DIGITAL SAFETY AND SECURITY

Threats, Issues, and Defenses

OBJECTIVES

- Define the term, digital security risks, and briefly describe the types of CYBERCRIMINALS
- Describe various types of internet and network attack, and explain ways to safeguard against these attacks
- Discuss techniques to prevent unauthorized computer access and use
- Explain the ways that software manufacturers protect against software piracy
- Discuss how encryption, digital signatures, and digital certificates work

OBJECTIVES

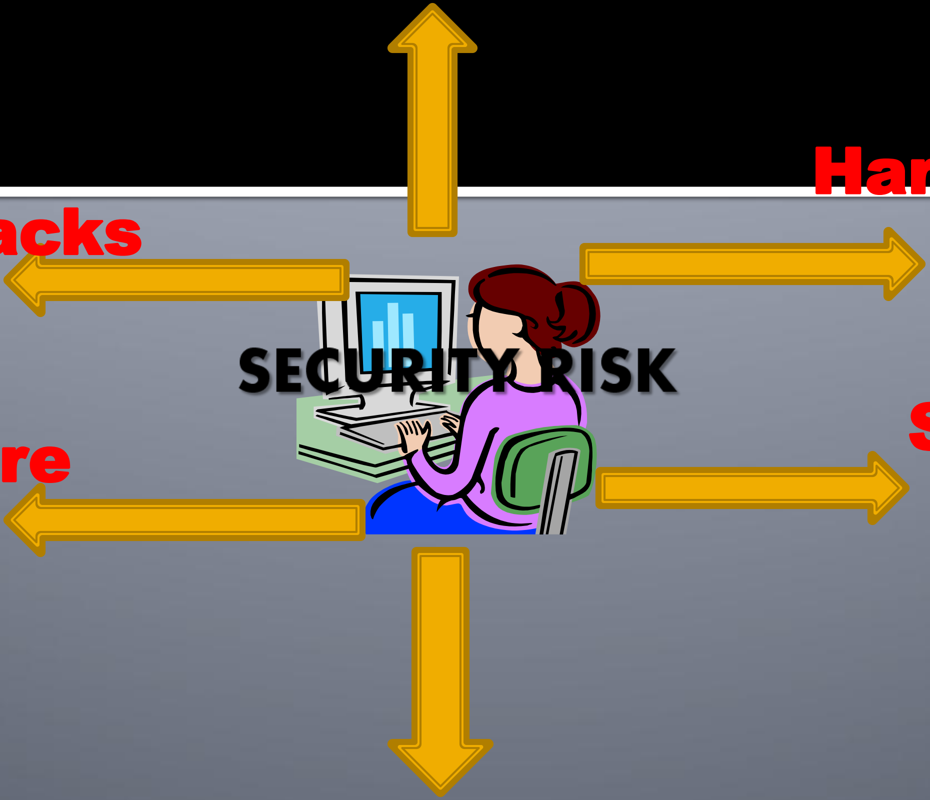
- Identify safeguards against hardware theft, vandalism, and failure
- Explain the options available for backing up
- Identify risks and safeguards associated with wireless communication
- Recognize issues related to information accuracy, intellectual property rights, codes of conduct, and green computing
- Discuss issues surrounding information privacy

DIGITAL SECURITY RISKS

- A digital security risk is any event or action that could cause a loss or damage to a computer or mobile device hardware, software, data, information, or processing capability
- Any illegal act involving the use of a computer or related devices generally is referred to as a COMPUTER CRIME.
- CYBERCRIME is an online or Internet-based illegal act

Unauthorized access and use

Intercepting wireless communication



SECURITY RISK

Internet and Network Attacks

Virus Attack

Hardware Theft

Stolen Computer

System Failure

Lightning Strike

Software Theft

Illegal Copying

Information Theft

Stolen Identity

HACKER

CRACKER

SCRIPT KIDDIE

CORPORATE SPIES

UNETHICAL EMPLOYEES

CYBEREXTORTIONIST

CYBERTERRORIST

DIGITAL SECURITY RISKS/HACKERS

HACKER- someone who discovers and exploits a computer system weakness or vulnerability.

