oras kung kailan nilabas ang balita.



# HOMEPAGE (HOW CLICKSMART WORKS)

**CLICKSMART**[Cybercrime Guide](#)[Cybercrime Statistics](#)[About Us](#)[Resources Hub](#)

## Here's how ClickSmart works:

>

LEARN:

### Understand the Threats

- Dive into our **Cybercrime Guide**, a comprehensive resource that explains various types of cybercrime, how they occur, and how to stay protected.
- Interactive Chatbot Assistance: Need quick answers or clarification? Our friendly ClickBot is here 24/7 to answer your questions, offer personalized advice, and guide you through the site.
- Access examples and scenarios to better understand how cybercriminals operate.

>

ASSESS:

>

REPORT:

### Take Action When It Matters

- If you suspect or know you've been targeted by cybercrime, redirect to **Reporting Guide** and scroll down to find step-by-step guidance on how to report incidents.
- It has direct links to relevant authorities or agencies in the Philippines are available to ensure prompt action.
- If unsure about the reporting process, ask ChatBot to guide you through it interactively.

>

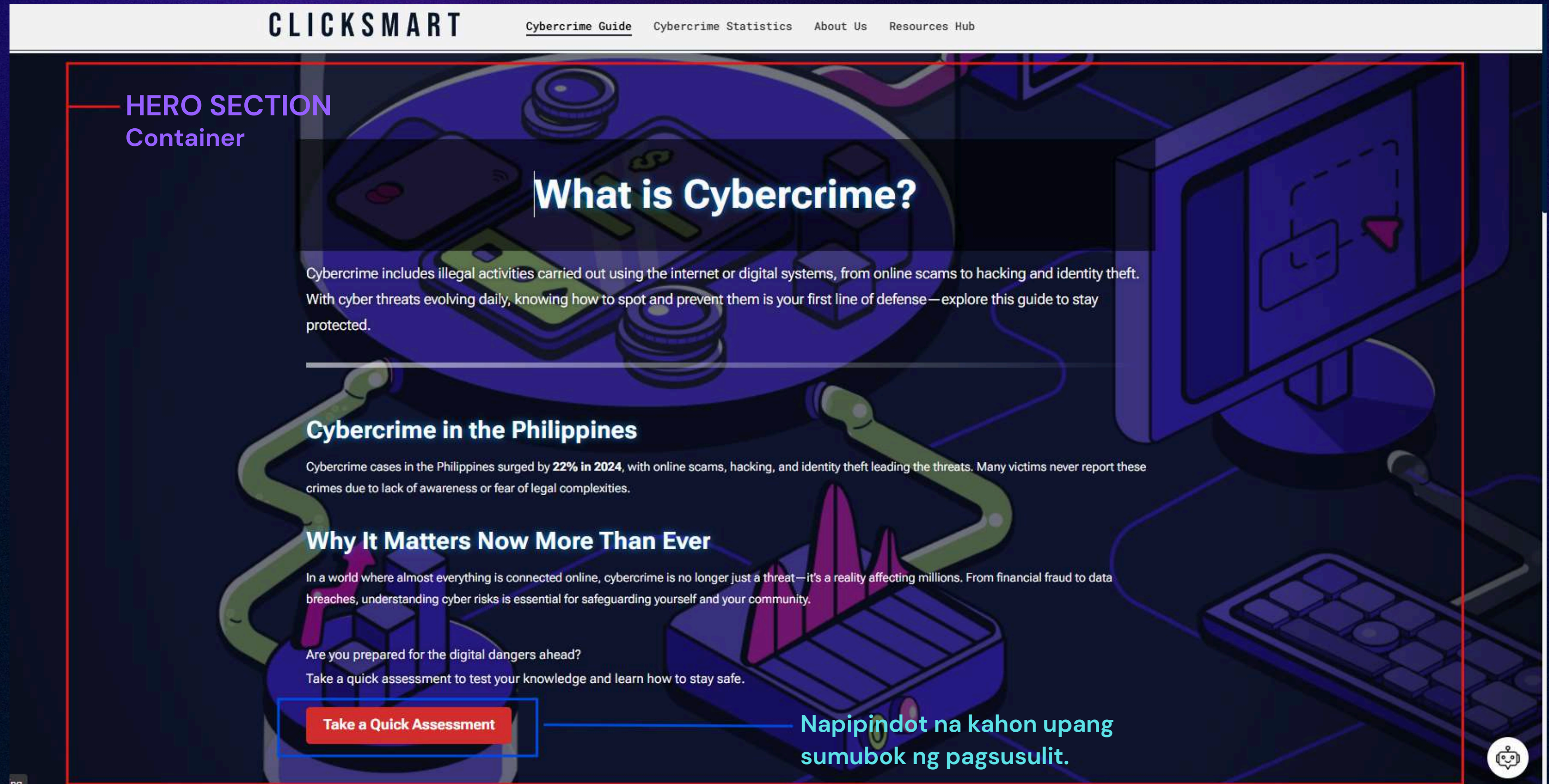
STAY UPDATED:

### Keep Yourself Ahead

- Visit our **Cybercrime Statistics** section for the latest data on cybercrime trends in the Philippines.
- Download **offline resources**, including **infographics and educational materials**, from our **Resources Hub**.
- Find official **PNP Anti-Cybercrime Group contact details** and other important **hotlines** to report cybercrime incidents.
- Get in touch with the **ClickSmart development team** for inquiries or support.



