

# Computer Security Awareness

Protecting PNP Computer Systems and Data Against

**“Ransomware”**

**Prepared by:**

Web Service and Cyber Security Division  
Information Technology Management Service  
Philippine National Police



# Related Terminologies

- **Malware** – software programs designed to alter, damage, steal or conduct unauthorized actions on a computer system and data.
- **Bitcoin** – a form of digital currency, created and held electronically used to buy things electronically.
- **Trojan** – a form of malware that pretends to be a legitimate software or file but deploys a host of malware to the infected computer system.



# Related Terminologies

- **Phishing** – is the attempt to obtain sensitive information, by pretending to be a legitimate source, usually through email or fake/illegal websites.
- **Drive-by downloading** – the unintentional downloading and installation of malware such as RANSOMWARE by visiting illegal websites or opening email links or attachments from unknown senders .



# Related Terminologies

- **Malicious email** – a suspicious email received from an unknown sender containing links or attachments.
- **Software** – a program or a set of instructions and applications used to manage and control various functions of a device such as a computer

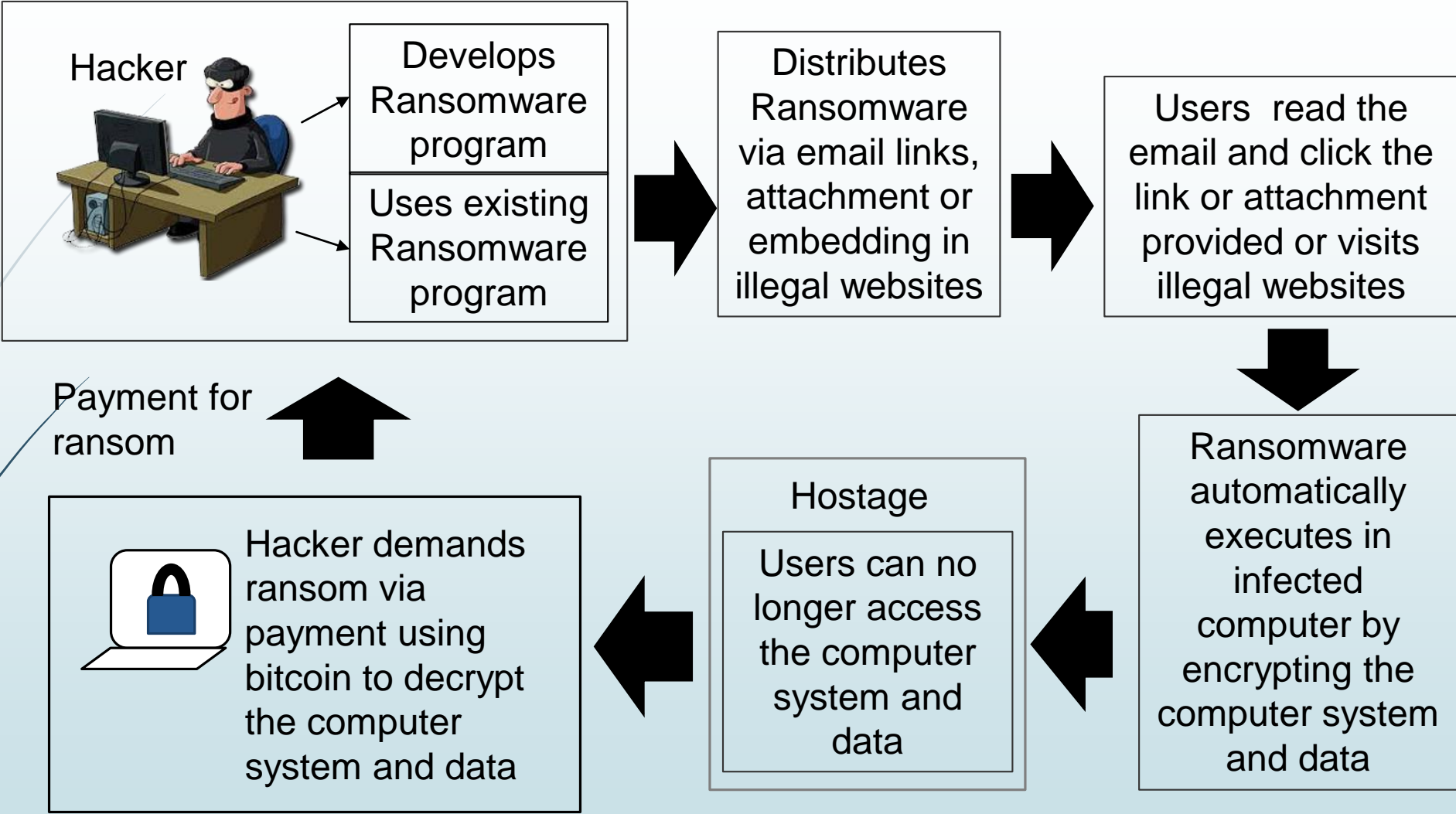


# What is Ransomware?

- A type of malware that infects computer systems and data rendering them unusable for “ransom”.
- Holds computer files for "ransom" by encrypting or preventing access to operating system such as Windows.
- Spreads through phishing emails or drive-by downloading websites; and
- Uses a Trojan, disguised as a legitimate file or software that automatically installs on the infected computer system.



# How Ransomware works:



**NOTE:** Payment of ransom is no guarantee that hacker will send a decryption key to unlock the infected computer system and data.



# Two (2) Kinds of Ransomware

- **Locker ransomware** – locks the operating system, making it impossible to access the computer and/or any software or files and demands payment in order to unlock the computer system and data.
- **Crypto ransomware** – designed to encrypt and block system files and demands payment in order to decrypt the computer system and data using a screen message.





# Top 10 Ransomwares

(as of December 18, 2016)

1. Locky > Crypto  
- Dharma
2. Teslacrypt > Crypto
3. Hddcryptor > Crypto
4. Crylocker > Locker
5. Cerber > Crypto
6. Petya and Mischa > Crypto
7. Chimera > Crypto
8. Jigsaw > Crypto
9. Samsam > Crypto
10. Cryptowall > Crypto

Source: <https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/top-10-ransomware-strains-2016/>