CRACKER - **describe someone who broke into computer systems.**

SCRIPT KIDDIE - a person who uses existing computer scripts or code to hack into computers, lacking the expertise to write their own.

CORPORATE SPIES -can run legitimate offices and are usually hired by firms to spy on other firms. If business is slow, a corporate spy may pick a company without being hired and then collect information to sell to interested bidders

DIGITAL SECURITY RISKS/HACKERS

UNETHICAL EMPLOYEES -may break into their employers' computers for a variety of reasons. They may want to exploit a security weakness, receive financial gains from selling confidential information, or even to seek revenge.

CYBEREXTORTIONIST -**demanding payment through the use of or threat of some form of malicious activity against a victim**, such as data compromise or denial of service attack.

CYBERTERRORIST -is someone who uses the Internet or network to destroy or damage computers for political reasons.

Internet and Network Attacks

➢Information transmitted over networks has a higher degree of security risk than information kept on an organization’s premises.

➢To determine if your computer is vulnerable to an Internet or Network attack, you could use an **online security service**, which is a Web site that evaluates your computer to check for Internet and e-mail vulnerabilities.

Internet and Network Attacks

- Companies and individuals requiring assistance or information about Internet security branches can contact or visit the Web site for the Computer Emergency Response Team Coordination Center, or CERT/CC, which is a federally funded Internet security research and development center.
- Malware, short for malicious software, consist of program that act without a user's knowledge and deliberately alter the operations of computers and mobile devices

Computer Viruses, Worm, Trojan Horses, Rootkits, Spyware and Adware

- A computer virus is a potentially damaging computer program that affects, or infects, a computer negatively by altering the way the computer works without the user’s knowledge.
- A worm is a program that copies itself repeatedly, in memory or on a network, using up resources and shutting down the computer or network.
- A Trojan horse (named after the Greek myth) is a program that hides within or looks like a legitimate program and causes a condition or action when triggered.

Computer Viruses, Worm, Trojan Horses, Rootkits, Spyware and Adware

- A rootkit is a program that hides in a computer and allows someone from a remote location to take full control of the computer.

Execute programs, change settings, etc.

- Computer viruses, worms, Trojan horses, and rootkits are all classified as malware(malicious software), which are programs that act without a user's knowledge and deliberately alter the computer's operations.
- The payload is the destructive event or prank the program is intended to deliver.

Computer Viruses, Worm, Trojan Horses, Rootkits, Spyware and Adware

➢Infected computers can suffer from one or more of the following symptoms:

- OS running slower
- Less available memory
- Corrupted files
- Unusual message or images
- Unusual sounds playing
- Existing programs and files disappear
- Programs or files not working properly
- Unusual programs or files appear
- OS does not start up or unexpectedly shuts down

