Digital Threats, Real Consequences: The Societal Impact of Cybercrime

ATTY. ABRAM M. GERONAGA, LPT
Fraud and Financial Crimes Division
NBI Manila

CONTEXT AND RELEVANCE

The **Philippine Development Plan (PDP) 2023-2028** **highlights digital transformation as a underlying theme, aiming to establish a strong digital economy** that positions the Philippines as a "globally competitive" nation. A key objective is to close the "digital divide" across the country, where almost 40% of the population still lacks reliable internet access.

It lays the groundwork for transforming public financial management through the digitalization of payment systems. By bridging the digital divide, improving infrastructure, and promoting inclusivity, the Philippines can enhance governance, boost economic competitiveness, and better serve its citizens.

Addressing infrastructure gaps, enhancing cybersecurity to protect digital payment platforms, and improving digital and cybersecurity literacy among citizens and government workers are essential for successful digitalization of government payments

NAVIGATION OF TOPICS

01

Introduction to Cybercrime

02

Economic Effects of Cybercrime

03

Technological and Infrastructural Challenges

04

Legal and Policy Framework

05

Prevention and Mitigation

01

Introduction to Cybercrime

Cybercrime is a complex global concern involving criminals and nation-states aiming to compromise networks, disrupt critical infrastructure, and steal money and intellectual property.

Section 4 of Cybercrime Prevention Act of 2012 (RA 10175)

A. Offenses Against the Confidentiality, Integrity, and Availability of Computer Data and Systems
1. Illegal Access: Unauthorized access to a computer system.
2. Illegal Interception: Interception of communications without authorization.
3. Data Interference: Unauthorized alteration, deletion, or destruction of computer data.
4. System Interference: Hindering or interfering with computer system functioning.
5. Misuse of Devices: Possession, production, or distribution of tools intended for committing cybercrimes.
5. Cyber-squatting: Using a domain name in bad faith to profit from another's trademark or name

ILLEGAL ACT	ILLEGAL ACCESS	ILLEGAL INTERCEPTION	DATA INTERFERENCE	SYSTEM INTERFERENCE	MISUSE OF DEVICES	CYBER-SQUATTING
TARGET	COMPUTER SYSTEMS OR NETWORKS	DATA IN TRANSIT (COMMUNICATION)	STORED OR TRANSMITTED DATA	COMPUTER SYSTEMS OR NETWORKS	TOOLS OR DEVICES ENABLING CYBERCRIMES	DOMAIN NAMES OR TRADEMARKS
ACTION	GAINING UNAUTHORIZED ACCESS	INTERCEPTING OR CAPTURING TRANSMISSIONS	ALTERING, DELETING, OR CORRUPTING DATA	DISRUPTING OR DISABLING SYSTEMS	CREATING, POSSESSING, OR DISTRIBUTING TOOLS	REGISTERING DOMAINS IN BAD FAITH
GOAL	GAIN UNAUTHORIZED CONTROL OR INFORMATION	SPY ON OR STEAL PRIVATE INFORMATION	DAMAGE OR MANIPULATE DATA	PREVENT SYSTEMS FROM FUNCTIONING PROPERLY	FACILITATE OR ENABLE CYBERCRIMINAL ACTIVITIES	PROFIT FROM OR EXPLOIT ANOTHER'S REPUTATION
EXAMPLES	HACKING INTO ACCOUNTS, ACCESSING SERVERS	TAPPING PHONE CALLS, INTERCEPTING EMAILS	MODIFYING FINANCIAL RECORDS, DELETING FILES	DDOS ATTACKS, MALWARE CRASHES	SELLING HACKING SOFTWARE, CREATING KEYLOGGERS	REDIRECTING TRAFFIC, SELLING DOMAINS TO OWNERS
LEGAL FOCUS	PREVENTS UNAUTHORIZED ACCESS TO SYSTEMS	PROTECTS COMMUNICATION CONFIDENTIALITY	PROTECTS DATA INTEGRITY AND AVAILABILITY	PROTECTS SYSTEM FUNCTIONALITY	PREVENTS USE AND SPREAD OF MALICIOUS TOOLS	PROTECTS INTELLECTUAL PROPERTY AND TRADEMARKS

Section 4 of Cybercrime Prevention Act of 2012 (RA 10175)

B. Computer-Related Offenses

1. **Computer-Related Forgery**: Alteration of data to deceive.
2. **Computer-Related Fraud**: Inputting or altering data to cause damage or gain.
3. **Computer-Related Identity Theft**: Unauthorized acquisition or use of someone else’s identity

Section 4 of Cybercrime Prevention Act of 2012 (RA 10175)

C. Content-Related Offenses

1. **Cybersex**: Using a computer system for sexually explicit acts for profit or favor.
2. **Child Pornography**: Producing, distributing, or accessing child pornography through a computer.
3. **Unsolicited Commercial Communications**: Sending spam with misleading or fraudulent content.
4. **Libel**: Committing libel through computer systems or other digital mean

Section 5 of Cybercrime Prevention Act of 2012 (RA 10175)

Attempt to Commit Cybercrime

Any individual who attempts to commit any of the offenses listed in Section 4 (e.g., hacking, cyber libel, cyber fraud) is punishable under the law.

Aiding or Abetting Cybercrime

Any person who assists, facilitates, or supports the commission of cybercrimes is also liable under this act.

Section 6 of Cybercrime Prevention Act of 2012 (RA 10175)

Section 6 of the Cybercrime Prevention Act of 2012 (Republic Act No. 10175) provides for the Penalties for Cybercrimes. It emphasizes that if a crime punishable under the Revised Penal Code or special laws is committed with the use of information and communications technology (ICT), the penalty imposed will be one degree higher than that specified for the crime.

SIGNIFICANT EVENTS IN THE EVOLUTION OF CYBERCRIME

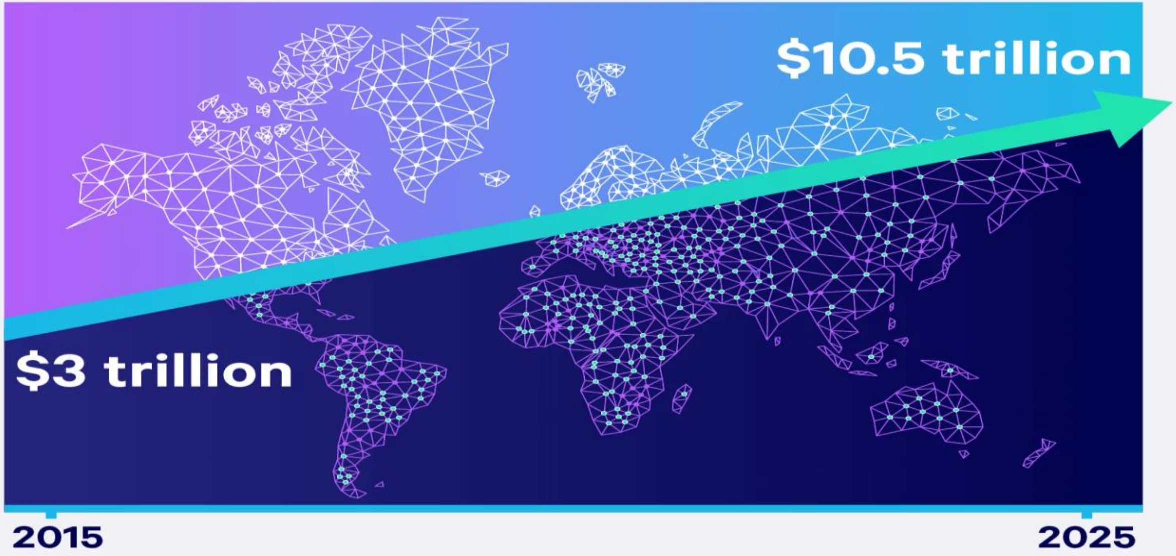
1. **1971**: First computer virus, Creeper Virus, created.
2. **1980s**: Rise of hacker culture and **phone phreaking** for free calls.
3. **1988**: Morris Worm causes first major internet disruption.
4. **1990s**: Internet proliferation enables widespread **malware** and hacking
5. **2000s**: Surge in **identity theft**, **phishing scams**, and **botnets** for attacks.
6. **2010s**: Emergence of **ransomware**, **APTs**, and illegal **dark web** marketplaces.
7. **Present**: Increasing **data breaches** and sophisticated nation-state cyberattacks.
8. **Future: ---**

HOW COULD CYBERCRIME COULD EVOLVE IN THE COMING YEARS?

A. Cyber Espionage and Manipulation of Public Financial Data
- Manipulation of Financial Records: In the future, state-sponsored or organized criminal groups could engage in **cyber espionage** to manipulate public financial records, altering tax information, disbursement logs, or payments. This could distort government accounting, lead to misallocation of public funds, and undermine the accuracy of public financial reporting.

B. Rise of Bio-Cybercrime
- Biometric Spoofing: As biometrics like facial recognition and fingerprints become common, criminals may develop advanced techniques to spoof them.
- Biotech Hacks: Hacking into biotechnology systems to alter medical records, manipulate genetic data, or compromise health devices like pacemakers.

Growth of Cybercrime Costs



THESE COSTS CAN BE CATEGORIZED AS FOLLOWS:

1. Direct Costs

-Financial losses from theft, fraud, or ransom payments.

-Costs of repairing systems or recovering lost data.

-Legal fees, regulatory fines, or penalties.

2. Indirect Costs

-Business disruption, downtime, and loss of productivity.

-Damage to reputation and loss of customer trust.

-Increased spending on cybersecurity measures to prevent future attacks.

3. Societal Costs

-Breaches of privacy and exposure of personal information.

-Emotional distress for victims.

-Economic impact on industries and economies due to reduced trust in digital systems

CHALLENGES TO THE DIGITALIZATION OF GOVERNMENT SERVICES

1. Increased Financial Burden on Governments

- Higher Security Investments: Governments must allocate substantial resources to strengthen their cybersecurity infrastructure to protect against growing threats. This includes spending on **advanced security tools**, hiring specialized **cybersecurity professionals**, conducting regular **vulnerability assessments**, and investing in **cyber defense technologies**. These increasing costs can divert funds away from other critical areas, such as healthcare, education, or strengthening ICT infrastructure, thus affecting overall public service delivery.

2. Erosion of Trust in Digital Systems

- Public Distrust: As the frequency and sophistication of cybercrimes increase, citizens may become more reluctant to use digital payment systems for government transactions. Public **trust** in the security of online payment platforms is essential for the success of **e-government initiatives**. If people fear that their **financial information** or **personal data** could be compromised, they might resist using digital systems, thereby slowing down the **adoption of e-payments**.

3. Strain on Operational Efficiency

- Disruptions in Service Delivery: As cybercriminals become more sophisticated, they are likely to target the **underlying payment infrastructure** of government systems. **Successful cyberattacks could disrupt essential services, such as salary disbursements, social security payments, or pension transfers, leading to delays, errors, and loss of funds**. These disruptions could create operational inefficiencies, affect public service continuity, and reduce the effectiveness of digital transformation initiatives.

4. Slowing Down of Technological Progress: Increased cybercrime risks may cause conservative stand in their adoption of new digital technologies. This could slow down the **digitalization process**, preventing the government from leveraging **technological advancements** that could improve efficiency, reduce costs, and foster economic growth.

SUMMARY OF CYBERSECURITY TRENDS IN THE PHILIPPINES (2023):

A. Cyberattacks:

- The Philippines experienced **76 million cyberattacks** last year.
- This marks a **20% decrease** from 2022 but remains a high and serious number.