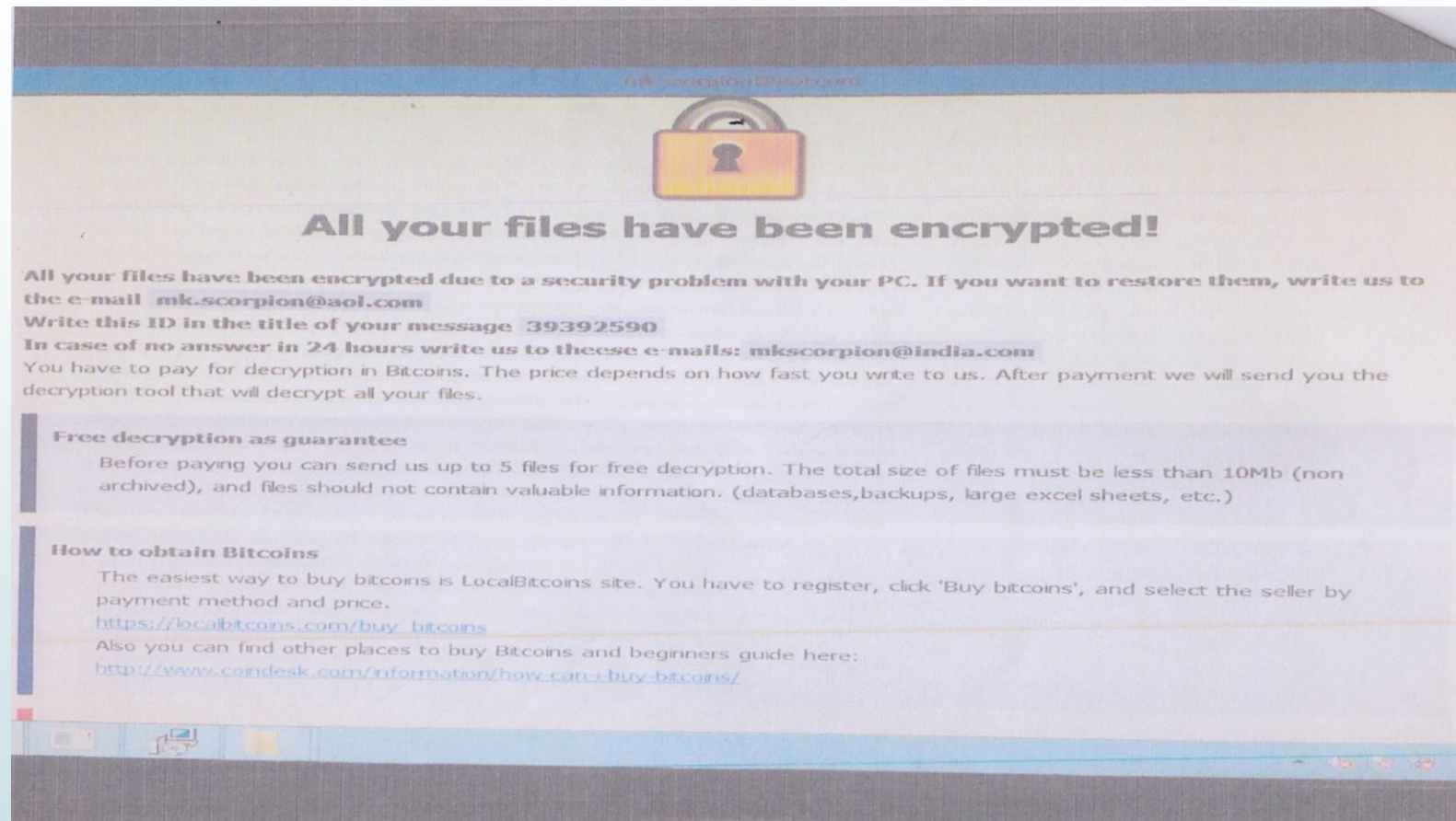


# Modus Operandi on Ransomware Propagation

- Via email pretending to be from a legitimate source and ask the reader to click the link or download the attachment provided.
- Ransomware links are also provided in social media messages from unknown sources.
- Using hidden links in illegal websites and online games.



# A sample screenshot of a ransomware



Warning pop up on the screen with instructions on how to pay for the decryption key.



# Security Risks to PNP Computer Systems and Data

- Data can be altered, damaged, deleted, and infused with additional computer viruses.
- Interfere with the normal functioning of the computer system or prevent its utilization.



# Offense Committed Using Ransomware

**Under R.A. 10175 “Cybercrime Prevention Act of 2012”**

- **Data Interference** – the intentional alteration, damaging, deletion of data and transmission of viruses.
- **System Interference** – the intentional inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, and transmission of viruses.



