DLE 2083: INTRODUCTION TO SECURITY MANAGEMENT

CHAPTER 13

INFORMATION, COMMUNICATION & CYBER SECURITY

VISION COLLEGE

Chapter 13: Learning Outcomes

- At the end of the topic, students should be able to:
  - Defines computer security.
  - Describes all types of computer security threats.
  - Defined information, ICTs, and cyber space.
  - Described the typical access vectors.
  - Defined the typical malicious activities.

VISION COLLEGE

Information Security

- Information security includes the security of information in all its forms, of which the most important conventional categories are verbal and cognitive forms, hard forms (including paper documents and artifacts), information technology (IT), information and communications technology (ICT), and cyber space (essentially electronically networked information and ICTs).

ICTs

- Information technology normally refers to any electronic or digital means of holding or communicating information.
- Some authorities prefer to refer to information and communications technology (ICT) in order to bring more attention to communications technologies, such as radios, telephones, and e-mail.

VISION COLLEGE

Cyber Space

- Cyber space best refers to digitally networked information and information technologies, normally personal computer terminals, but increasingly also mobile devices such as mobile telephones, connected to remote computers or hard drives (“servers”) via a digital network (either the Internet/World Wide Web, or an organizational Intranet).

Sources of Attacks

- The sources of cyber attacks are the human sources of the attacks.
- These sources include:
  - Official actors (such as spies)
  - Profit-oriented organized criminals
  - Terrorists
  - Commercial competitors
  - Ideologically motivated hackers (including campaigners for political and Internet freedoms)
  - Inquisitive and curious people
  - Journalists

Sources of Attacks

- Another key categorization is between external and internal threats (those without or within the target organization).

Access Vectors

- While the ultimate sources of cyber attacks are human actors, most cyber attacks are vectored by some sort of information technology or communication technology.

Access Vectors

- Examples of these vectors are as follow:
  - Printed documents
  - Social interactions
  - Malware
  - Databases
  - Webpages
  - Social media
  - Postal communications
  - Telephone communications
  - E-mail
  - Removable digital media
  - Cloud computing
  - Unsecured wireless networks

Malicious Activities

- Malicious activities can be categorized by their four (4) primary objectives or effects:

i. Misinformation

ii. Control of information or censorship

iii. Espionage, including the collection of information and the observation of the target

iv. Sabotage, or some sort of deliberate disruption or damage of the target, and terrorism

Computer Security

- Computer security is the protection of computer systems from the theft or damage to hardware, software, and information. **OR**
- Simply said; Computer security is the protection of computing systems and the data that is store or access.

VISION COLLEGE

Why is Computer Security Important?

- Computer Security allows the organization to carry out its business operation by:
  - Enabling people to carry out their daily tasks and jobs.
  - Supporting critical business process.
  - Protecting personal and sensitive information.

Why need to learn Computer Security?

- Good security standards follow the **"90 / 10" Rule**:
  - **10% of security safeguards are technical.**
  - **90% of security safeguards rely on the computer user (people) to adhere to good computing practices.**
- Example: The lock on the door is the 10%. You remembering to lock the lock, checking to see if the door is closed, ensuring others do not prop the door open, keeping control of the keys, etc. is the 90%. You need both parts for effective security.

VISION COLLEGE

Why need to learn Computer Security?

- This means that everyone who uses a computer or mobile device needs to understand how to keep their computer, device, and data secure.
- Information technology **security is everyone's responsibility.**

VISION COLLEGE

The internet can be a hazardous place

- Hundred or thousands of attacks per minute bombard the organization network.
- An unprotected computer can become infected or compromised within a few seconds after it is connected to the network.
- A compromised computer is a hazard to everyone else and not only for one computer.

VISION COLLEGE

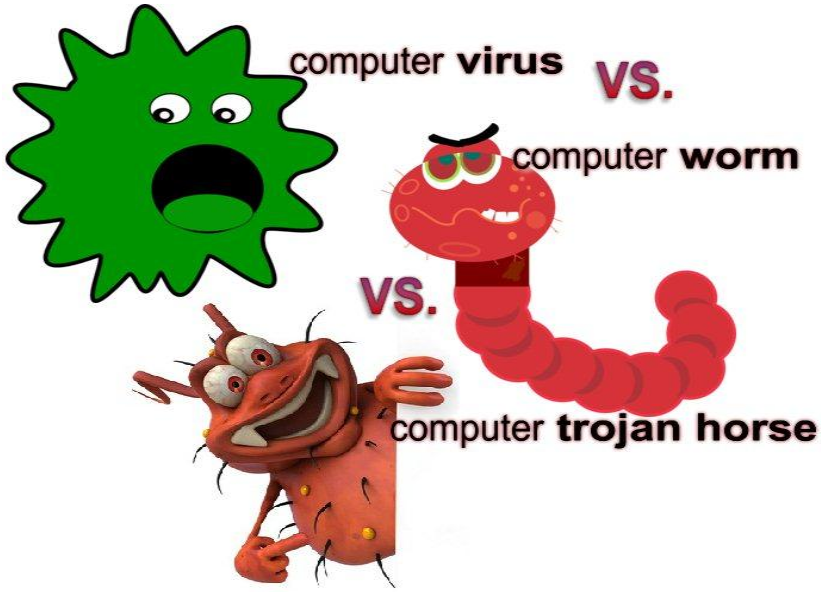
Types of computer security threats

1. Trojan

- Trojan is one of the most complicated threats among all. Most of the popular banking threats come from the Trojan family such as Zeus and SpyEye.
- It has the ability to hide itself from antivirus detection and steal important banking data to compromise your bank account.