B. Types of Threats:

- Attacks included **cyber espionage** and bypassing security in **Windows operating systems**.
- **Advanced Persistent Threats (APTs)**: These are long-term, stealthy attacks aimed at secretly accessing networks.

C. Main Attackers:

- Groups like **Earth Estries** and **Mustang Panda** targeted Philippine organizations.
- **Earth Estries** and Mustang Panda are Chinese APTs - https://business.inquirer.net/457808/cyberattacks-in-ph-down-20-in-2023

SUMMARY OF CYBERSECURITY TRENDS IN THE PHILIPPINES (2023):

A. **Cyberattacks**:

–The Philippines experienced **76 million cyberattacks** last year.

- This marks a **20% decrease** from 2022 but remains a high and serious number.

B. **Types of Threats**:

- Attacks included **cyber espionage** and bypassing security in **Windows operating systems**.

- Advanced Persistent Threats (APTs): These are long-term, stealthy attacks aimed at secretly accessing networks.

C. **Main Attackers**:

- Groups like **Earth Estries** and **Mustang Panda** targeted Philippine organizations.

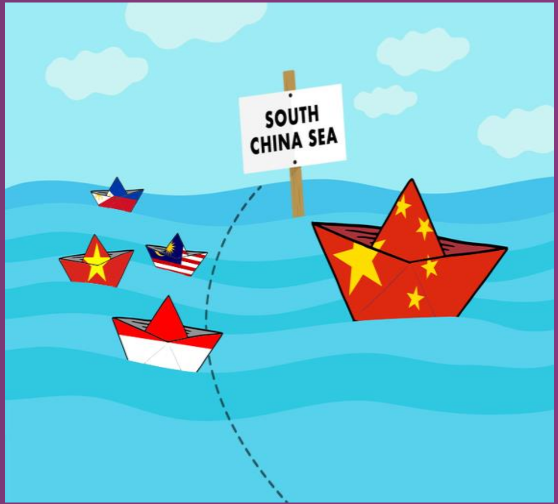
- Earth Estries and **Mustang Panda** are Chinese APTs - https://business.inquirer.net/457808/cyberattacks-in-ph-down-20-in-2023

SUMMARY OF CYBERSECURITY TRENDS IN THE PHILIPPINES (2023

The Philippines had the highest number of financial-related phishing attempts on business devices in 2023 in the Southeast Asian region with 163,279 incidents. Financial phishing refers to fraudulent resources related to banking, payment systems, and digital shops.
- *Kaspersky*

GEOPOLITICS AND CYBERATTACKS

Cyberattacks are a modern tool of statecraft, closely tied to geopolitics. They allow nations to compete, disrupt, or assert influence over rivals in ways that are less visible but highly impactful, making cyberspace a key battleground in global power struggles.



GEOPOLITICS AND CYBERATTACKS

1. Cyberattacks as a Tool of Power and Influence

- Nations leverage **cyber capabilities** to advance geopolitical agendas without engaging in open conflict.

- Cyberattacks can disrupt an opponent's critical infrastructure, economy, or communication systems, weakening their position without physical warfare.

2. Espionage and Intelligence Gathering

- Cyber operations are used to collect **sensitive information** about foreign governments, military plans, and industries.

- This data provides a strategic edge in negotiations, decision-making, or planning future actions.

3. Economic Warfare

- Cyberattacks can harm a nation's economy by targeting banks, stock markets, or major industries.

- This is often part of a broader geopolitical strategy to weaken an economic rival.

GEOPOLITICS AND CYBERATTACKS

5. Influence and Misinformation Campaigns

- Cyberattacks often include elements of **disinformation** or propaganda to influence public opinion and destabilize governments.
- These campaigns aim to sow division, manipulate elections, or shift political narratives in target countries

6. Critical Infrastructure Targeting

- Nations may target critical infrastructure (e.g., energy, transportation, healthcare) to cause chaos or weaken a rival's ability to function.
- Such attacks often occur during times of heightened geopolitical tension

7. Deterrence and Defense

- Cyberattacks can also serve as a show of force to deter adversaries, similar to military exercises.
- A nation might demonstrate its capabilities to signal strength and warn rivals against escalating tensions

GEOPOLITICS AND CYBERATTACKS

5. Influence and Misinformation Campaigns

- Cyberattacks often include elements of **disinformation** or propaganda to influence public opinion and destabilize governments.
- These campaigns aim to sow division, manipulate elections, or shift political narratives in target countries

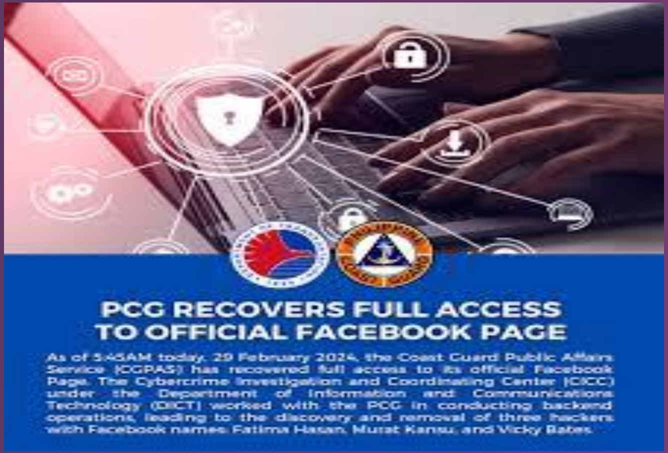
6. Critical Infrastructure Targeting

- Nations may target critical infrastructure (e.g., energy, transportation, healthcare) to cause chaos or weaken a rival's ability to function.
- Such attacks often occur during times of heightened geopolitical tension

7. Deterrence and Defense

- Cyberattacks can also serve as a show of force to deter adversaries, similar to military exercises.
- A nation might demonstrate its capabilities to signal strength and warn rivals against escalating tensions