Computer Viruses, Worm, Trojan Horses, Rootkits, Spyware and Adware

➢Malware delivers its payload on a computer when a user

•Opens an Infected file

•Runs an infected program

•Boots the computer with infected removable media inserted

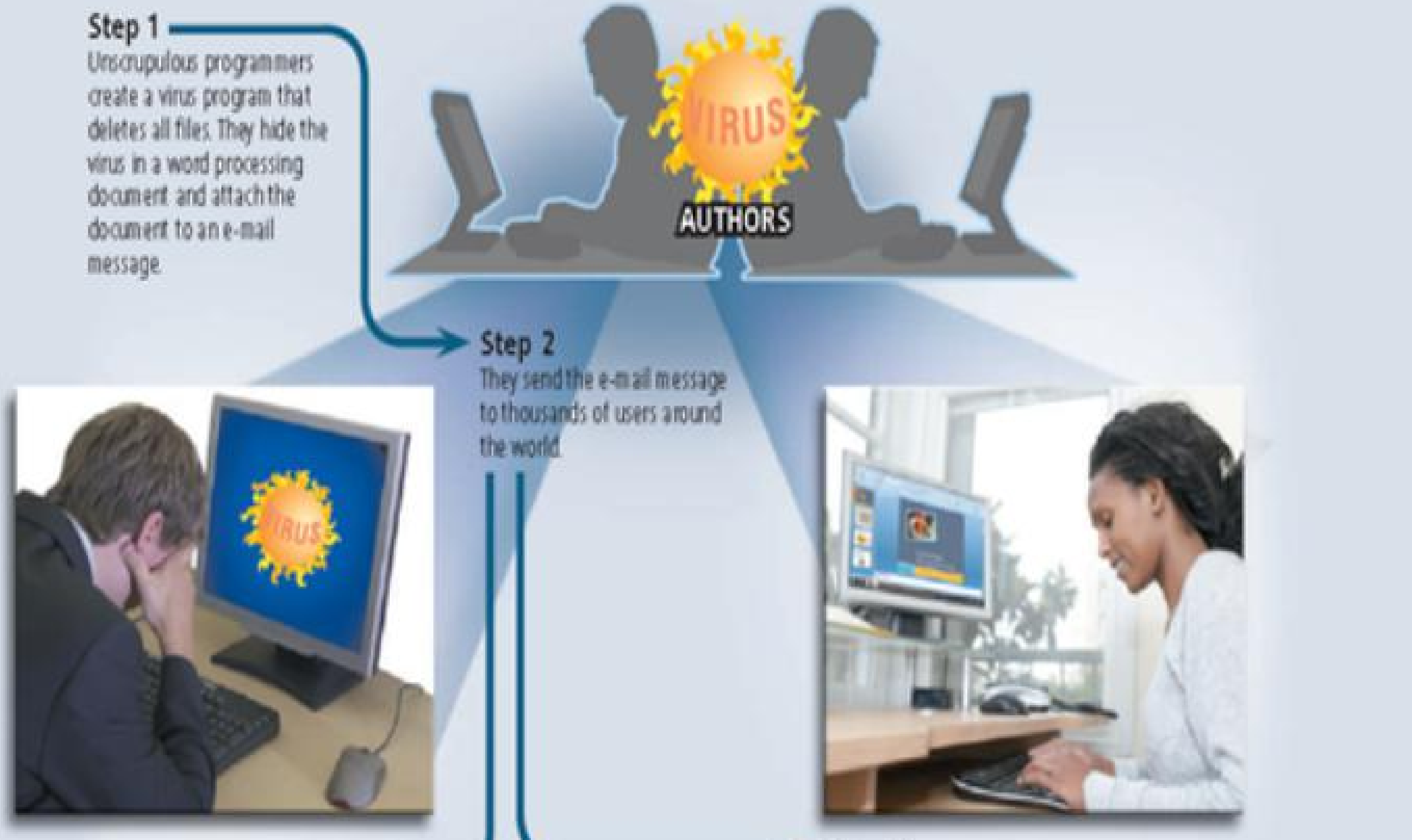
•Connects to an unprotected computer or network

•When a certain condition or event occurs, such as the clock changing to a specific date

Computer Viruses, Worm, Trojan Horses, Rootkits, Spyware and Adware

- Spyware – A program placed on a computer or mobile device without the user's knowledge that secretly collects information about the user and then communicates the information it collects to some outside source while the user is online.
- Adware – A program that displays an online advertisement in a banner or pop-up window on webpages, email messages, or other Internet services.

How a Virus Can Spread through an E-Mail Message



Step 1
Unscrupulous programmers create a virus program that deletes all files. They hide the virus in a word processing document and attach the document to an e-mail message.

Step 2
They send the e-mail message to thousands of users around the world.

Step 3a
Some users open the attachment and their computers become infected with the virus.

Step 3b
Other users do not recognize the name of the sender of the e-mail message. These users do not open the e-mail message — instead they immediately delete the e-mail message and continue using their computers. These users' computers are not infected with the virus.

