VISION UNIVERSITY COLLEGE

DLE 2083: INTRODUCTION TO SECURITY MANAGEMENT

CHAPTER 13

INFORMATION, COMMUNICATION & CYBER SECURITY

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.

Information Security

- Information security includes the security of information in all its forms including paper documents and artifacts, information technology (IT), information and communications technology (ICT), and cyber space.

VISION
UNIVERSITY
COLLEGE

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

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.

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.

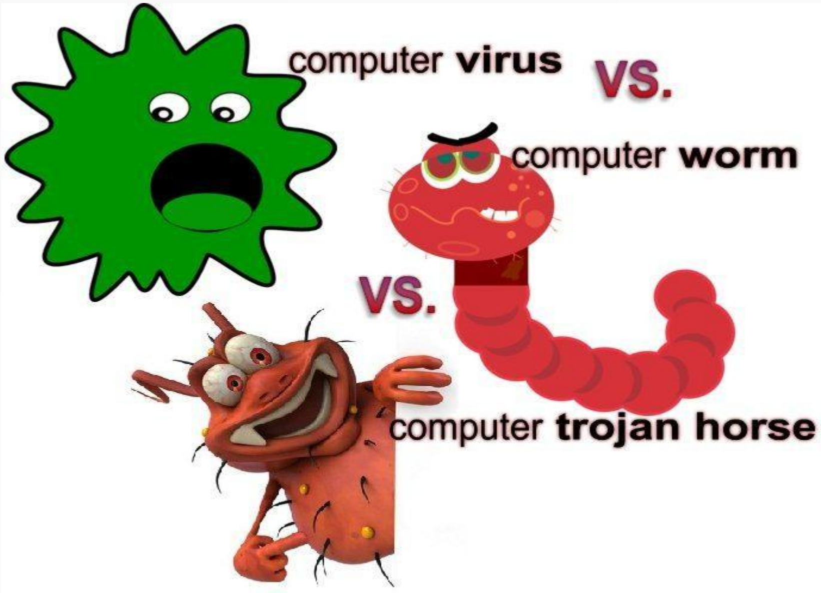
Types of computer security threats

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.

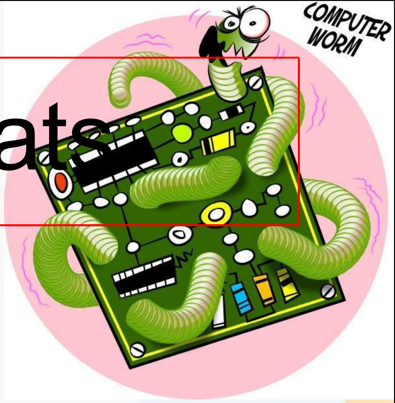


Types of computer security threats

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 UNIVERSITY COLLEGE

Types of computer security threats

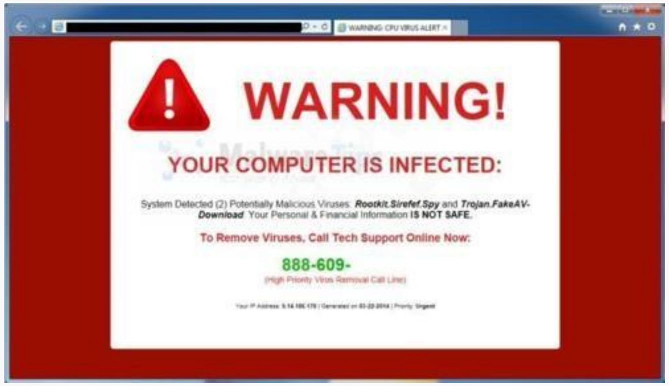
4. Spyware

- 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.

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.



WARNING!

YOUR COMPUTER IS INFECTED:

System Detected (2) Potentially Malicious Viruses: ***Rootkit.Sirefef.Spy*** and ***Trojan.FakeAV-Download*** Your Personal & Financial Information **IS NOT SAFE.**

To Remove Viruses, Call Tech Support Online Now:

888-609-

(High Priority Virus Removal Call Line)

Your IP Address: 5.14.186.170 | Generated on 03-22-2014 | Priority: Urgent

Types of computer security threats

- Others types of computer security threats include:
  - **Ransomeware**
  - **Identity Theft**
  - **DDoS Attack**
  - **Love Scam**
  - **Exploit**
  - **Phishing**

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.

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 UNIVERSITY 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

Steps to protect computer

Back up your files regularly.

Read Web site privacy statements.

Close pop-ups using red “X”.

Think before you click.

