MANAGING CYBERSPACE EFFICIENTLY TO MINIMISE CYBERCRIME

Dr. Najim Ussiph
Department of Computer Science
Kwame Nkrumah University of Science and Technology, Kumasi.
nussiph.cos@knust.edu.gh
nussiph@yahoo.com

5th KNUST SUMMER SCHOOL (AUGUST 17 – 20, 2015)

CYBER CRIME: WHAT IT IS

Cybercrime is a term for ***any illegal activity that uses a computer or computer network*** as its primary means of commission

The U.S. Department of Justice expands the definition of cybercrime to include any illegal activity that uses a computer for the ***storage of evidence.***

The growing list of cybercrimes includes crimes that have been made possible by computers, such as:

Network intrusions, dissemination of computer viruses and computer-based variations of existing crimes such as:

- identity theft
- stalking
- bullying and
- terrorism.

- Opinions differ, for example, as to whether some widespread activities (such as file sharing) should be classified as criminal acts.

- Another controversy related to cybercrime is the issue of ***digital surveillance*** and its impact on civil liberties.

THE FACTS

- *Cybercrime is a bigger risk now than ever before due to the sheer number of connected people and devices and advances in IT.*
  - Cybercrime has now surpassed illegal drug trafficking as a criminal moneymaker
  - Somebody's identity is stolen every 3 seconds as a result of cybercrime
  - Without a sophisticated security package, your unprotected PC can become infected within four minutes of connecting to the Internet.

CATEGORIES OF CYBER CRIME

Cyber crimes are broadly categorized into three categories, namely crime against

- Individual
- Property
- Government

Each category can use a variety of methods and the methods used vary from one criminal to another.

Individual:

This type of cyber crime can be in the form of cyber stalking, distributing pornography, trafficking and "grooming".

Today, law enforcement agencies are taking this category of cyber crime very seriously and are joining forces internationally to reach and arrest the perpetrators.

Property:

In this case, cyber criminals can steal a person's bank details and siphon off money; misuse the credit card to make numerous purchases online; run a scam to get naïve people to part with their hard earned money; use malicious software to gain access to an organization's website or disrupt the systems of the organization.

The malicious software can also damage software and hardware, just like vandals damage property in the offline world.

Government:

Also referred to as *cyber terrorism*. If successful, this category can wreak havoc and cause panic amongst the civilian population.

In this category, criminals hack government websites, military websites or circulate propaganda. The perpetrators can be terrorist outfits or unfriendly governments of other nations.

TYPES OF CYBER CRIMES

Hacking:

This is a type of crime wherein a person's computer is intruded to gain access to his personal or sensitive information.

In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

Theft:

This type violates copyrights and downloads files such as e-books, music, movies, games and software.

There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by monitoring agents like FBI.

Today, the justice system is addressing this type cyber crime and there are laws that prevent people from illegal downloading.

Cyber Stalking:

This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk.

Identity Theft:

Big headache in e-commerce and banking services.

In this this type cyber crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history.

Malicious Software:

These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

Child soliciting and Abuse:

This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography.

The FBI and similar agencies have been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

MODUS OPERANDI

Operandi 1

Relates to theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud.

Usually a single event from the perspective of the victim.

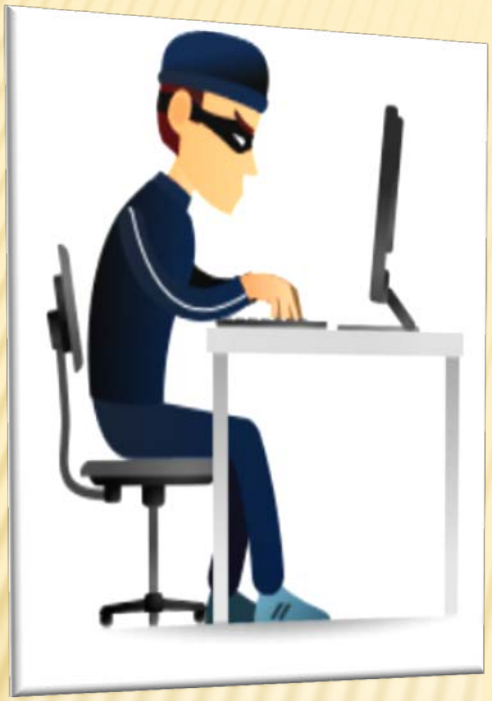
An example would be where the victim unknowingly downloads a Trojan horse virus, which installs a keystroke logger on his or her machine. The keystroke logger allows the hacker to steal private data such as internet banking and email passwords.