Safeguards against Computer Viruses and Other Malware

- ➢Methods that guarantee a computer or network is safe from computer viruses and other malware simply do not exist.
- ➢Do not start a computer with removable media inserted in the drives.
- •If you must start the computer with removable media, be certain it is from a trusted source, which is an organization or person you believe will not send a virus.

Safeguards against Computer Viruses and Other Malware

- ➢Never open an e-mail attachment unless you are expecting the attachment and it is from a trusted source.
- ➢Some viruses are hidden in macros, which are instructions saved in software such as a word processing or spreadsheet program.
- ➢Users should install an antivirus program and update it frequently.

Safeguards against Computer Viruses and Other Malware

- An antivirus program protects a computer against viruses by identifying and removing any computer virus found in memory, storage, or incoming files.
- An antivirus program scans for programs that attempt to modify the boot program, the operating system, and other programs that normally are read from but not modified.
- One technique used to identify a virus is to look for virus signatures, also called virus definitions. Which are a known specific pattern of virus code.

Safeguards against Computer Viruses and Other Malware

- Another technique that antivirus program use to detect viruses is to inoculate existing program files.
- To inoculate a program files, the antivirus program records information such as the file size and creation date in a separate inoculation file, thus enabling it to tell if a file has been tampered with.
- If an antivirus program identifies an infected file, it attempts to remove the malware.
- If it cannot remove the infected file, it attempt to quarantine it.

Safeguards against Computer Viruses and Other Malware

- A quarantine is a separate area of a hard disk that holds infected files until the infection can be removed, ensuring other files will not become infected.
- In extreme cases, you may need to reformat the hard disk to remove malware from an infected computer.
- Stay informed about new virus alerts and virus hoaxes.
- A virus hoaxis an e-mail message that warns users of a nonexistent virus or other malware.
- They come in the form of chain mail and inform users to delete an important system file claiming it is malware.

Botnets

- A botnet is a group of compromised computers connected to a network such as the Internet that are used as part of a network that attacks other networks.
- A compromised computer, known as a **zombie**, is one whose owner is unaware the computer is being controlled remotely by an outsider.
- Cybercriminals install malicious bots on unprotected computers to create a botnet, also called a **zombie army.**

Denial of Service Attacks

- A **denial of service attack**, or **DoS attack,** is an assault whose purpose is to disrupt computer access to an Internet service such as the Web or email.
- This is done by flooding a victim computer with confusing data messages, thus making it unresponsive.
- A DDoS (distributed DoS) attack, is more devastating, in which a zombie army is used to attack computers or computer networks.

Back Doors

- A **back door** is a program that allow users to bypass security controls when accessing a program, computer, or network.
- Some malware will install a back door once it infects the victim computer.

