Attack Tactics

- Social engineering is a tactic used by cyber criminals that uses lies and manipulation to trick people into revealing their personal information. Social engineering attacks frequently involve very convincing fake stories to lure victims into their trap. Common social engineering attacks include:
  - Sending victims an email that claims there's a problem with their account and has a link to a fake website. Entering their account information into the site sends it straight to the cyber criminal (phishing)
  - Trying to convince victims to open email attachments that contain malware by claiming it is something they might enjoy (like a game) or need (like anti-malware software)
  - Pretending to be a network or account administrator and asking for the victim's password to perform maintenance
  - Claiming that the victim has won a prize but must give their credit card information in order to receive it
  - Asking for a victim's password for an Internet service and then using the same password to access other accounts and services since many people re-use the same password
  - Promising the victim they will receive millions of dollars, if they will help out the sender by giving them money or their bank account information

---

Cyberspace's Most Wanted Cyber Criminals

Cyber Criminal #1

Location: Email attachments, downloaded files
Primary attack: Virus
Weakness: Anti-malware software, the cold shoulder

Cyber Criminal infects files all over Cyberspace with their sneaky viruses by tempting people into opening them and unleashing the malware. They flirt with you by sending email attachments promising cool games or free software that secretly contain harmful malware. They also hide viruses in music and other downloadable files.

Cyber Criminal’s contaminated files look harmless, but their viruses can cause severe damage to your computer. They can be even more dangerous if they gain access to your computer, using your computer to attack others!

To defend yourself, be very careful with files from Cyberspace and email attachments. Ask a trusted adult before downloading any files, download only from reliable sources, and scan everything with anti-malware software before you open it. Also, scan all email attachments before opening and don't open email attachments from people you don't know.

---

Learning about them can provide more awareness towards preventing Personal Loss.
Who are the Cyber Criminals?

Most cyber crimes are committed by individuals or small groups. However, large organized crime groups also take advantage of the Internet. These "professional" criminals find new ways to commit old crimes, treating cyber crime like a business and forming global criminal communities.

• Criminal communities share strategies and tools and can combine forces to launch coordinated attacks. They even have an underground marketplace where cyber criminals can buy and sell stolen information and identities.

• It's very difficult to crack down on cyber criminals because the Internet makes it easier for people to do things anonymously and from any location on the globe. Many computers used in cyber attacks have actually been hacked and are being controlled by someone far away. Crime laws are different in every country too, which can make things really complicated when a criminal launches an attack in another country.

Cyber Crimes & Criminals

Computer crime, or cybercrime, is any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Netcrime is criminal exploitation of the Internet, inherently a cybercrime.

According to the United States Department of Justice, there are three different types of cyber crimes:

• The computer as a target - attacking other people's computers with malware or other damaging attacks.

• The computer as a weapon - committing "traditional" crimes that can be committed offline too, such as theft or illegal gambling.

• The computer as an accessory - using a computer to store illegal or stolen information.

Victims of cyber crimes can lose their money, their jobs, their dignity and their good name, and it can take years to repair the damage. Remember, if it's a crime offline, you can bet it's also a crime online, and it can have just as severe of a punishment.

Ways they Attack

Here are a few types of attacks cyber criminals use to commit crimes. You may recognize a few of them:

• Botnet - a network of software robots, or bots, that automatically spread malware

• Fast Flux - moving data quickly among the computers in a botnet to make it difficult to trace the source of malware or phishing websites

• Zombie Computer - a computer that has been hacked into and is used to launch malicious attacks or to become part of a botnet

• Social Engineering - using lies and manipulation to trick people into revealing their personal information. Phishing is a form of social engineering

• Denial-of-Service attacks - flooding a network or server with traffic in order to make it unavailable to its users

• Skimmers - Devices that steal credit card information when the card is swiped through them. This can happen in stores or restaurants when the card is out of the owner's view, and frequently the credit card information is then sold online through a criminal community.