# DISCOVERING COMPUTERS CHAPTER 10 KHANH TRUONG

Computer Security and Safety, Ethics, and Privacy

## Computer Security Risks

- Any event or action that could cause the loss of or damage to computer hardware, software, data, information, or processing capability.

**Key Terms**

Computer Crime: illegal act involving a computer

Cyber-crime: online or internet illegal acts.

## Perpetrators of Cyber- Crime

- Hacker: refers to someone who accesses a computer or network illegally.
- Cracker: refers to someone who accesses a computer or network illegally but has the intent of destroying data.
- Script Kiddie: has the same intent as a cracker but does not have the technical skills and knowledge.
- Corporate Spy: hired to break into a specific computer and steal its proprietary data and information.

## Perpetrators of Cyber- Crime cont.

- Unethical Employee: employees who break into their employer's computer for a variety of reasons.
- Cyberextortionist: someone who use e-mail as a vehicle of extortion.
- Cyberterrorist: someone who uses the internet or network to destroy or damage computers for political reasons.

## Internet and Network Attacks

Every unprotected computer is susceptible to the first type of computer security risk –

- **Virus**: potentially damaging computer program that affects, or infects, a computer negatively by altering the way the computer works without the use's knowledge or permission.
- **Worm**: a program that copies itself repeatedly using up resources and possibly shutting down the computer or network.
- **Trojan horse**: a program that hides within or looks like a legitimate program. A certain condition or action usually triggers the Trojan horse.

## Internet and Network Attacks cont.

- Root-kit: is a program that hides in a computer and allows someone from a remote locations to take full control of the computer.

These attacks are classified as **malware** (short for malicious software).

**Payload** is the destructive event or prank the program is intended to deliver.

# Internet and Network Attacks cont.

| Infected computers generally have one or more of the following symptoms | |
|---|---|
| • Operating system runs much slower | • Music or unusual sounds play randomly |
| • Available memory is less than expected | • Existing programs and files appear |
| • Files become Corrupted | • Programs or files don't work properly |
| • Screen displays unusual message/image | • System properties change |
| • Programs/files mysteriously appear | • Operating system does not start |

# Safeguard against Computer Viruses and other Malware

Users can take several precautions to protect their home and work computers and mobile devices.

- **Antivirus**: a program that protects a computer against viruses by identifying and removing any computer viruses found in memory, on storage media, or on incoming files – they also protect against other malware.

They primarily scan for programs that attempt to modify the boot system, and other programs that normally are read from but not modified.

## Safeguard against Computer Viruses and other Malware cont.

- One technique that antivirus programs use to identify a virus is to look for virus signatures. A **virus signature** (aka., **Virus Definition**), is a known specific pattern of virus code.
- If an antivirus program identifies an infected file, its attempts to remove the malware.
- If the antivirus program cannot remove the infection, it often quarantines the infected file. This ensures that other files are not infected.

## Safeguard against Computer Viruses and other Malware cont.

| Tips for Preventing Viruses and other Malware |
|---|
| 1. Never start a computer with removable media inserted in the drives or plugged in. |
| 2. Never open an e-mail attachment unless you are expecting it. |
| 3. Set the macro security in programs so that you can enable or disable macros. |
| 4. Install an antivirus program on all of your computers. Update the software regularly |
| 5. Scan all downloaded programs for viruses and other malware. |
| 6. If the antivirus program flags an e-mail attachment as infected, delete or quarantine the attachment immediately. |
| 7. Before using any removable media, scan the media for malware. |
| 8. Install a personal firewall program. |
| 9. Stay informed about new virus alerts and virus hoaxes. |

## Internet and Network Attacks cont.

- **Back Door**: a set of instructions in a program that allows users to bypass security controls when accessing a program, computer, or network.
- **Spoofing**: is a technique intruders use to make their networks or internet transmission appear legitimate to a victim computer or network.

## Safeguard against Back Doors and Spoofing

- **Firewall**: a hardware and/or software that protects a network's resources from intrusion by users on another network such as the internet.
  - All network and online computer users should implement a firewall solution.
- **Personal Firewall**: a utility program that detects and protects a personal computer and its data from unauthorized intrusion.

## Unauthorized Access and Use

- Another type of computer security risk is unauthorized access and use.
- **Unauthorized access** is the use of computer or network without permission.
- **Unauthorized use** is the use of computer or its data for unapproved or possibly illegal activities.

## Safeguard: Indentifying and Authenticating Users

- **User Names and Passwords**: a **user name** or user ID (Identification), is a unique combination of characters, such as letters of the alphabet or numbers, that identifies one specific user.
- A **password** is a private combination of characters associated with the user name that allows the access to certain computer resources.

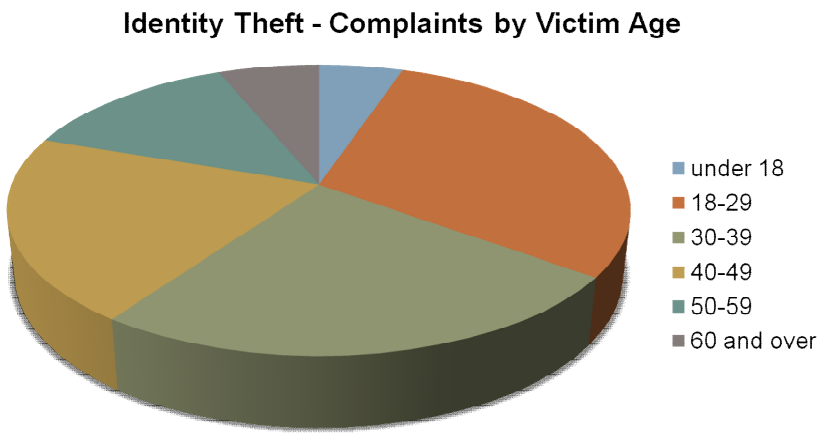
Note ~ Choosing easy-to-remember passwords are easily hacked by intruders. Hackers use computer automated tools to assist them with them guessing passwords.

# Safeguard: Indentifying and Authenticating Users

| Password Protection | | | |
|---|---|---|---|
| Number of characters | Possible Combinations | Time to discover Human | Time to discover Computer |
| 1 | 36 | 3 minutes | .000018 sec |
| 2 | 1,300 | 2 hours | .00065 sec |
| 3 | 47,000 | 3 days | .02 seconds |
| 4 | 1,700,000 | 3 months | 1 seconds |
| 5 | 60,000,000 | 10 years | 30 seconds |
| 10 | 3,700,000,000,000,000 | 580 million year | 59 years |

- Possible characters include the letters A-Z and numbers 0-9
- Human discovery assumes 1 try every 10 seconds
- Computer discovery assumes 1 million tries per second
- Average time assumes the password would be discovered in approximately half the

# Unauthorized Access and Use



## Information Theft

Information theft is yet another type of computer security risk, it occurs when someone steals personal or confidential information.

In order to protect information individuals use a variety of encryption techniques.

**Encryption** is the process of converting readable data into unreadable characters to prevent unauthorized access.

**Digital Signature** is an encrypted code that a person attaches to an electronic message to verify the identity of the message sender.

## Information Theft

**Secure Site**: a website that uses encryption techniques to secure its data.

**Digital certificate:** is a notice that guarantees a user or website is legitimate.

**Certificate authority:** is an authorized person or a company that issues and verifies digital certificates.

## System Failure

- **System failure** is prolonged malfunction of a computer. System failure can cause loss of hardware, software, data, or information.

Electrical power variations can cause loss of data and loss of equipment. A **Surge Protector** use special electrical components to provide a stable current flow to the computer.

An **Uninterruptible power supply (UPS)** is a device that contains surge protection circuits and one or more batteries that can provide power during a loss of power.

## System Failure

To prevent against data loss caused by a system failure or hardware/software/information theft, computer users should back up files regularly.

A **backup** is a duplicate of a file, program, or disk that can be used if the original is lost, damaged, or destroyed.

## Information Privacy

- **Spyware:** is a program placed on a computer without the user's knowledge that secretly collects information about the user.
- **Adware:** a program that displays an online advertisement in a banner or pop-up window on Web pages, email messages, or other Internet services.
- **Spam**: unsolicited e-mail message or newsgroup posting sent to multiple recipients or newsgroups at once.

**- E-mail filtering** is a service that blocks e-mail messages from designated sources.

## Information Privacy

- **Phishing:** a scam in which the perpetrator sends an official looking e-mail message that attempts to obtain your personal and financial information.
- **Phishing filter**: a program that warns or blocks you from potentially fraudulent or suspicious Web sites.
- **Pharming**: is a scam, similar to phishing, where a perpetrator attempts to obtain your personal and financial information, except that do so via spoofing
- **Clickjacking**: an object that can be clicked on a Web site, such as a button, image, or link, contains a malicious program.