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 UNIVERSITY COLLEGE

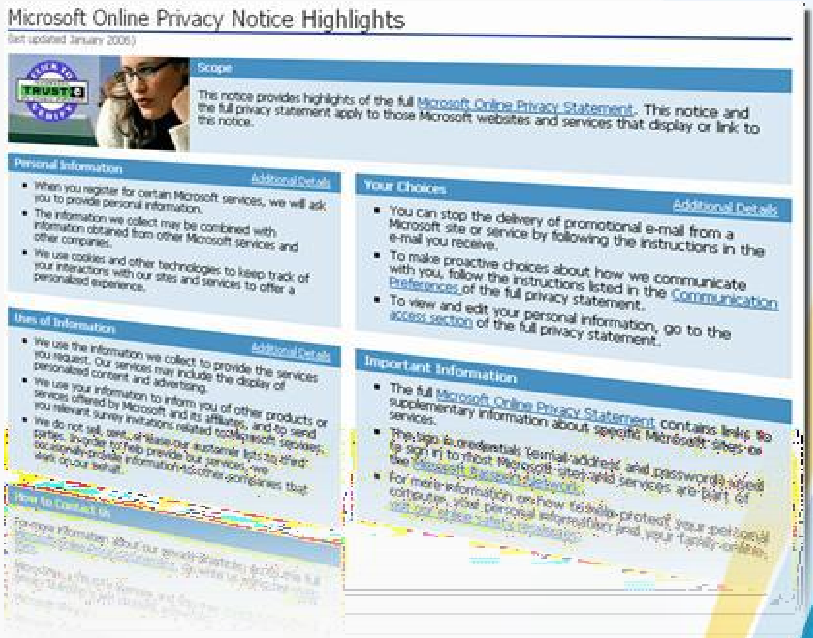
Think Before You Click

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

VISION UNIVERSITY COLLEGE

Read Privacy Statements

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



Microsoft Online Privacy Notice Highlights

(last updated January 2006)

Scope

This notice provides highlights of the full Microsoft Online Privacy Statement. This notice and the full privacy statement apply to those Microsoft websites and services that display or link to this notice.

Personal Information Additional Details

- When you register for certain Microsoft services, we will ask you to provide personal information.
- The information we collect may be combined with information obtained from other Microsoft services and other companies.
- We use cookies and other technologies to keep track of your interactions with our sites and services to offer a personalized experience.

Uses of Information Additional Details

- We use the information we collect to provide the services you request. Our services may include the display of personalized content and advertising.
- We use your information to inform you of other products or services offered by Microsoft and its affiliates, and to send you relevant survey invitations related to Microsoft services.
- We do not sell, rent, or lease our customer lists to third parties. In order to help provide our services, we occasionally provide information to other companies that work on our behalf.

How to Contact Us

For more information about our privacy practices, go to the full [illegible]

[illegible]

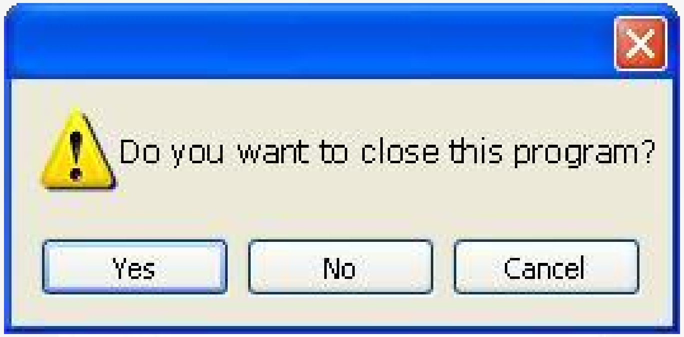
Your Choices Additional Details

- You can stop the delivery of promotional e-mail from a Microsoft site or service by following the instructions in the e-mail you receive.
- To make proactive choices about how we communicate with you, follow the instructions listed in the Communication Preferences of the full privacy statement.
- To view and edit your personal information, go to the access section of the full privacy statement.

Important Information

- The full Microsoft Online Privacy Statement contains links to supplementary information about specific Microsoft sites or services.
- The sign in credentials (e-mail address and password) used to sign in to most Microsoft sites and services are part of the Microsoft Passport Network.
- For more information on how to help protect your personal computer, your personal information and your family online, visit our online safety resources.

Use the Red “X” to Close Pop-ups

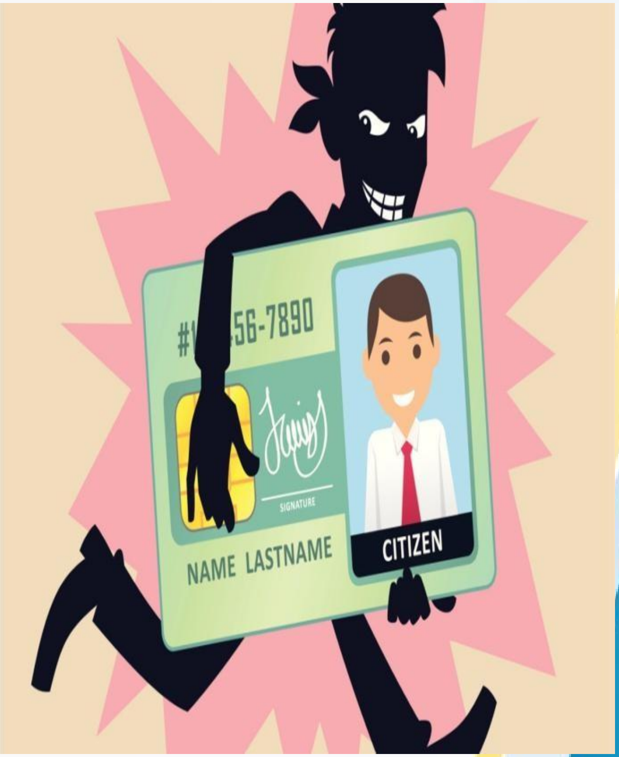


Do you want to close this program?

- 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.

Don’t Forget to....

- 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



Thank you

VISION
UNIVERSITY
COLLEGE