# CYBERCRIME GUIDE PAGE





# CYBERCRIME GUIDE PAGE

CLICKSMART

[Cybercrime Guide](#) [Cybercrime Statistics](#) [About Us](#) [Resources Hub](#)

## CYBERCRIMINAL SECTION CONTAINER

Napipindot na  
kahon para  
interaktibong  
maipakita ang  
impormasyon.

## Types of Cybercriminals

Before exploring cybercrimes, let's first identify those who commit them. [Click to learn more.](#)



Hackers



Cybercriminal  
Organizations



Scammers &  
Fraudsters



Cyber  
Extortionists



Cyber Terrorists



The Insider  
Threats



Cyberbullies &  
Harassers



Dark Web  
Criminals



AI  
Cybercriminals



IoT Hackers



NFT & Crypto  
Scammers

However, as technology evolves, new types of cybercriminals will continue to emerge.  
Staying informed about their tactics is crucial in protecting yourself from digital threats.






# CYBERCRIME GUIDE PAGE

**CLICKSMART**[Cybercrime Guide](#)[Cybercrime Statistics](#)[About Us](#)[Resources Hub](#)

## Types of Cybercriminals

Before exploring cybercrimes, let's first identify those who commit them. [Click to learn more.](#)



### Hackers

Individuals who gain unauthorized access to systems for different reasons.

**Black Hat Hackers** – Exploit security flaws for malicious intent.

**White Hat Hackers** – Security experts who help companies find vulnerabilities legally.

**Grey Hat Hackers** – Sometimes help fix security issues after breaking in.

**Red Hat Hackers** – Actively attack black hat hackers.

**Blue Hat Hackers** – Security testers hired by companies before product launches.

**Script Kiddies** – Use pre-made hacking tools with no deep knowledge.

**Insider Hackers** – Employees who exploit internal systems.

Maaring pumindot kahit saan sa madilim na parte, upang bumalik sa nakaraang pahina.

Ang container ng naipakitang impormasyon.



# CYBERCRIME GUIDE PAGE


**CLICKSMART**[Cybercrime Guide](#)[Cybercrime Statistics](#)[About Us](#)[Resources Hub](#)

**CYBERCRIME  
GUIDE SECTION  
CONTAINER**


Napipindot na kahon para interaktibong maipakita ang impormasyon.

## TYPES OF CYBERCRIME


Cybercrime comes in many forms. Select a category below to understand its impact and how to stay safe.




Personal Cybercrimes



Government & Critical Infrastructure Cybercrimes



Corporate/Business Cybercrimes




Emerging Cybercrime Threats

Kaunting imporsyon tungkol sa batas.

**Empower Yourself Against Cybercrime:** Awareness is your first line of defense against cybercriminals. Understanding your rights under **Philippine law** helps you **stay protected** and **take action**. The **Cybercrime Prevention Act of 2012 (RA 10175)** provides legal measures to combat digital crimes, ensuring accountability for online threats. [Click here](#) to learn more about your rights.

Napipindot na salita upang maipakita ang mga batas tungkol sa cybercrime sa Pilipinas.





# CYBERCRIME GUIDE PAGE

CLICKSMART

Cybercrime Guide

Cybercrime Statistics

About Us

Resources Hub

Maaring pumindot kahit saan sa madilim na parte, upang bumalik sa nakaraang pahina.

Napipindot na kahon para interaktibong maipakita pa ang adisyonal na impormasyon.

Personal Cybercrimes

Personal cybercrime refers to digital crimes that directly target individuals, affecting their finances, personal security, privacy, or reputation. These crimes often involve identity theft, scams, financial fraud, harassment, hacking, and data breaches that impact an individual rather than a business or government entity.

Scams & Online Fraud

Financial Fraud

Identity Theft

Phishing Attacks

Ransomware & Malware

Hacking & Unauthorized Access

Cyberstalking & Online Harassment

Sextortion & Revenge Porn

Online Shopping Fraud

Fake Social Media Profiles & Catfishing

Online Defamation & Doxxing

Child Exploitation & Grooming

⚠️ Note:

The information provided in this section is subject to updates and revisions by the development team. Cybercrime trends are constantly evolving, and details may change over time to ensure accuracy and relevance.

Stay safe.

Ang container ng naipakitang impormasyon.



# CYBERCRIME GUIDE PAGE

Maaring pumindot  
kahit saan sa  
madilim na parte,  
upang bumalik sa  
nakaraang pahina.

## SCAMS & ONLINE FRAUD

### What is it?

Scammers trick victims into giving money or personal information through deception. This includes investment fraud, fake online stores, job scams, and romance scams.