Spoofing

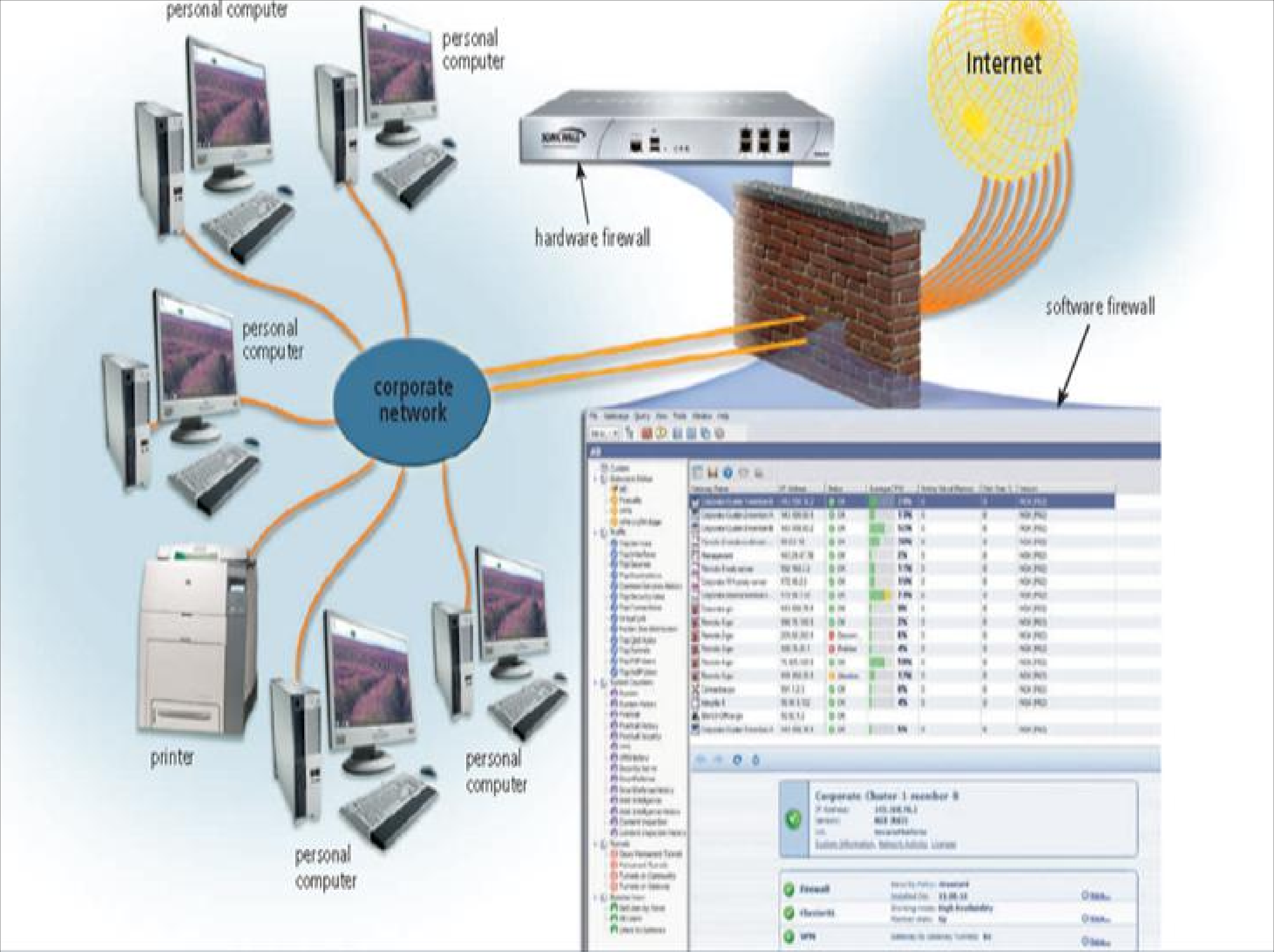
- **Spoofing** is a technique intruders use to make their network or Internet transmission appear legitimate to a victim computer or network.
- **E-mail spoofing occurs when the sender's address or other components of the e-mail header are altered so that it appears the e-mail originated from a different sender.**
- **IP spoofing occurs when an intruder computer fools a network into believing its IP address is associated with a trusted source.**

Safeguards against Botnets, DoS/DDoS Attack, Back Doors, and Spoofing

- Some of the latest antivirus programs include provisions to protect a computer form DoS and DDoS attacks.
- Users can also implement firewall solutions, install intrusion detection software, and set up honeypots.

Firewalls

- A **firewall** is a hardware and/or software that protects a network's resources from intrusion by users on another network such as the Internet.
- A **proxy server** is a server outside the organization's network that controls which communications pass into the organization's network.
- A **personal firewall** is a utility program that detects and protects a personal computer and its data from unauthorized intrusions.


personal computer
personal computer
Internet
hardware firewall
personal computer
corporate network
software firewall
printer
personal computer
personal computer
Corporate Cluster 1 member B
Firewall
ClusterXL
VPN

Intrusion Detection Software

- