CYBERCRIMES

Criminals constantly exploiting Internet's global reach and its technological growth to develop new types of crime and at the same time facilitating traditional crimes in new ways. Every year trillions of ringgits are lost to cybercrimes and those figures are only for the reported ones. Many cybercrimes went unreported because of the guilt or shame felt by the victims. There are no signs that these criminals are slowing down anytime soon, so it is important for Internet users to know the threats they are facing online in order to protect themselves.

TYPES OF CYBERCRIMES

Cyber criminals come up with a variety of ways to steal precious personal information or wealth from their victims, and their methods become more sophisticated along the way. Here are some of them:

Trojan Horse Virus
The virus often disguise as a legitimate software. Criminals usually use social engineering techniques to trick users into loading and launching the virus into their computer systems. The trojan enables cyber criminals to spy on your activities, steal and hold your personal data at ransom, and gain remote access to your computer system.

Ransomware
This malware can modify or block data on your computer. In order to restore the computer's performance and data, victims have to pay ransom to the cyber criminals. However, experts have warned that access to the blocked data or security of the computer is not guaranteed.

Keystroke logger
A keylogger is a type of surveillance technology used to monitor and record each keystroke typed on the keyboard of the device on which it is installed. Though there are ethical usages of it, cybercriminals have known to use it to steal sensitive personal information, login credentials, or sensitive enterprise data.

Distributed Denial of Service (DDoS)
In a DDoS attack, hundreds or thousands of compromised machines (multiple computers and internet connections) are used to flood the access to a targeted system (this could be a machine, network resource, or website). Victims of a DDoS attack include both the end targeted system and all systems controlled by the hacker in the attack. DDoS attacks are usually distributed via botnets globally.

Botnet
A "bot" is a type of malware that allows an attacker to take control over an affected computer. Botnet is a network of infected machines ranging from a few hundreds to hundreds of thousands stretching across the globe. Many of these computers are infected without their owners' knowledge. Botnets can be used to carry out a variety of automated tasks, including sending spams, viruses, and spyware; steal sensitive information such as credit card numbers, banking credentials, and personal information; DDoS; and Clickfraud.

Phishing
Victims of phishing often would receive an e-mail from a source posing as a legitimate company (e.g. banks). Once the attachment or the link in the email is clicked on, the victim's device will be infected with a malware. The malware allows the criminals to control the infected computer or steal data from it. Criminals use social engineering to lure victims to click on phishing emails.

Identity Theft
Cyber criminals steal victims' personal information such as full name, date of birth, or credit card number to commit financial fraud or other crimes, such as entering or exiting a country illegally, laundering money and drug trafficking. The consequences that follow can be detrimental to the victims.

E-Commerce fraud
The most popular e-commerce transactions associated with fraud occur in the airline industry, followed by general retail, electronics, ticketing, telecom, money transfers, toys, clothing, etc. Criminals use methods such as phishing and identity theft to facilitate commission of the crime.

Online fraud
Cyber criminals use e-mails, websites, chat rooms, and social media sites to make connections with victims. By exploiting the victims' trust, criminals deceive and manipulate the victims into giving up confidential information or even money to them. The types of online frauds include:

- 419 scams, miracle cures, advance fees for credit cards, parcel scam, shopping and auction sites fraud, mule recruitment, "something is wrong with your pc", fake check scams, identity theft, business opportunities, "relative in distress", sweeps-take offer, foreign lottery, secret shopper, phishing emails, prize winner, charity donation, love scam, and many more.

Key Risk Factors Of Becoming An Online Fraud Victim

Life circumstance

Feeling isolated/lonely
Loss of a job
Negative change in financial status
Being concerned about debt

Knowledge

Being unaware that banks do not send emails to their customers asking them to click on a link to verify personal information
Being unaware that a privacy policy does not always mean the website will not share their information with other companies

Behaviour

Visiting a website that required them to read a privacy policy and terms of agreement
Opening email from unknown sources
Selling products on online auction
Purchasing through an online payment transfer site
Signing up for free-limited-time trial offers
Downloading apps
Being impulsive
Clicking on pop-ups

What is social engineering attack?

Through interactions with their victims, cyber criminals manipulate victims into making security mistakes and give away confidential information such as banking details, passwords or other personal information, or handover their money. Exploiting people's natural inclination to trust and help others, these social engineering techniques are becoming more sophisticated with criminals including details that make messages look real.

Though everyone, regardless of background or age, is at risk, elderly people are especially vulnerable to this attack.

A Guideline to Identify Phishing Email

Uses a public Internet account

If the email is from a public account (such as Gmail, Yahoo, etc.) but claims to be from your bank or other business, do not trust the email.

Uses an incorrect URL

Always double check to make sure that the site address in the provided link is accurate. You can also hover your mouse pointer over a link in the email to verify that the URL link is the same as the genuine site of the organization the email claims it represents. Once your mouse is on the link, the actual URL will appear at the bottom left of your PC screen.

Asks for banking information

A real bank would never ask for your bank account information, your debit card and PIN numbers or other sensitive information (such as your IC number) via email.

A lot of misspelled words and grammatical errors

Real companies have experienced staff who will not make such mistakes in official emails.

Sounds urgent

Cyber criminals count on natural human responses towards emotional triggers such as fear, urgency, and offers that are too good to be true.

What do you do?

Is this email a legitimate or phising email?

Source: Dell.com