### Common Types of Scams in the Philippines:

- **Investment Scams (Ponzi, Pyramid Schemes)**  
Fraudsters promise high returns with little to no risk, luring victims into investing in fake schemes. Early investors may receive small payouts to build trust, but eventually, the scam collapses, and people lose their money.
- **Online Shopping Scams**  
Fraudulent sellers pretend to sell products online but never deliver the items or send defective ones.
- **Fake Job Offers**  
Scammers pose as employers, promising high-paying jobs but requiring applicants to pay a "training fee" or "processing fee" upfront.
- **Lottery & Prize Scams**  
Victims receive fake notifications claiming they have won a prize but must pay taxes or fees to claim it.
- **Romance Scams**  
Scammers pretend to be in a romantic relationship with victims, gaining their trust and eventually asking for money.

Ang container ng  
naipakitang  
impormasyon.



# CYBERCRIME GUIDE PAGE

CLICKSMART

Cybercrime GuideCybercrime StatisticsAbout UsResources Hub

How to Report Cybercrime in the Philippines

If you are a victim of cybercrime, follow the steps below to report the crime to the appropriate authorities.

Step-by-Step Guide

1. Gather Evidence: Take screenshots of the cybercrime.

2. Identify the Right Agency: Different agencies handle different types of cybercrime.

3. File an Online or In-Person Report: Report the crime to the appropriate agency.

4. Submit Required Documents: Bring the necessary documents to the agency.

5. Follow Up: Track your report status.

Select a Cybercrime Type:

-- Select Cybercrime Type --

Identity Theft

Online Scams & Fraud

Phishing & Online Fraud

Cyberbullying & Online Harassment

Sextortion & Online Blackmail

Cyber Libel & Defamation

Hacking & Unauthorized Access

Insider Threats & Data Leaks

Cyber Espionage & Spying

Child Exploitation & Online Grooming

Sexting Blackmail & Threats

Revenge Porn & Non-Consensual Image Sharing

Financial Fraud & Online Scams

Ransomware Attacks & Data Hijacking

Ransomware-as-a-Service (RaaS) Attacks

Distributed Denial of Service (DDoS) Attacks

Election Cybercrime & Voter Manipulation

Deepfake Scams & AI-Generated Fraud

What Should You Do?

Secure your accounts: Change passwords & enable Two-Factor Authentication (2FA).

Gather evidence: Take screenshots of unauthorized transactions and messages.

Report identity theft to PNP-ACG, NBI Cybercrime Division, or NPC.

TIP: Monitor your credit and bank statements regularly for unauthorized activities.

Where to Report	Contact Information	Online Report Link
PNP-ACG	(632) 723-0401 / acg@pnp.gov.ph	<a href="#">Report Here</a>
NBI Cybercrime Division	(632) 8523-8231 / ccd@nbi.gov.ph	<a href="#">Report Here</a>
National Privacy Commission (NPC)	(632) 8234-2228 / complaints@privacy.gov.ph	<a href="#">Report Here</a>

1. Napipindot na kahon upang interaktibong maipakita ang mga uri ng cybercrime.

2. Ang container ng naipakitang impormasyon matapos makapili ng cybercrime.

3. Napipindot na links upang madirekta sa orihinal na website ng mga awtoridad sa Pilipinas.



# ASSESSMENT FORM

CLICKSMART

Cybercrime GuideCybercrime StatisticsAbout UsResources 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

Container ng tanong sa pagsusulit

Pindutan sa pagpili ng sagot

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

☐ E-Commerce Act of 2000

☐ Anti-Hacking Act

Which government agency handles cybercrime complaints in the

Limang pahina ng pagsusulit na binubuo ng dalawangpung tanong.



# ASSESSMENT FORM

**CLICKSMART**[Cybercrime Guide](#)[Cybercrime Statistics](#)[About Us](#)[Resources Hub](#)

☐ Cybercrime Prevention Act of 2012

☒ E-Commerce Act of 2000

☐ Anti-Hacking Act

Which government agency handles cybercrime complaints in the Philippines? \*

☐ Department of Trade and Industry (DTI)

☐ National Bureau of Investigation (NBI) Cybercrime Division

☐ Department of Science and Technology (DOST)

☒ Commission on Information and Communications Technology (CICT)

What is a phishing attack? \*

☐ A type of fishing game played online

☐ An attempt to steal sensitive information by pretending to be a trustworthy entity

☐ A computer virus that deletes files

☒ A hacking method used to overload servers

Next


Pindutan para sa susunod na pahina.