CASES OF CYBERATTACKS IN THE PHILIPPINES

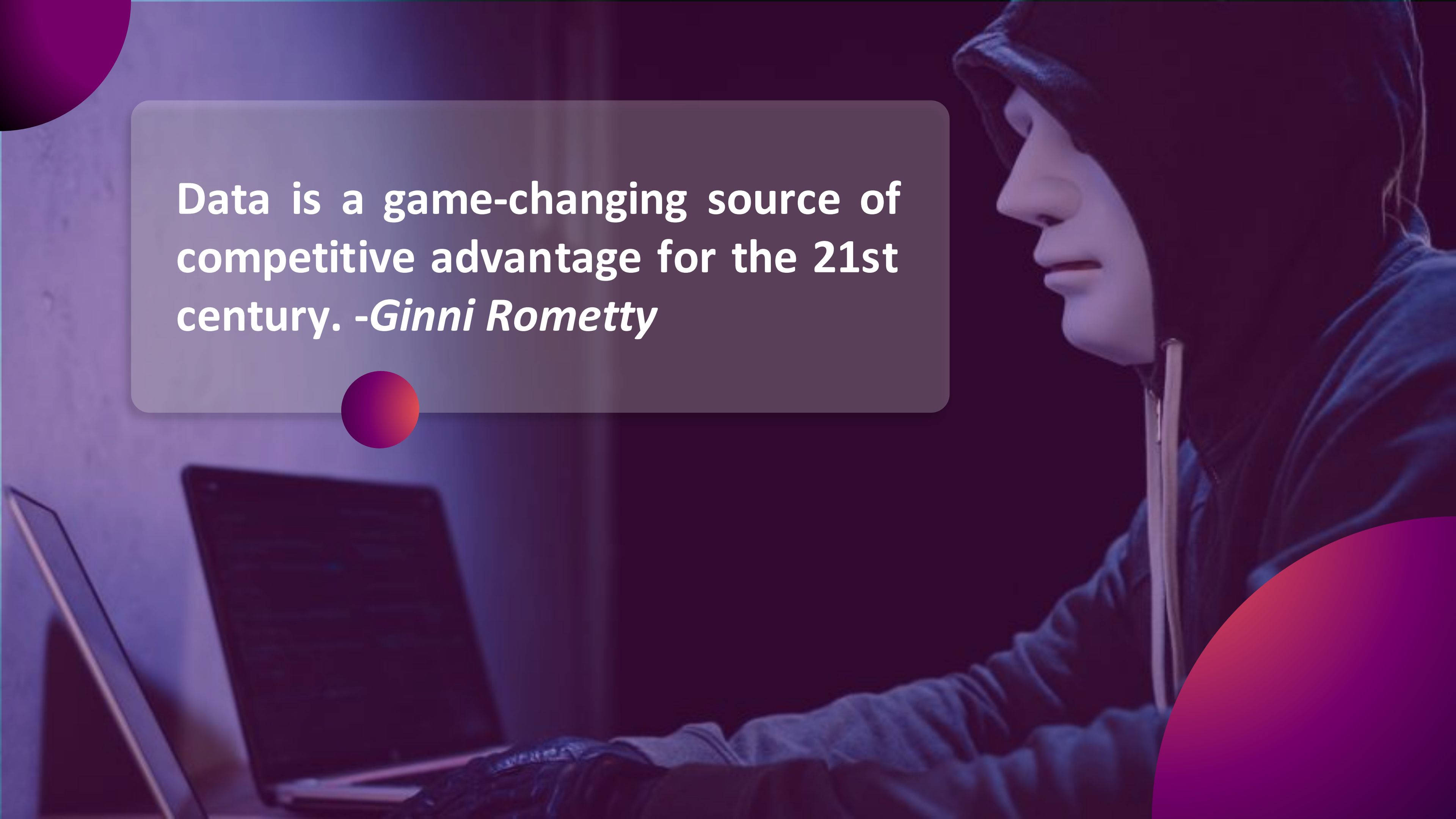


PCG RECOVERS FULL ACCESS TO OFFICIAL FACEBOOK PAGE

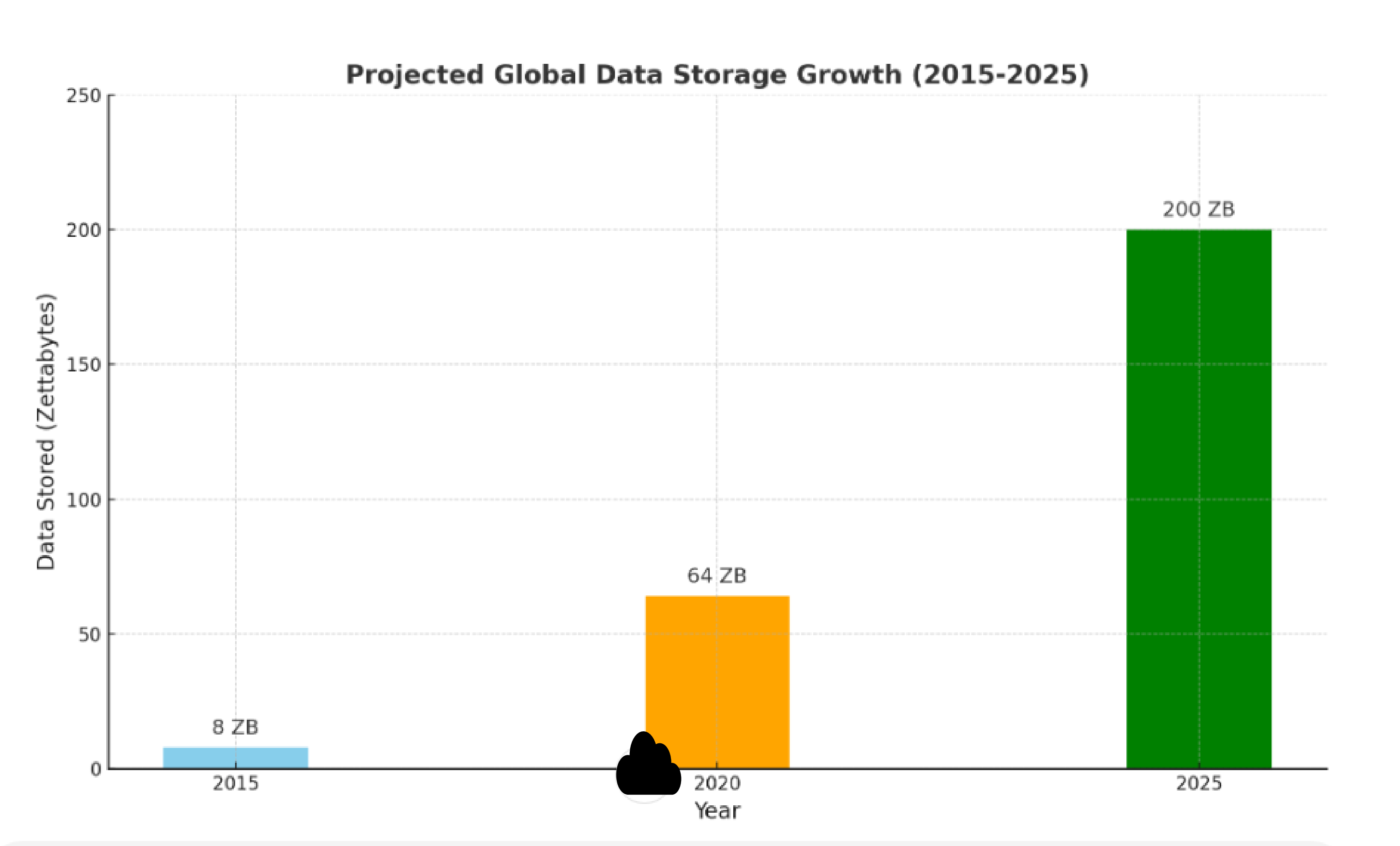
As of 5:45AM today, 29 February 2024, the Coast Guard Public Affairs Service (CGPAS) has recovered full access to its official Facebook Page. The Cybercrime Investigation and Coordinating Center (CICC) under the Department of Information and Communications Technology (DICT) worked with the PCG in conducting backend operations, leading to the discovery and removal of three hackers with Facebook names Fatima Hasan, Murat Kansu, and Vicky Babes.

Philippines Police Employee Records Leaked Online in a Massive Data Breach
vpnMentor

02
Economic Effects of Cybercrime

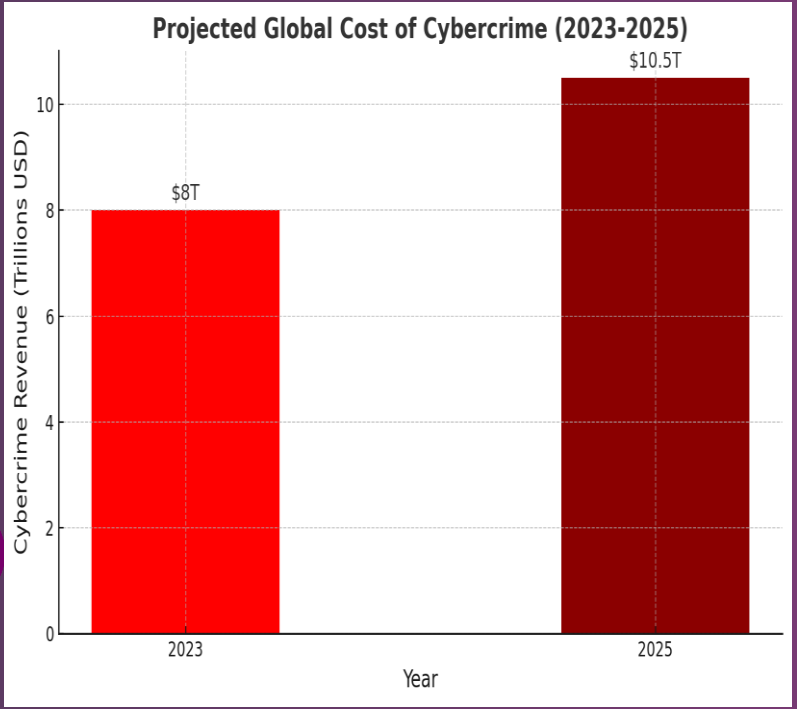


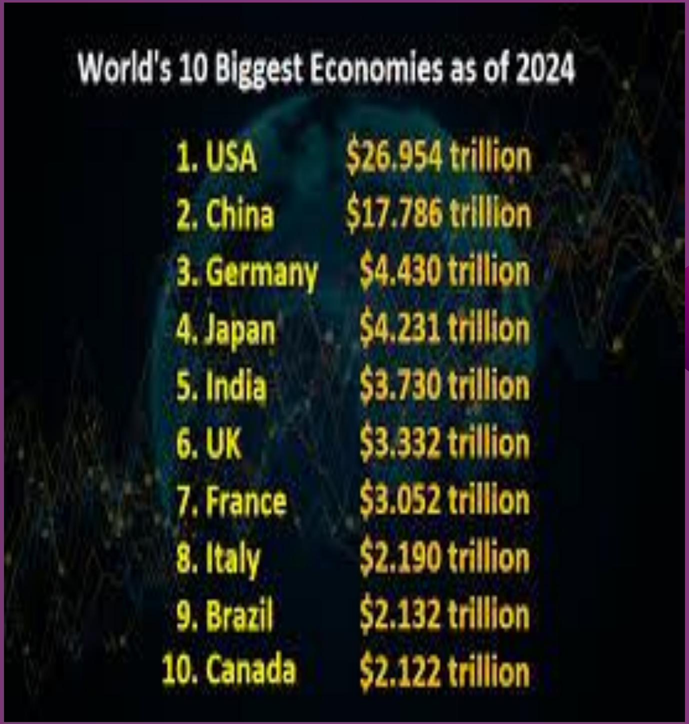
Data is a game-changing source of competitive advantage for the 21st century. *-Ginni Rometty*



Projected Global Data Storage Growth (2015-2025)