Types of computer security threats

- If the Trojan is really powerful, it can take over your entire security system as well. As a result, a Trojan can cause many types of damage starting from your own computer to your online account.



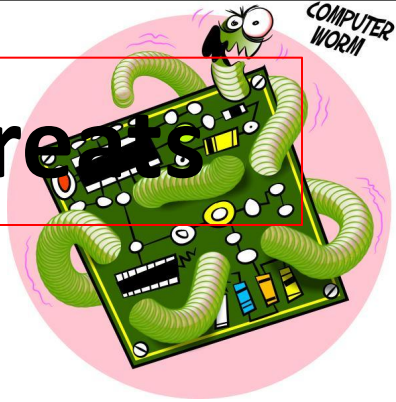
VISION COLLEGE

Types of computer security threats

2. Virus

- It is a malicious program where it replicates itself and aim to only destroy a computer. The ultimate goal of a virus is to ensure that the victim's computer will never be able to operate properly or even at all. It is not so popular today because Malware today is designed to earn money over destruction. As a result, Virus is only available for people who want to use it for some sort of revenge purpose.

Types of computer security threats



3. Worms

- One of the most harmless threats where it is program designed only to spread. It does not alter your system to cause you to have a nightmare with your computer, but it can spread from one computer to another computer within a network or even the internet.
- The computer security risk here is, it will use up your computer hard disk space due to the replication and took up most of your bandwidth due to the spread.

VISION
COLLEGE

Types of computer security threats

4. Spyware

- Is a Malware which is designed to spy on the victim's computer. If you are infected with it, probably your daily activity or certain activity will be spied by the spyware and it will find itself a way to contact the host of this malware. Mostly, the use of this spyware is to know what your daily activity is so that the attacker can make use of your information.

VISION COLLEGE

Types of computer security threats

5. Scareware

- Scareware is something that plant into your system and immediately inform you that you have hundreds of infections which you don't have. The idea here is to trick you into purchasing a bogus anti-malware where it claims to remove those threats. It is all about cheating your money but the approach is a little different here because it scares you so that you will buy.

VISION COLLEGE

Types of computer security threats

- Others types of computer security threats include:
  - **Keylogger**
  - **Adware**
  - **Backdoor**
  - **Wabbits**
  - **Exploit**
  - **Phishing**

VISION COLLEGE

Consequences for Security Violations

- Risk to security and integrity of personal or confidential information.
  - e.g. identity theft, data corruption or destruction, unavailability of critical information in an emergency, etc.
- Loss of valuable business information.
- Loss of employee and public trust, embarrassment, bad publicity, media coverage, news reports, etc.

VISION COLLEGE

Consequences for Security Violations

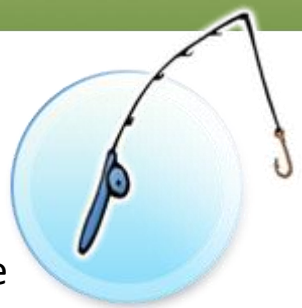
- Costly reporting requirements in the case of a compromise of certain types of personal, financial and health information.
- Internal disciplinary action's up to and including termination of employment, as well as possible penalties, prosecution and the potential for sanctions or lawsuits.

VISION COLLEGE

Measures to Minimize Computer Security Threats

- Use good, cryptic passwords that can't be easily guessed and keep your passwords secret.
- Make sure your computer, devices and applications are current and up to date.
- Make sure your computer is protected with up-to-date antivirus and anti-spyware software.
- Don't click on unknown links or attachments, and don't download unknown files or programs into your computer or other devices.

Primary Threats to Personal Online Safety



Phishing

E-mail sent by online criminals to trick you into going to fake Web sites and revealing personal information

Spam

Unwanted e-mail, instant messages, and other online communication

Identity Theft

A crime where con artists get your personal information and access your cash and/or credit

Hoaxes

E-mail sent by online criminals to trick you into giving them money

VISION COLLEGE

Steps to protect computer

Back up your files regularly.

Read Web site privacy statements.

Close pop-ups using red “X”.

Think before you click.

VISION COLLEGE

Back up Your Files

- Save to CD/DVD, a USB drive, or other external source.
- Use a Web-based backup service, e.g. Google drive or your own email.

VISION COLLEGE

Think Before You Click

- Be cautious with e-mail attachments and links.
- Only download files from Web sites you trust.

VISION COLLEGE

Read Privacy Statements

Understand what you are getting before you agree to download or share your personal information.

VISION COLLEGE

Use the Red "X" to Close Pop-ups

- Always use the red "X" in the corner of a pop-up screen.
- Never click "yes," "accept," or even "cancel," because it could be a trick that installs software on your computer.

VISION COLLEGE

If your identity is stolen…What to do??

- Report it to the relevant parties such as bank, police, etc.
- Deactivate and stop all bank account and transaction.
- Follow up via e-mail.
- Change all passwords

VISION COLLEGE