# ASSESSMENT FORM

**CLICKSMART**[Cybercrime Guide](#)[Cybercrime Statistics](#)[About Us](#)[Resources Hub](#)

**Matapos ang pagsusulit, ang user ay maaring masuri ang kanilang sagot o sumubok muli.**

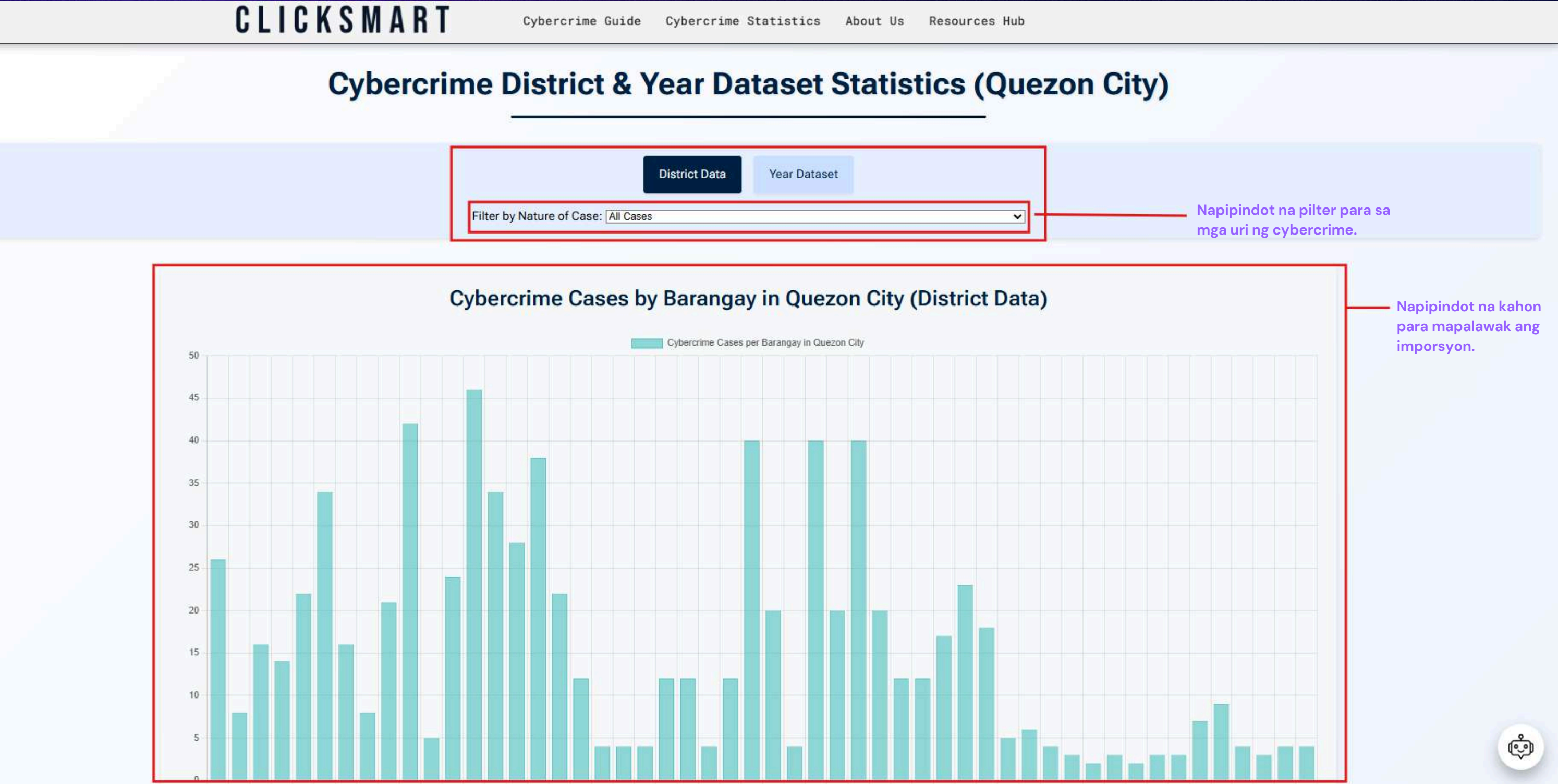
 **Keep learning! Cyber threats evolve — stay informed.**

**Your Score: 6 / 20**

[Review Answers](#)[Try Again](#)