CYBERCRIME REVENUES VERSUS THE WORLD’S BIGGEST ECONOMIES

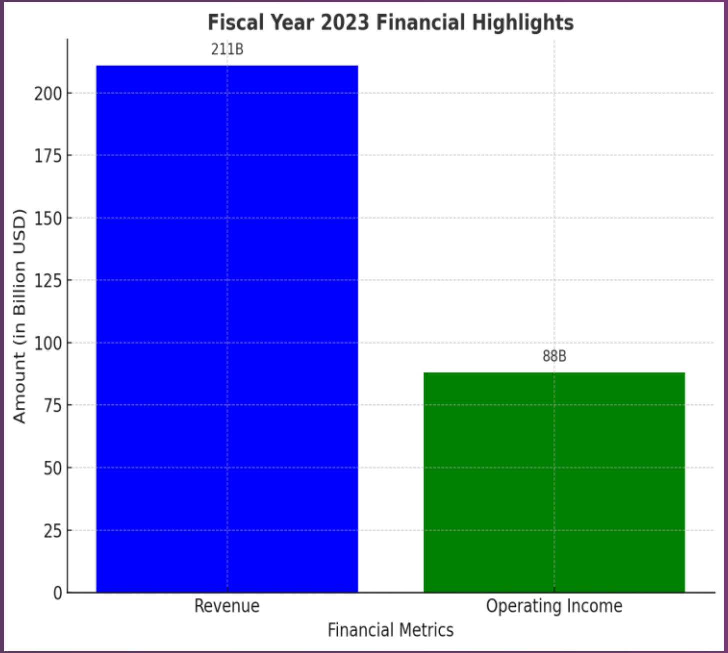


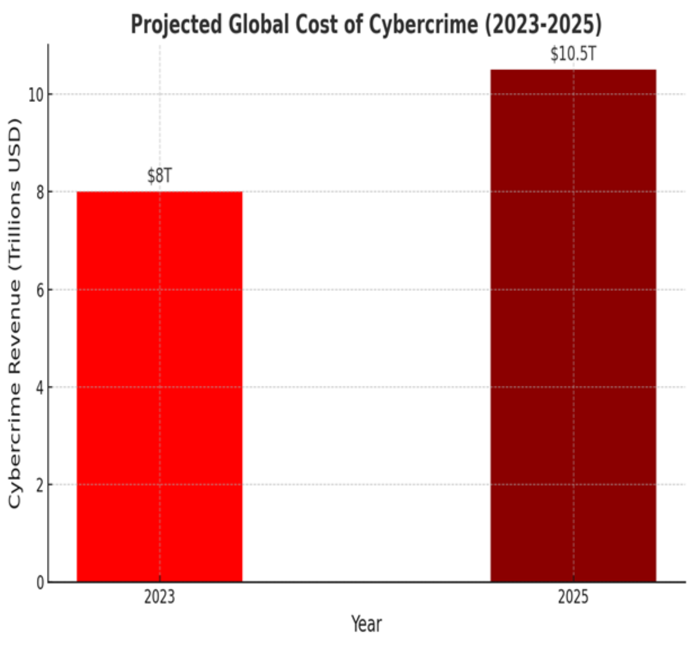


World's 10 Biggest Economies as of 2024

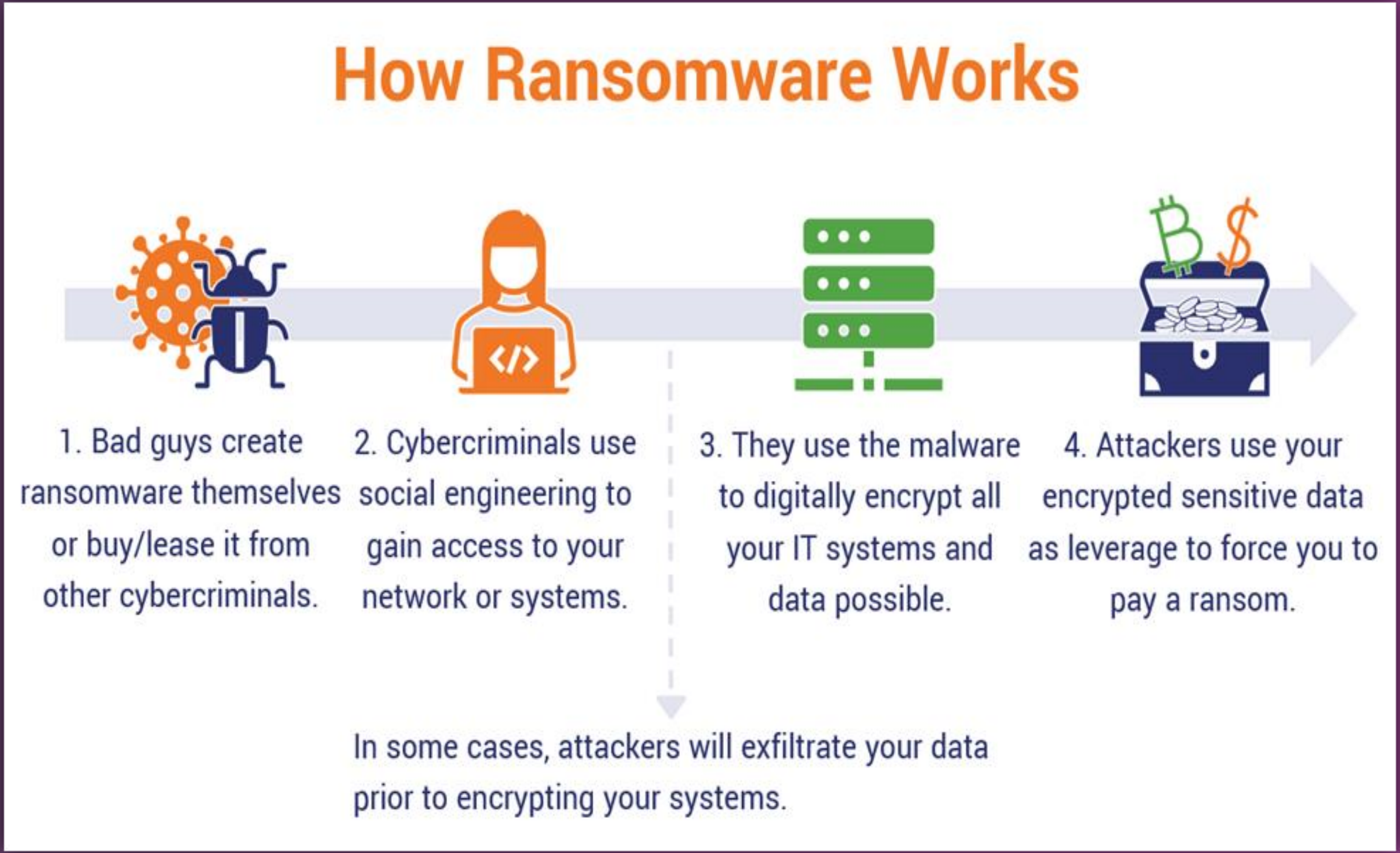
1. USA	$26.954 trillion
2. China	$17.786 trillion
3. Germany	$4.430 trillion
4. Japan	$4.231 trillion
5. India	$3.730 trillion
6. UK	$3.332 trillion
7. France	$3.052 trillion
8. Italy	$2.190 trillion
9. Brazil	$2.132 trillion
10. Canada	$2.122 trillion

MICROSOFT AND CYBERCRIME: REVENUE COMPARISON





RANSOMWARE



How Ransomware Works

1. Bad guys create ransomware themselves or buy/lease it from other cybercriminals.

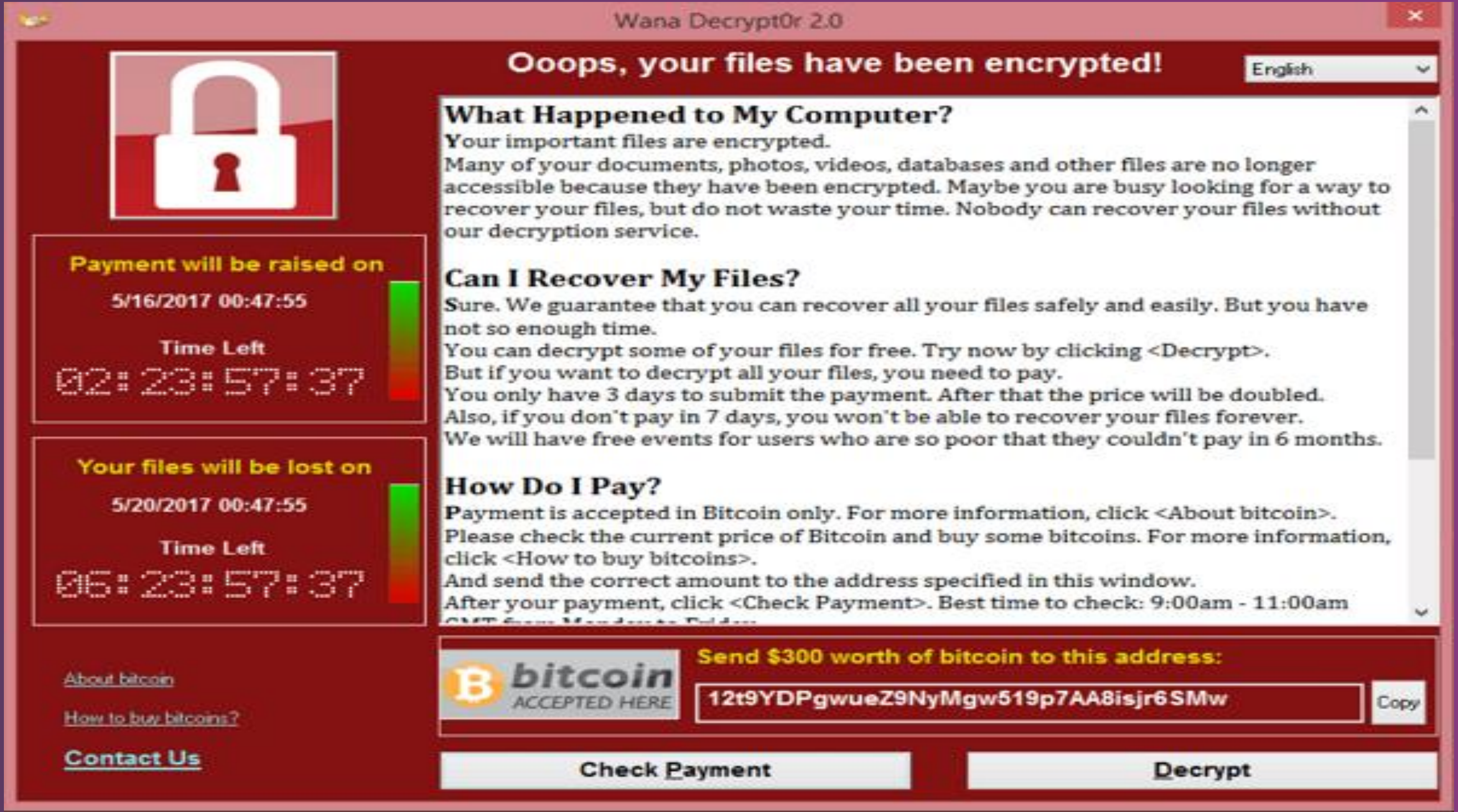
2. Cybercriminals use social engineering to gain access to your network or systems.

3. They use the malware to digitally encrypt all your IT systems and data possible.

4. Attackers use your encrypted sensitive data as leverage to force you to pay a ransom.

In some cases, attackers will exfiltrate your data prior to encrypting your systems.

RANSOMWARE ATTACKCASE EXAMPLE



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

WANNACRY RANSOMWARE ATTACK IN BRIEF DETAILS

Date of Attack	12 May 2017 – 15 May 2017 (initial outbreak)
Location	Worldwide
Approach	Ransomware encrypting files with US$300–600 demand (via bitcoin)
Outcome	More than 300,000 computers infected
Losses	More than US$4 billion
Responsible Group	Lazarus Group (North Korea)
Convicted	None

DATA BREACH

USD 4.88M:
The global average cost of a data breach in 2024—a 10% increase over last year and the highest total ever

KEY ASPECTS OF THE ECONOMIC IMPACT OF A DATA BREACH

Direct Costs:

- **Incident Response:** Costs associated with investigating the breach, containing the damage, and notifying affected individuals.

- **Legal Fees:** Costs related to legal compliance, lawsuits, and regulatory penalties.

- **Credit Monitoring:** Providing credit monitoring services to affected customers.

- **Data Recovery:** Costs to restore compromised data

- **Insurance Premiums:** Increased insurance premiums due to higher cybersecurity risk

Indirect Costs:

- **Reputational Damage:** Negative publicity and loss of customer trust due to the breach

- **Lost Business:** Customers choosing to do business elsewhere following a breach

- **Stock Price Decline:** A drop in company stock value upon news of a data breach

- **Employee Morale:** Decreased employee morale and productivity due to security concerns

- **Business Disruption:** Operational disruptions while addressing the breach

Capital One is a Fortune 500 financial services company that offers a variety of banking products and services to consumers, small businesses, and commercial clients.	
Services	Financial products and services, including credit cards, retail banking, and business banking
Customers	100 Million
Locations	USA, UK, Canada, and the Philippines
Headquarters	Virginia, USA

Date	July 19, 2019
Attack Vector	Misconfigured Web Application Firewall leading to an unauthorized access and privilege escalation
Data Exposed	Names, addresses, credit scores, bank account numbers, and social security numbers
Extent	100 Million customers in the US and 6 Million in Canada
Losses	190 Million settlement for affected customers 80 Million fine by the US govt.
Reputational Damage	The breach raised concerns about Capital One's security practices and their reliance on cloud infrastructure
Convicted	Paige Thompson

03

Technological and Infrastructural Challenges

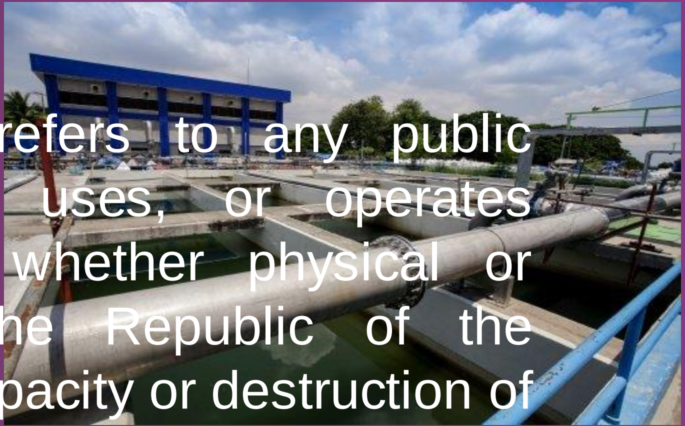
From bank accounts to financial systems, power grids to air traffic controls - our most critical infrastructure remain attractive cyber targets, and if they are ever compromised, the effects could be devastating.

- *Mike Quigley*

The physical structures, facilities, networks and other assets which provide services that are essential to the social and economic functioning of a community or society.

UNDRR

UN Office for Disaster Risk Reduction



Critical Infrastructure refers to any public service which owns, uses, or operates systems and assets, whether physical or virtual, so vital to the Republic of the Philippines that the incapacity or destruction of such systems or assets would have a detrimental impact on national security, including telecommunications and other such vital services as may be declared by the President of the Philippines. – *Section 2 (e) of RA 11659*

CYBERATTACK AGAINST CRITICAL INFRASTRUCTURE: IMPACT AGAINST GOVERNMENT OPERATIONS

1. Disruption of Essential Services

- **Energy Systems**: An attack on power grids can cause widespread blackouts, disrupting government buildings, hospitals, transportation, and communication systems. Without electricity, many government functions halt, delaying services and emergency response.
- **Telecommunications**: Targeting communication networks can sever connections between government agencies, hindering coordination, decision-making, and public communication during emergencies

2. Economic Disruptions

- **Financial Infrastructure**: Attacks on banking systems or financial networks can prevent government agencies from processing payments, collecting taxes, and funding operations.
- **Cost of Recovery**: Governments may need to divert resources toward recovery and strengthening cybersecurity, reducing funds available for public programs.

CYBERATTACK AGAINST CRITICAL INFRASTRUCTURE: IMPACT AGAINST GOVERNMENT OPERATIONS

3. Loss of Public Trust

- **Perception of Weakness**: Repeated cyberattacks on critical infrastructure may erode public trust in the government's ability to protect the nation, leading to discontent and political instability.
- **Spread of Fear**: High-profile attacks can create widespread fear, making citizens feel vulnerable and less secure in their everyday lives.

7. Operational Paralysis

- **Administrative Slowdown**: Attacks that lock or disrupt IT systems through malware or ransomware can bring entire government operations to a standstill, preventing access to important files and delaying decisions.
- **Overburdening Resources**: Responding to the crisis diverts personnel and resources from other essential services, slowing down overall government functioning.

UKRAINIAN POWER GRID ATTACK

Date	December 23, 2015
Target	PRYKARPATTYA OBLENERGO and other Ukrainian power companies
Attack Vector	PHISING
Method	The attackers used malware known as BLACKENERGY, alongside other techniques such as spear-phishing emails and remote access tools.
Initial Breach	The attackers gained access to the network through phishing emails containing malicious attachments.
System Compromise	They deployed BLACKENERGY malware to infiltrate the industrial control systems (ICS) responsible for managing the power grid
Impact	Approximately 230,000 residents experienced power outages lasting up to six hour
Coordinated Tactics	The attack included phone-based tactics, such as flooding customer service lines to delay response efforts.

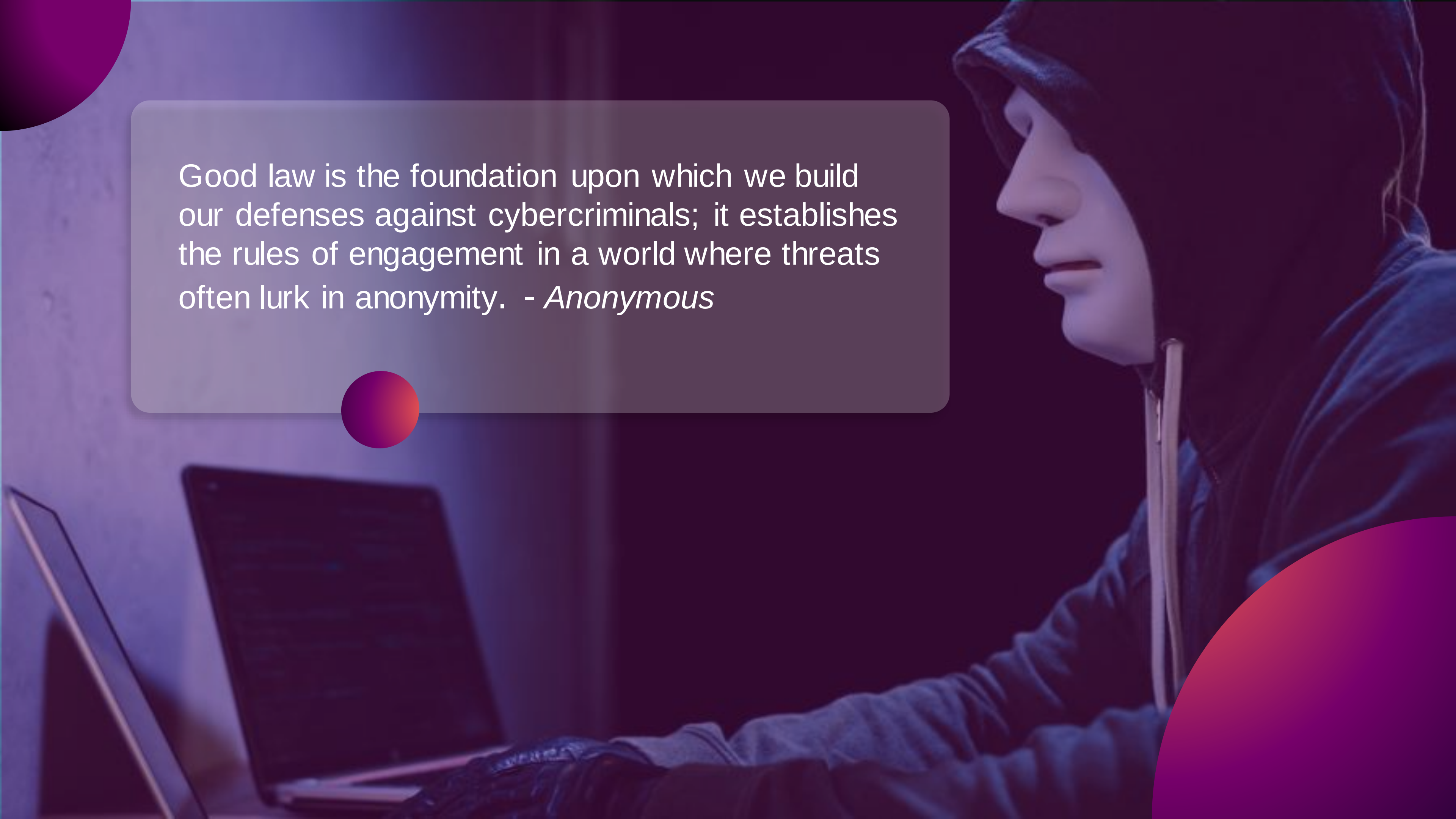
NATIONAL GRID CORPORATION OF THE PHILIPPINES

NGCP is a privately owned corporation in charge of operating, maintaining, and developing the country's state-owned power grid, an interconnected system that transmits gigawatts of power at thousands of volts from where it is made to where it is needed.

The company performs its mandate as transmission service provider with the full awareness of its nature as a public utility, and in full compliance with the rules and regulations of the regulator, and existing laws governing its transmission operation

05

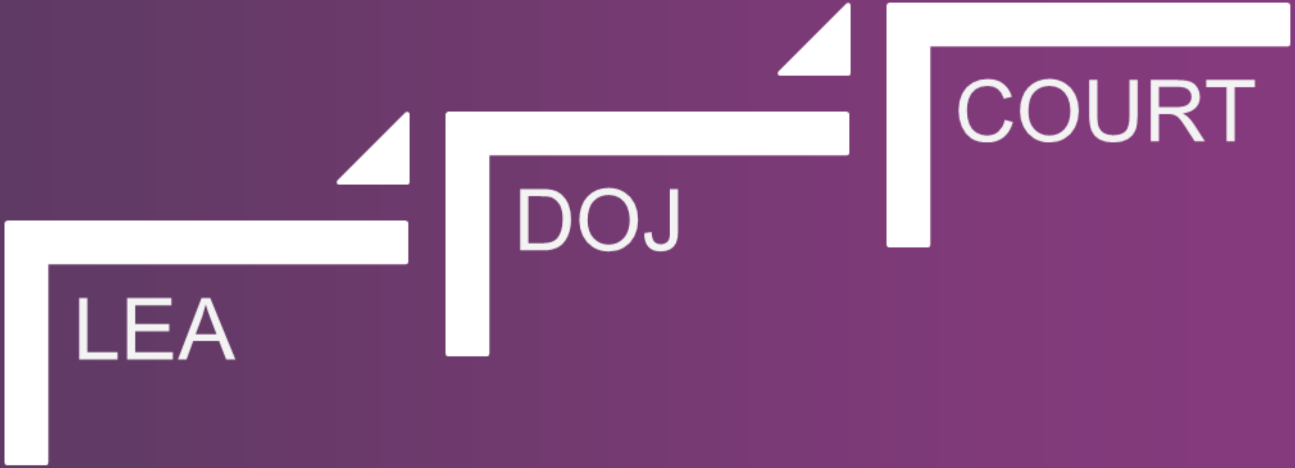
Legal and Policy Framework



Good law is the foundation upon which we build our defenses against cybercriminals; it establishes the rules of engagement in a world where threats often lurk in anonymity. - *Anonymous*

RELATED LAWS

- RA 10175 (Cybercrime Prevention Act of 2012);
- RA 10173 (Data Privacy Act of (2012);
- RA 11930 (Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act.
- RA 8792 (Electronic Commerce Act);
- RA 12010 (Anti-Financial Account Scamming Act);and
- Revised Penal Code, as amended

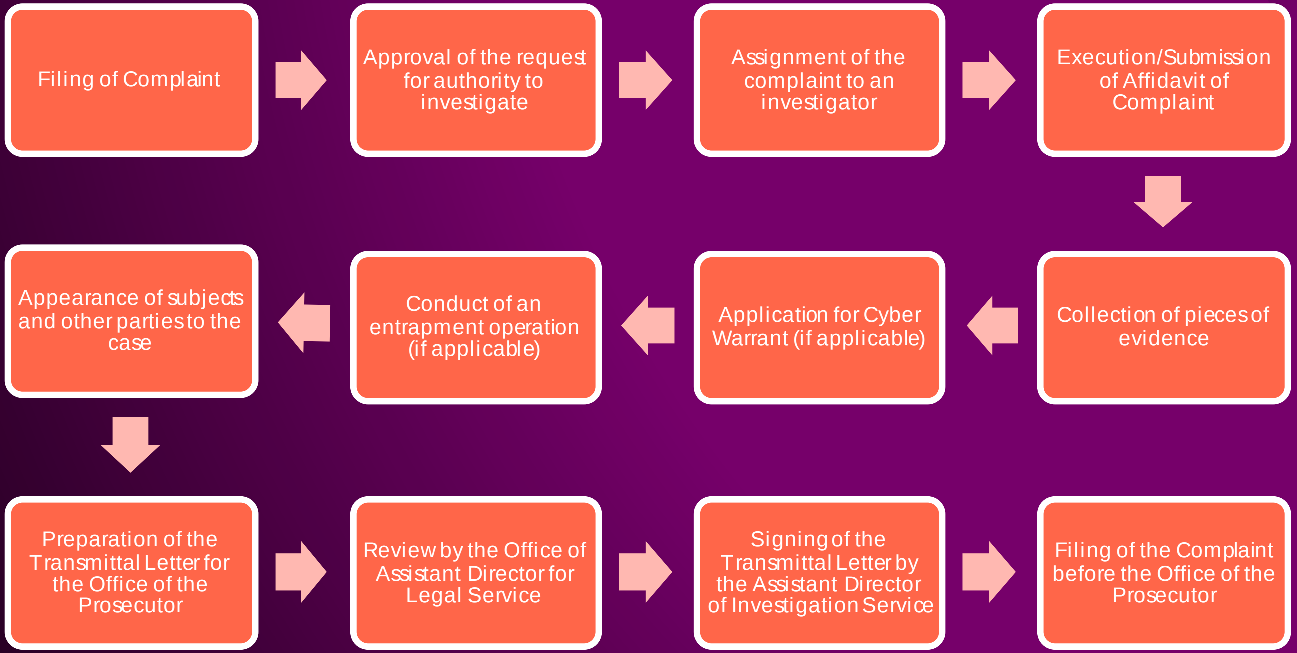


LEA

DOJ

COURT

PROCESS FLOW OF INVESTIGATION IN THE NBI



Filing of Complaint

Approval of the request for authority to investigate

Assignment of the complaint to an investigator

Execution/Submission of Affidavit of Complaint

Collection of pieces of evidence

Application for Cyber Warrant (if applicable)

Conduct of an entrapment operation (if applicable)