# Mitigation Measures

- Back up and test your data regularly.
- Avoid opening e-mails from unverified or questionable sources.
- Avoid illegal websites or torrent sites.
- Use genuine software and patch/update.
- Scan your computer regularly using antivirus software.



# Mitigation Measures (continued)

If infected:

- Disconnect system from network immediately to avoid infecting other computers connected.
- Use Ransomware decryptors for many types of Ransomware.
- Restore latest backup of computer system and data.
- Contact ITMS WSCSD for technical support assistance.

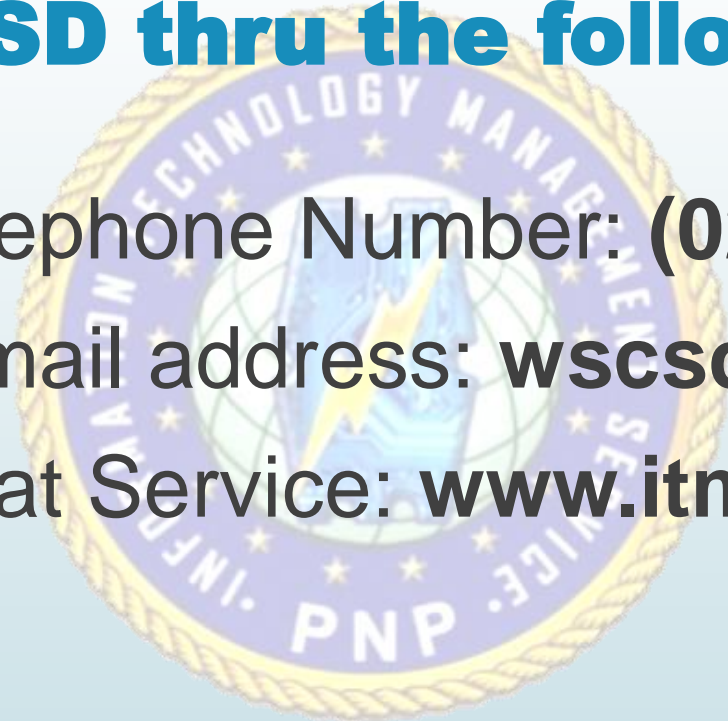
Warning: Once infected by ransomware there is a high risk that the computer system cannot be restored to its working condition or recover the infected files.





# For further inquiries, you may contact ITMS WSCSD thru the following:

- Telephone Number: **(02) 7230401 local 4225;**
- E-mail address: **wscsditms@pnp.gov.ph;** and
- Chat Service: **www.itms.pnp.gov.ph**



and CYBER SECURITY DIVISION





**THANK YOU**