# CYBERCRIME STATISTICS PAGE





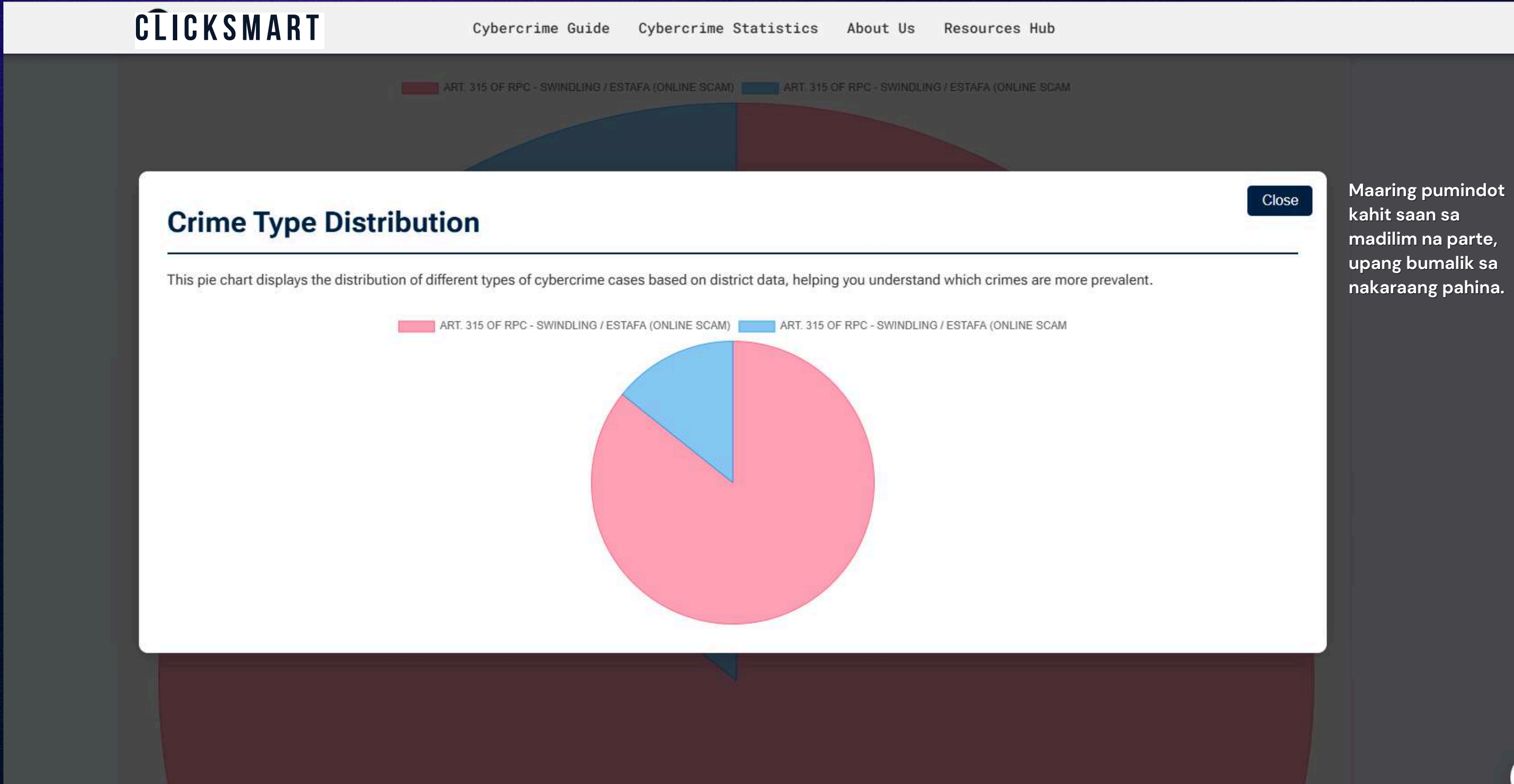
# CYBERCRIME STATISTICS



Maaring pumindot  
kahit saan sa  
madilim na parte,  
upang bumalik sa  
nakaraang pahina.



# CYBERCRIME STATISTICS



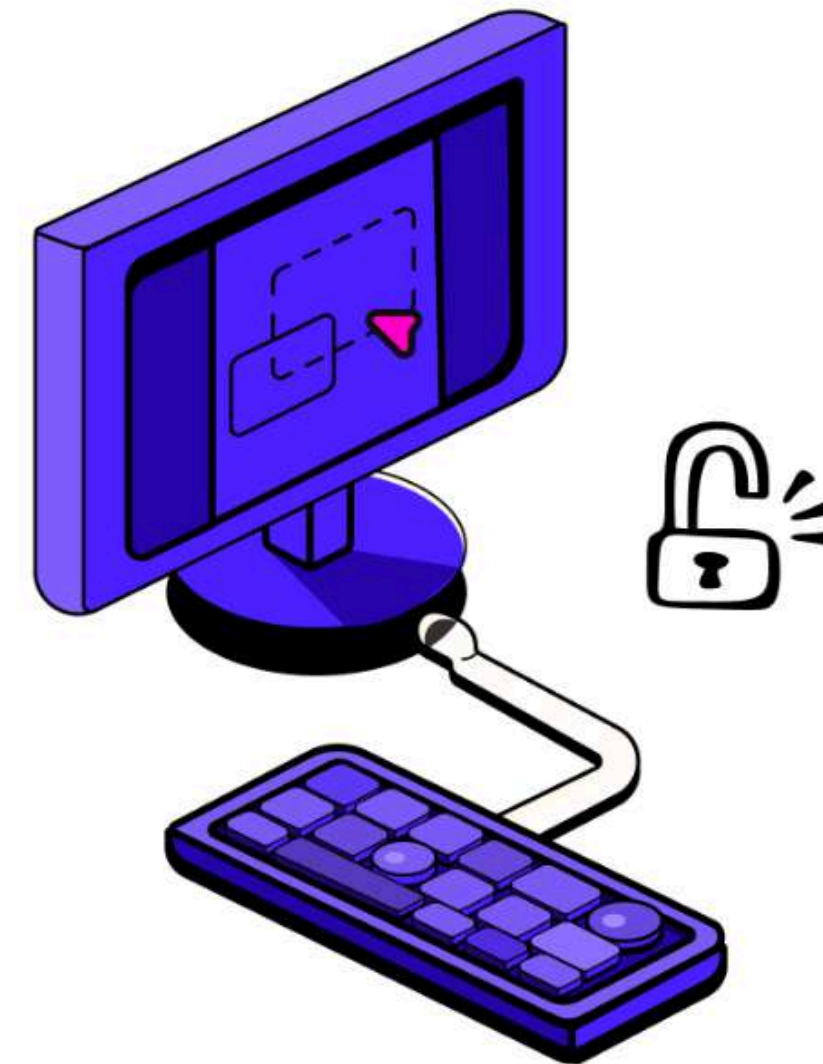


# ABOUT PAGE

## 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

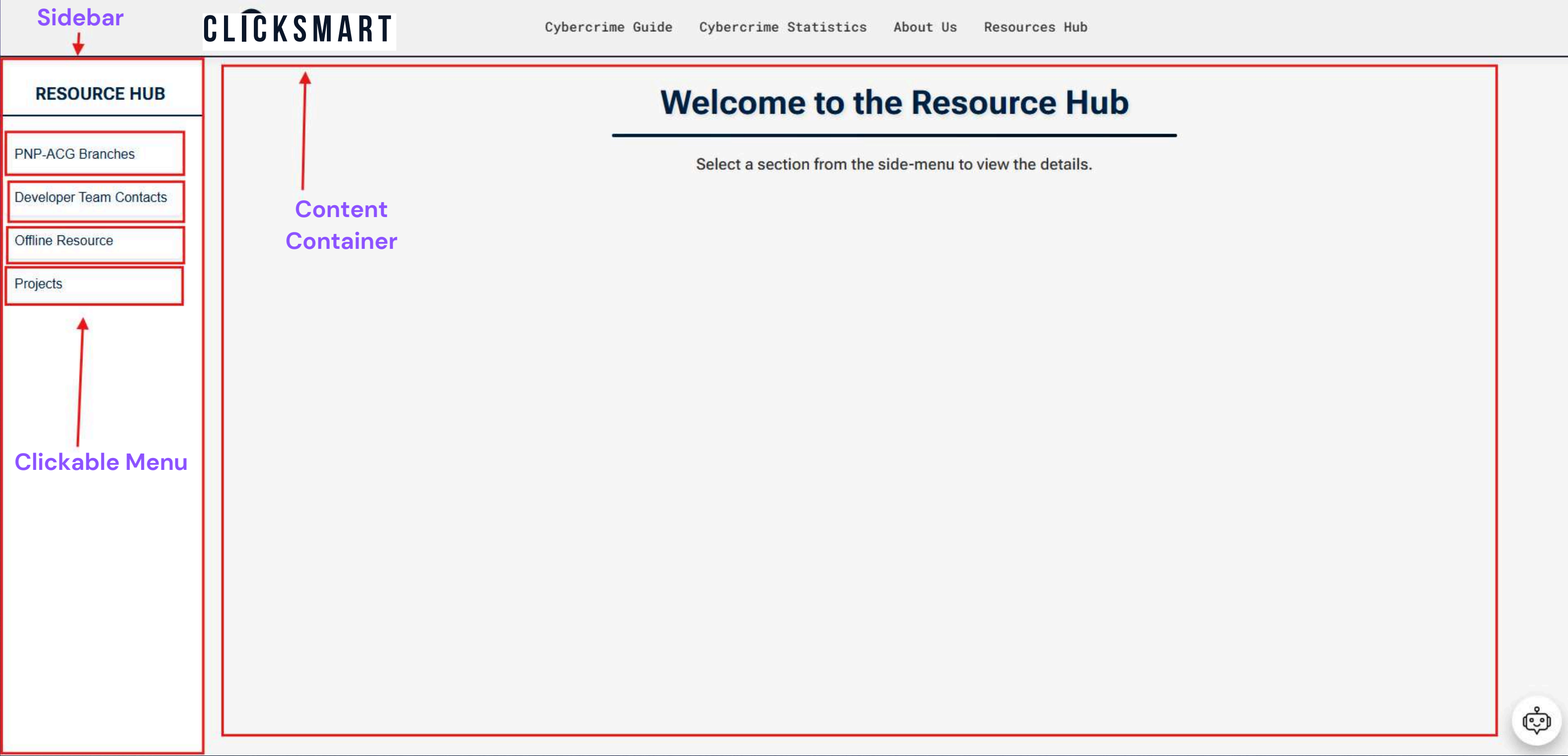
ClickSmart is a **thesis project by students of National University Philippines**, created to help **raise awareness and educate Filipinos about online threats**.

**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





# RESOURCE HUB

CLICKSMART

Cybercrime GuideCybercrime StatisticsAbout UsResources 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 / qcpcd.act2018@gmail.com / 2018dact@gmail.com

Address: Makadios 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

Source: PNP-ACG Official Website



# RESOURCE HUB

PNP-ACG Regional Contact List

PNP-ACG Region 1

**Address:** San Fernando, La Union  
**Contact:** (072) 607-6586 /  
acgregion1@pnp.gov.ph

PNP-ACG Region 2

**Address:** Tuguegarao City,  
Cagayan  
**Contact:** (078) 304-1860 /  
acgregion2@pnp.gov.ph

PNP-ACG Region 3

**Address:** Camp Olivas, Pampanga  
**Contact:** (045) 963-7753 /  
acgregion3@pnp.gov.ph

PNP-ACG Region 4A

**Address:** Calamba City, Laguna  
**Contact:** (049) 545-2223 /  
acgregion4a@pnp.gov.ph

PNP-ACG MIMAROPA

**Address:** Calapan City, Oriental  
Mindoro  
**Contact:** (043) 288-2329 /  
acgregion4b@pnp.gov.ph

PNP-ACG Region 5

**Address:** Legazpi City, Albay  
**Contact:** (052) 742-8155 /  
acgregion5@pnp.gov.ph

PNP-ACG Region 6

**Address:** Iloilo City, Iloilo  
**Contact:** (033) 329-9955 /  
acgregion6@pnp.gov.ph

PNP-ACG Region 7

**Address:** Cebu City, Cebu  
**Contact:** (032) 254-7417 /  
acgregion7@pnp.gov.ph

PNP-ACG Region 8

**Address:** Tacloban City, Leyte  
**Contact:** (053) 832-0405 /  
acgregion8@pnp.gov.ph

PNP-ACG Region 9

**Address:** Pagadian City,  
Zamboanga del Sur  
**Contact:** (062) 215-3677 /  
acgregion9@pnp.gov.ph

PNP-ACG Region 10

**Address:** Cagayan de Oro City,  
Misamis Oriental  
**Contact:** (088) 857-2955 /  
acgregion10@pnp.gov.ph

PNP-ACG Region 11

**Address:** Davao City, Davao del Sur  
**Contact:** (082) 224-1625 /  
acgregion11@pnp.gov.ph

PNP-ACG Region 12

**Address:** General Santos City,  
South Cotabato  
**Contact:** (083) 552-9735 /  
acgregion12@pnp.gov.ph

PNP-ACG CAR

**Address:** Baguio City, Benguet  
**Contact:** (074) 422-5515 /  
acgcar@pnp.gov.ph

PNP-ACG ARMM

**Address:** Cotabato City,  
Maguindanao  
**Contact:** (064) 421-2552 /  
acgarmm@pnp.gov.ph

PNP-ACG CARAGA

**Address:** Butuan City, Agusan del  
Norte  
**Contact:** (085) 342-6177 /  
acgcaraga@pnp.gov.ph

Source: PNP-ACG Official Website





# RESOURCE HUB

CLICKSMART

[Cybercrime Guide](#)[Cybercrime Statistics](#)[About Us](#)[Resources Hub](#)

Other Cybercrime-Related Agencies in the Philippines

**NBI Cybercrime Division**

**Contact:** (632) 8523-8231

**Email:** [ccd@nbi.gov.ph](mailto: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](mailto: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](mailto: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](mailto: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](mailto:cybersecurity@dict.gov.ph)

**Address:** DICT Central Office, C.P. Garcia Ave, Diliman, Quezon City

Quick Links

[Home](#)[Cybercrime Guide](#)[About ClickSmart](#)[Resources Hub](#)

Support

[PNP-ACG Branches](#)[Developer Team Contacts](#)[Downloadable Material](#)[Direct Message PNP-ACG](#)[ACG Social Media Link](#)

© 2025 ClickSmart. All Rights Reserved.



# RESOURCE HUB

CLICKSMART

Cybercrime GuideCybercrime StatisticsAbout UsResources Hub

RESOURCE HUB

PNP-ACG BranchesDeveloper Team ContactsOffline ResourceProjects

The Developer Team Contacts

For support or collaboration, contact the development team.

Meet the Development Team

Hanst Diether B. Abalos

Role: Project Manager / Researcher

Email: abaloshb@students.national-u.edu.ph

John Russell M. Castillo

Role: AI Chatbot Model Developer

Email: castillojm@students.national-u.edu.ph

Joshua M. Dia

Role: Frontend / Backend Developer

Email: diajm@students.national-u.edu.ph

Farrah V. Montalban

Role: Main UI/UX Designer

Email: montalbanfv@students.national-u.edu.ph

Vlademer Zane A. So

Role: Main Frontend Developer / Designer

Email: sova@students.national-u.edu.ph



# RESOURCE HUB

CLICKSMART

Cybercrime GuideCybercrime StatisticsAbout UsResources 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

Nadodownload na bagay.