MODUS OPERANDI

Operandi 1

- Another common form of this operandi of cybercrime is ***phishing.***
- This is where the victim receives a supposedly legitimate email (quite often claiming to be a bank or credit card company) with a link that leads to a hostile website. Once the link is clicked, the PC can then be infected with a virus.
- Hackers often use this strategy by taking advantage of flaws in a web browser to place a Trojan horse virus onto the unprotected victims computer

Operandi 2



- Op 2 cybercrime tends to be much more serious and covers things such as cyber-stalking and harassment, child predation, extortion, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities.
- It is generally an on-going series of events, involving repeated interactions with the target. For example, the target is contacted in a chat room by someone who, over time, attempts to establish a relationship. Eventually, the criminal exploits the relationship to commit a crime

Operandi 2

- Or, members of a terrorist cell or criminal organisation may use hidden messages to communicate in a public forum to plan activities or discuss money laundering locations, for example.
- More often than not, it is facilitated by programs that do not fit under the classification crimeware. For example, conversations may take place using IM (instant messaging) clients or files may be transferred using FTP.

CYBERCRIMES PREVENTION TIPS

Step One: Education and Training

- You wouldn't let your unlicensed employees drive your company van, would you? Like driving, you and any employees that have access to your business network must have a foundational education before taking the wheel.
- What are your security policies?
- Are they well defined?

- Do all your employees understand the most common hacking tactics, such as phishing, social engineering, or packet sniffing (to name just a few)?
- Education and awareness across your staff will go a long way to protect yourself against many types of cybercrime.

Step Two: Securing Computers, Digital Assets, and Networking

- How safe is your vehicle?
- Sure, small-business/organizations budgets are tight, and finding ways to save is always going to be a priority for small-business owners, but most of us wouldn't drive without our seat belts securely latched or in a car without basic safety features.

Step Two: Securing Computers, Digital Assets, and Networking

- Is all software housed within your network continually up to date?
- Exploits in software are very common ways hackers gain access to systems and sensitive data. Updating software on network-connected machines should always be a top priority.

Step Two: Securing Computers, Digital Assets, and Networking

- Do you have business-class antivirus software installed (and up to date) on all office workstations and servers?
- Leading antivirus software can detect, remove, and protect your machines and network from malware.

Step Two: Securing Computers, Digital Assets, and Networking

- Do you scan your website or web applications for malware?
- Many of us are used to checking for viruses and malware on our personal computers, but don't realize that websites and web applications are just as susceptible.

Step Two: Securing Computers, Digital Assets, and Networking

- Do you have reliable backups of all of your critical data?
- Recovering from many types of common cybercrimes often involves restoring your data from a point prior to the event in question. Not having reliable and securely stored backups of your data is a significant liability.

Step Two: Securing Computers, Digital Assets, and Networking

- Is your network equipped to handle network-specific attacks? Unsophisticated networks are particularly susceptible to attacks.
- DDOS mitigation devices and tools offer reliable protection though often require enterprise-sized budgets. If you own a small business, this type of luxury wouldn't normally be practical, financially speaking.

Step Two: Securing Computers, Digital Assets, and Networking

- However, with the growing adoption of cloud and utility computing services, using a quality cloud-computing partner— one that has already invested the necessary capital to protect its network—is a cost-effective solution.

OTHER COMMON PREVENTION TIPS

In general, online criminals are trying to make their money as quickly and easily as possible. The more difficult you make their job, the more likely they are to leave you alone and move on to an easier target

Below are some common tips:

- Keep your computer current with the latest patches and updates.
- Make sure your computer is configured securely.
- Choose strong passwords, review regularly and keep them safe.

OTHER COMMON PREVENTION TIPS

- Protect your computer with security software.
- Protect your personal information.
- Beware of Online offers that look too good to be true.
- Review bank and credit card statements regularly.

thank you