Appearance of subjects and other parties to the case

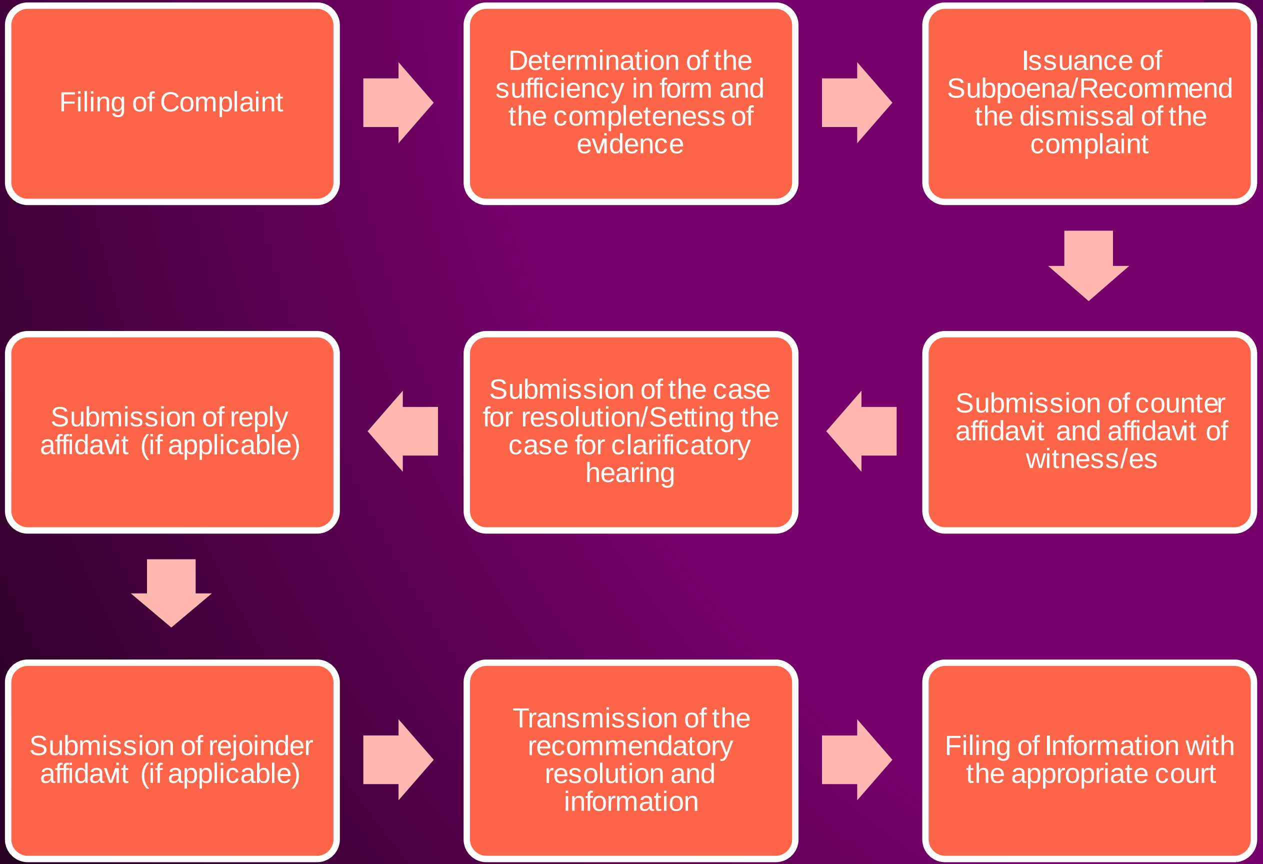
Preparation of the Transmittal Letter for the Office of the Prosecutor

Review by the Office of Assistant Director for Legal Service

Signing of the Transmittal Letter by the Assistant Director of Investigation Service

Filing of the Complaint before the Office of the Prosecutor

PROCESS FLOW OF PRELIMINARY INVESTIGATION



Filing of Complaint

Determination of the sufficiency in form and the completeness of evidence

Issuance of Subpoena/Recommend the dismissal of the complaint

Submission of counter affidavit and affidavit of witness/es

Submission of the case for resolution/Setting the case for clarificatory hearing

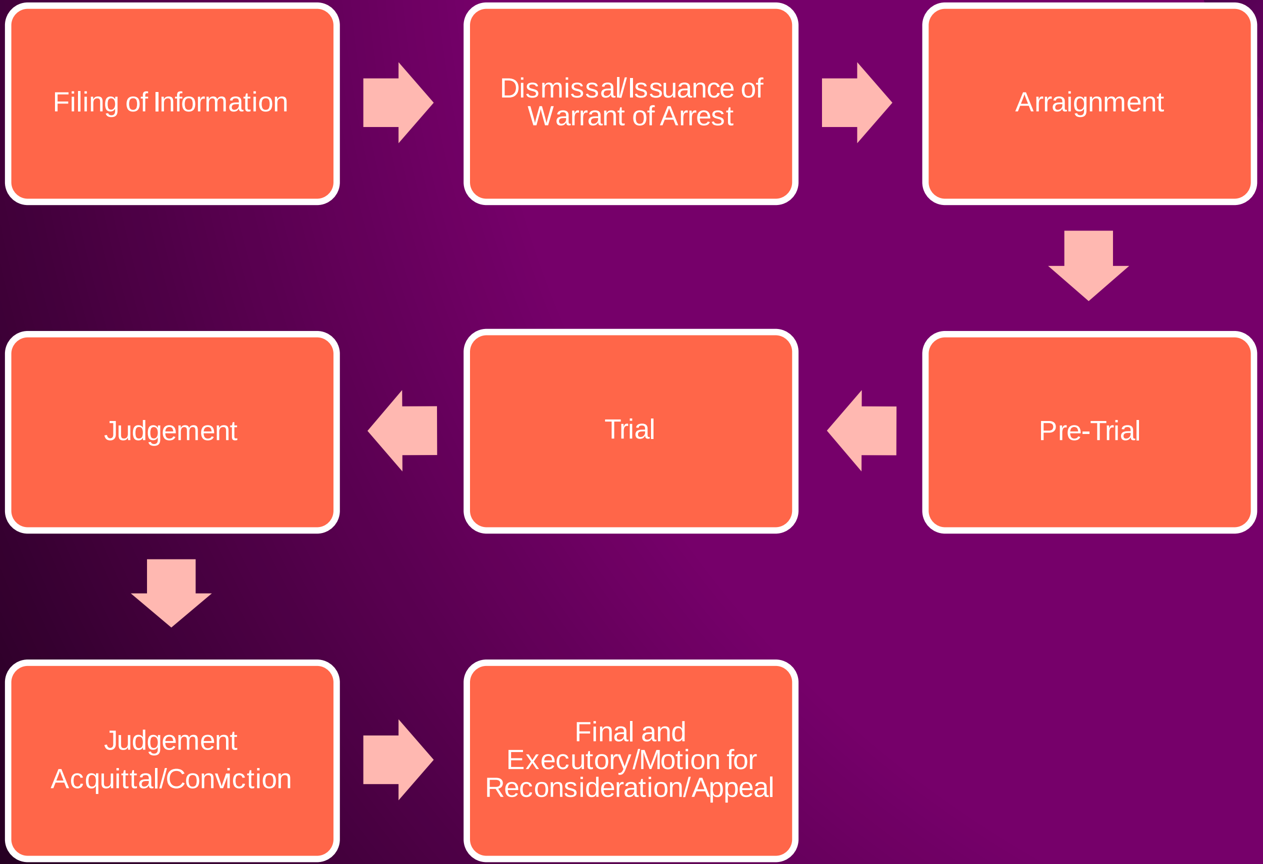
Submission of reply affidavit (if applicable)

Submission of rejoinder affidavit (if applicable)

Transmission of the recommendatory resolution and information

Filing of Information with the appropriate court

PROCESS FLOW IN THE FIRST LEVEL COURT



Filing of Information

Dismissal/Issuance of Warrant of Arrest

Arraignment

Pre-Trial

Trial

Judgement

Judgement Acquittal/Conviction

Final and Executory/Motion for Reconsideration/Appeal

05

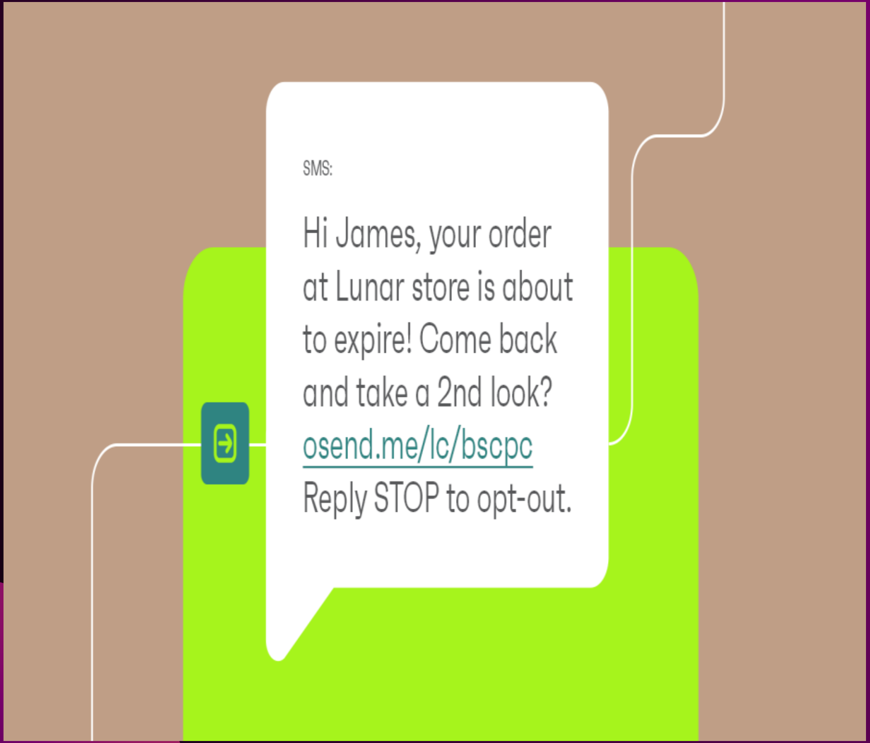
PREVENTION AND MITIGATION

Guarding your digital life on social media is crucial to protecting your personal information, privacy, and security from cyber threats, including hacking, identity theft, and online scams. - *Anonymous*

CYBER BEST PRACTICES

Cyber hygiene refers to the set of best practices, routines, and measures individuals and organizations follow to maintain the health and security of their digital devices, networks, and data.

UNSOLICITED OFFERS AND MESSAGES



SMS:

Hi James, your order at Lunar store is about to expire! Come back and take a 2nd look? osend.me/lc/bscpc Reply STOP to opt-out.

Unsolicited offers frequently contain phishing links, designed to trick you into providing personal information like login credentials, credit card details, or other sensitive data. Clicking on these links can lead you to fraudulent websites that mimic legitimate ones, making it easier for attackers to steal your information.

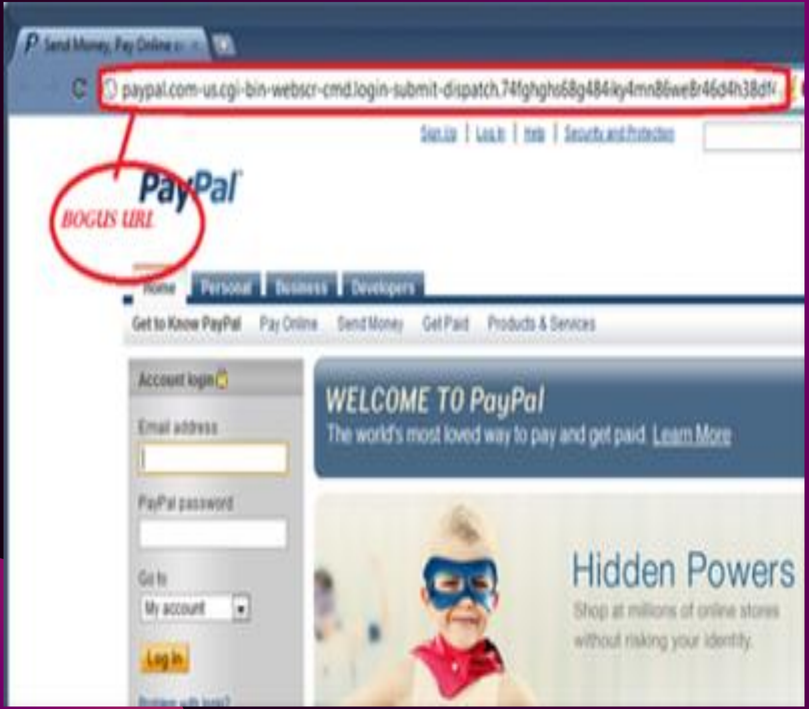
UNSOLICITED OFFERS AND MESSAGES

DATA HARVESTING

MALWARE DISTRIBUTION

ACCOUNT TAKE OVER

FAKE WEBSITES AND PAYMENT SYSTEMS



paypal.com-us.cgi-bin-webscr-cmd.login-submit-dispatch.74fghghs68g484ky4mn86we8r46d4h38df\

WELCOME TO PayPal

The world's most loved way to pay and get paid. Learn More

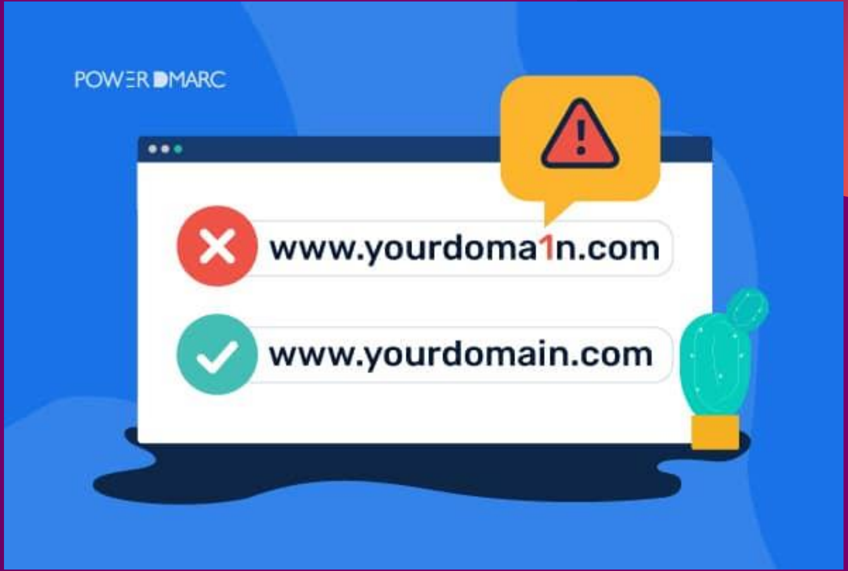
Hidden Powers

Shop at millions of online stores without risking your identity.

Identifying a fake payment system on a website is crucial to protect your financial information from fraud or theft. Cybercriminals create fake payment gateways or clone legitimate sites to steal credit card details or personal information.

URL ANOMALIES

Fake websites often use URLs that look very similar to the legitimate ones, but may have slight differences, such as misspellings (e.g., "faceboook.com" instead of "facebook.com") or unusual domain extensions (e.g., ".xyz" instead of ".com").

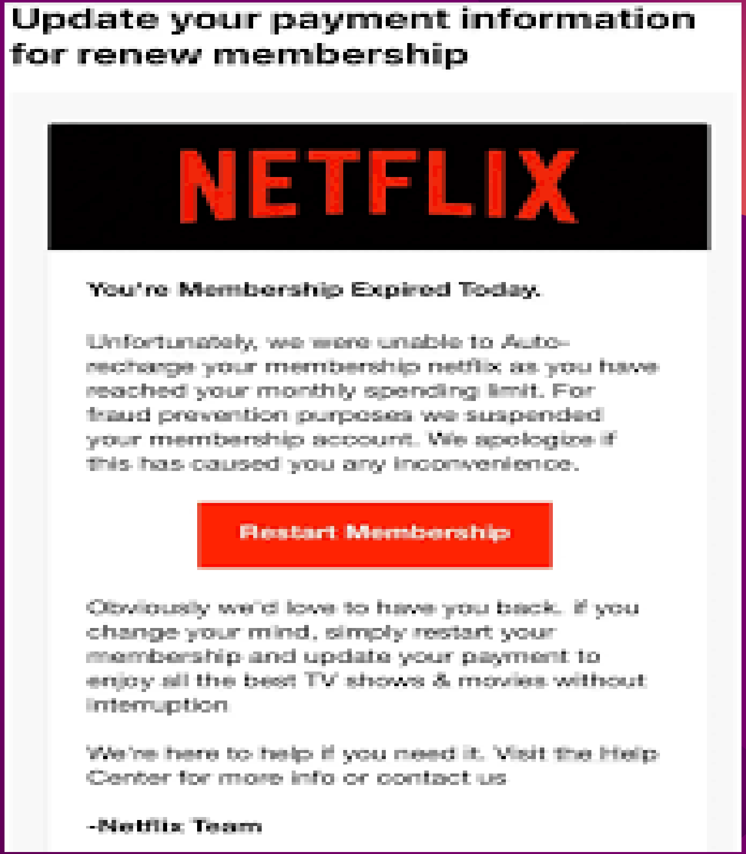


URL ANOMALIES

LACK OF SECURE HTTPS: Although attackers can sometimes fake HTTPS, many fake websites still use "http://" instead of "https://." Always ensure you're on a secure connection.

SUSPICIOUS REQUEST FOR ACCOUNT UPDATE

A suspicious request for an update on a website could be an attempt to trick users into downloading malware or providing sensitive information. These requests are often seen in the form of pop-ups, fake alerts, or phishing emails that claim a software or security update is required.



Update your payment information for renew membership

You're Membership Expired Today.

Unfortunately, we were unable to Auto-recharge your membership netflix as you have reached your monthly spending limit. For fraud prevention purposes we suspended your membership account. We apologize if this has caused you any inconvenience.

Obviously we'd love to have you back. if you change your mind, simply restart your membership and update your payment to enjoy all the best TV shows & movies without interruption

We're here to help if you need it. Visit the Help Center for more info or contact us

-Netflix Team

RISKS OF USING PUBLIC WIFI

Public Wi-Fi networks, such as those found in cafes, airports, and hotels, are convenient but carry significant risks. Because these networks are open and often unencrypted, they can expose users to various cybersecurity threats.

HOW TO PROTECT YOURSELF ON PUBLIC WI-FI:

□ USE A VIRTUAL PRIVATE NETWORK (VPN): A VPN encrypts your internet traffic, making it difficult for hackers to intercept your data, even on unsecured networks.

□ AVOID SENSITIVE ACTIVITIES: Avoid online banking, shopping, or accessing sensitive accounts when connected to public Wi-Fi.

□ VERIFY THE NETWORK: Always confirm that you're connecting to the legitimate public Wi-Fi network and not a fake hotspot.

□ ENABLE HTTPS: Ensure that websites you visit use HTTPS by checking for the padlock icon in the browser's address bar.

□ TURN OFF SHARING: Disable file sharing, printer sharing, and AirDrop while on public Wi-Fi to reduce your exposure to attacks.

□ USE TWO-FACTOR AUTHENTICATION (2FA): Add an extra layer of security to your accounts by enabling 2FA, which requires more than just a password to log in.

□ KEEP SOFTWARE UPDATED: Ensure your operating system, apps, and security software are up to date to protect against vulnerabilities that attackers could exploit.

EXERCISE CAUTION WITH THESE::

- **Requests for Personal Information**: You are asked to provide personal or account details directly via email, an unsecured webpage, or text message;

- **Threats of Account Suspension**: You receive a warning that your access will be closed or suspended unless you take immediate action;

- **Survey Invitations**: You are invited to complete a survey that requires you to input personal or account information;

- **Account Compromise Notifications**: You are informed that your account may have been compromised or that there has been unauthorized activity, and you are then asked to provide or verify your personal or account information;

- **Requests for Computer Access**: Another user asked to log in using your computer; and

- **Account Confirmation Requests**: You are asked to confirm, verify, or update your account, password, email, or other personal information.

REFRAIN FROM DOING THESE

- ❑ **AVOID OPENING SUSPICIOUS EMAILS OR CLICK SUSPICIOUS LINKS**: Do not open emails, click on links, or download attachments from unfamiliar sources;

- ❑ **DO NOT SHARE SENSITIVE INFORMATION**: Never disclose your user ID, password, secure token device, or answers to security questions to anyone;

- ❑ **SECURE YOUR LOGIN CREDENTIALS**: Refrain from leaving written notes with your login details near your computer or in easily accessible places where others can see them;

- ❑ **DEACTIVATE INACTIVE USER PROFILES**: Do not leave unused user profiles active online; and

- ❑ **KEEP DEVICES SECURE**: Ensure that your computer, mobile devices, and other digital media are not left in unsecured locations, such as inside your car.

BE MINDFUL OF DOING THESE::

❑ Pay special attention to links and attachments;

❑ Change your passwords often, choosing passwords that are hard for others to guess;

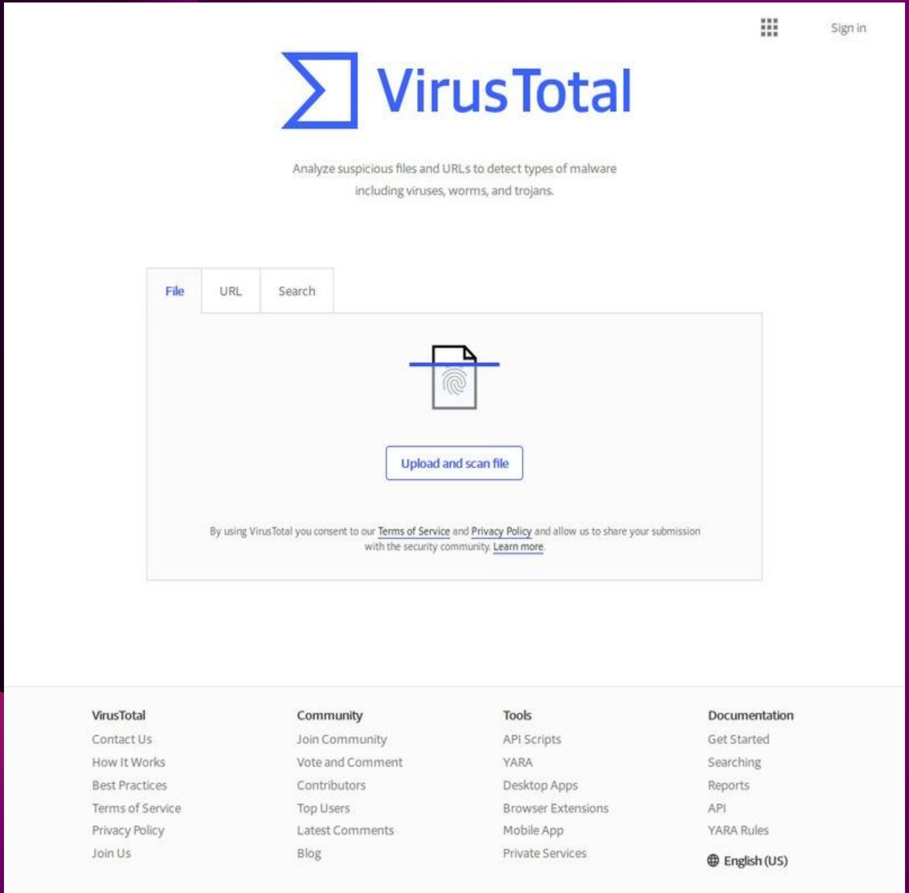
❑ Use different passwords for different accounts;

❑ Always log off at the end of a session;

❑ Use only software that is tested safe;

❑ Install and keep a strong firewall; and

❑ Keep anti-virus software up to date and use current versions of web browsers.



Sign in

VirusTotal

Analyze suspicious files and URLs to detect types of malware including viruses, worms, and trojans.

File | URL | Search

Upload and scan file

By using VirusTotal you consent to our Terms of Service and Privacy Policy and allow us to share your submission with the security community. Learn more

VirusTotal
Contact Us
How It Works
Best Practices
Terms of Service
Privacy Policy
Join Us

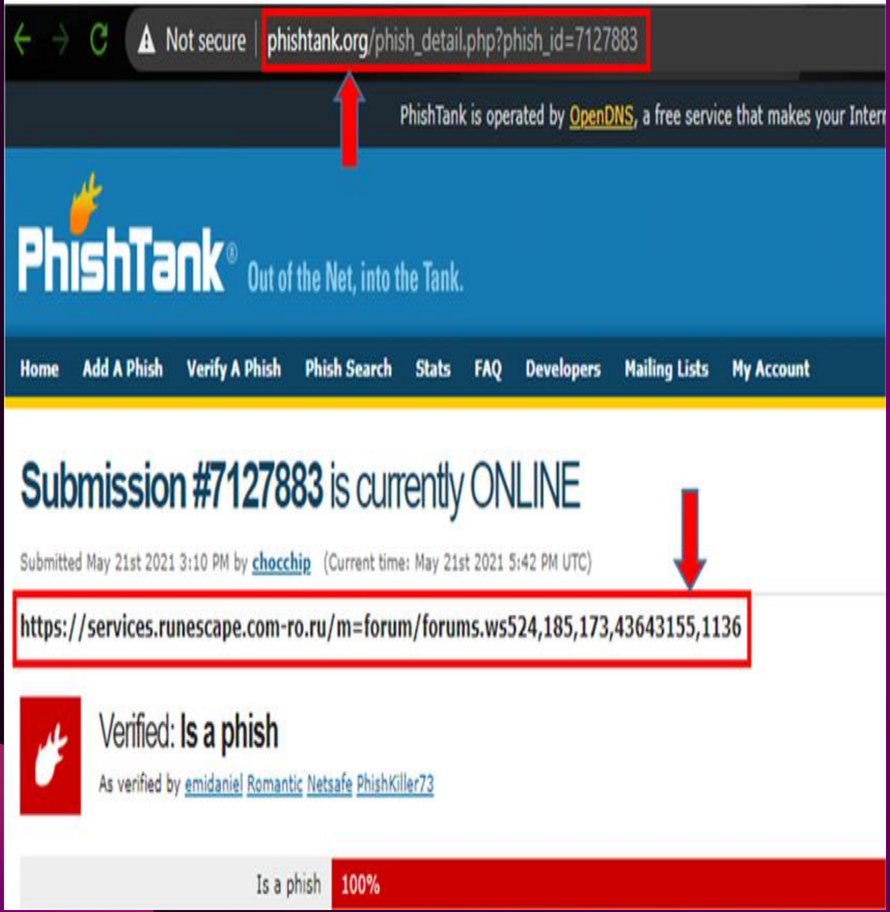
Community
Join Community
Vote and Comment
Contributors
Top Users
Latest Comments
Blog

Tools
API Scripts
YARA
Desktop Apps
Browser Extensions
Mobile App
Private Services

Documentation
Get Started
Searching
Reports
API
YARA Rules

English (US)

VirusTotal is a widely used online service that analyzes files and URLs to detect malware and other security threats. It aggregates results from multiple antivirus engines and website scanners to provide a comprehensive assessment of the safety and reputation of a file or URL.



PhishTank is operated by OpenDNS, a free service that makes your Inter

PhishTank® Out of the Net, into the Tank.

Submission #7127883 is currently ONLINE

Submitted May 21st 2021 3:10 PM by chocchip (Current time: May 21st 2021 5:42 PM UTC)

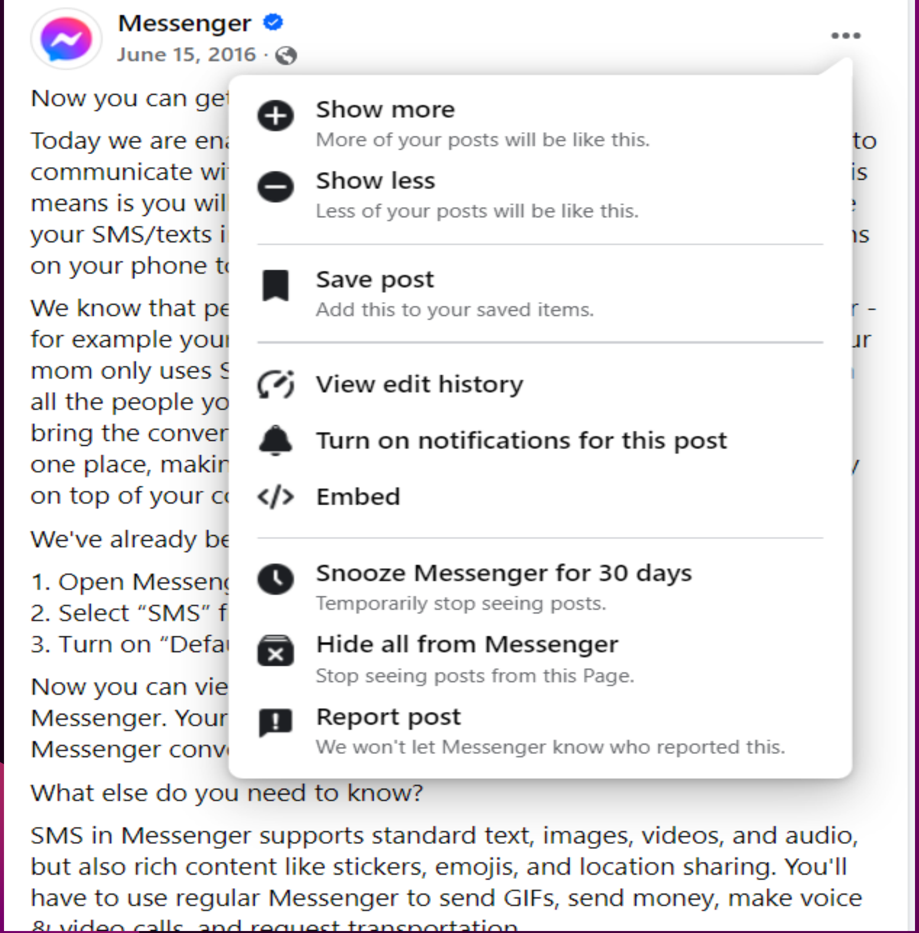
https://services.runescape.com-ro.ru/m=forum/forums.ws524,185,173,43643155,1136

Verified: Is a phish

As verified by emidaniel Romantic Netsafe PhishKiller73

Is a phish 100%

PhishTank is a community-driven platform that focuses on identifying and reporting phishing attempts. It serves as a resource for users and organizations to check URLs for potential phishing scams, helping to enhance online safety.



Messenger

June 15, 2016 ·

Now you can get

Today we are ena to
communicate wi is
means is you wil
your SMS/texts i ns
on your phone t

We know that pe r -
for example your ur
mom only uses S
all the people yo
bring the conver
one place, makin
on top of your c

We've already be

1. Open Messeng
2. Select "SMS" f
3. Turn on "Defa

Now you can vie
Messenger. Your
Messenger conv

What else do you need to know?

SMS in Messenger supports standard text, images, videos, and audio, but also rich content like stickers, emojis, and location sharing. You'll have to use regular Messenger to send GIFs, send money, make voice & video calls, and request transportation

Show more
More of your posts will be like this.

Show less
Less of your posts will be like this.

Save post
Add this to your saved items.

View edit history

Turn on notifications for this post

Embed

Snooze Messenger for 30 days
Temporarily stop seeing posts.

Hide all from Messenger
Stop seeing posts from this Page.

Report post
We won't let Messenger know who reported this.

REPORTING A SUSPICIOUS MESSAGE IN FB

If you believe your Facebook account has been compromised, it’s crucial to avoid logging into suspicious or third-party websites that claim to offer help. Many of these sites could be phishing attempts designed to steal your information.

SECURE HELPFUL INFORMATION WITHIN THE PLATFORM.

RECOVERING A COMPROMISED SOCIAL MEDIA ACCOUNT

- ❑ **CHANGE YOUR PASSWORD:**
  - ❑ Immediately change your password to a strong, unique one that you haven't used before.
  - ❑ Use a combination of letters, numbers, and special characters.
- ❑ **ENABLE MFA/2FA:**
  - ❑ Activate MFA2FA to add an extra layer of security, requiring a second form of verification (like a code sent to your phone) when logging in.
- ❑ **REVIEW ACCOUNT ACTIVITY:**
  - ❑ Check your account activity for any unauthorized posts, messages, or changes.
  - ❑ Report any suspicious activity to the platform.
- ❑ **REMOVE UNAUTHORIZED ACCESS:**
  - ❑ Review and remove any unfamiliar devices or sessions that have access to your account.
- ❑ **NOTIFY FRIENDS AND FOLLOWERS:**
  - ❑ Inform your contacts that your account was compromised, so they can be cautious of any suspicious messages that may come from your account

RECOVERING A COMPROMISED DEVICE

RUN A SECURITY SCAN:
Use reputable antivirus or anti-malware software to scan your device for threats and remove any detected malware.

UPDATE YOUR SOFTWARE:
Ensure that your operating system and all applications are up to date to protect against vulnerabilities.

RESET YOUR DEVICE:
If the device continues to behave unusually, consider performing a factory reset. Ensure you back up important data first.

CHANGE PASSWORDS:
Change passwords for accounts accessed on the compromised device, especially sensitive accounts like banking.

RECOVERING A COMPROMISED EMAIL ACCOUNT

CHANGE YOUR PASSWORD:
Change your email password immediately, using a strong and unique password.

ENABLE TWO-FACTOR AUTHENTICATION (2FA):
Activate 2FA on your email account to enhance security.

CHECK ACCOUNT RECOVERY SETTINGS:
Review and update your recovery email and phone number to ensure they are correct and secure.

REVIEW SENT AND INBOX FOLDERS:
Check for any unauthorized emails sent from your account and inform recipients if necessary.

SCAN FOR MALWARE:
Run a full scan on your device to ensure it is not infected with malware that could compromise your email again

CORE MESSAGE

Understanding **"Cybercrime and its Effect on Society"** is crucial in public financial management as it highlights the risks cyberattacks pose to government funds, digital payment platforms, and revenue systems. **Cybercrime not only threatens financial integrity but also undermines public trust in government operations, disrupts essential services, and creates broader societal impacts like privacy breaches and psychological stress.** By addressing these vulnerabilities, policymakers and financial managers can develop robust systems, ensure operational continuity, and align with digital transformation goals to safeguard public resources and maintain societal confidence.

Thank You

Thanks!

Do you have any questions?
youremail@freepik.com
+91 620 421 838
yourcompany.com

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon** and infographics & images by **Freepik**

Please keep this slide for attribution