# WEBSITE FOOTER

## Quick Links

- Home
- Cybercrime Guide
- About ClickSmart
- Resources Hub

Mga napipindot na links.

## Support

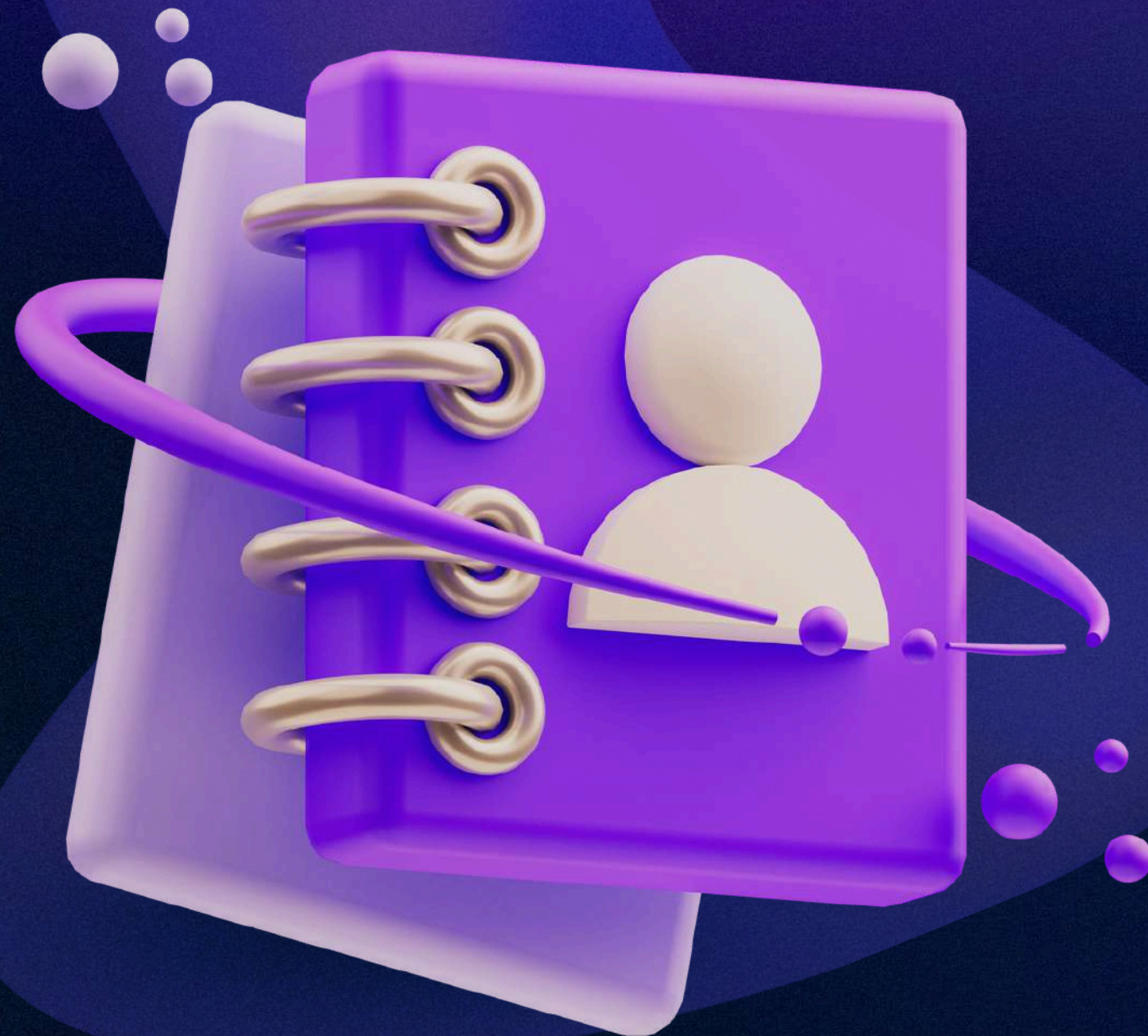
- PNP-ACG Branches
- Developer Team Contacts
- Downloadable Material
- Direct Message PNP-ACG
- ACG Social Media Link



# MGA EMERGENCY HOTLINE

Maaaring makipag-ugnay sa mga sumusunod na mga hotline para sa mga kaso na kinakailangan ng agarang atensyon.

- 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





# Aming Team

Para sa mga katanungan, suporta, o pag-uusap tungkol sa pagtutulungan, maaaring makipag-ugnay sa aming development team.

---

01

**Hanst Diether B. Abalos**

Team Leader / Researcher

abaloshb@students.national-  
u.edu.ph

02

**John Russell M. Castillo**

AI Chatbot Model Developer

castillojm@students.national-  
u.edu.ph

03

**Joshua M. Dia**

Frontend / Backend Developer

diajm@students.national-u.edu.ph

04

**Farrah V. Montalban**

Main UI/UX Designer

montalbanfv@students.national-  
u.edu.ph

05

**Vlademer Zane A. So**

Main Frontend Developer /  
Designer

sova@students.national-  
u.edu.ph

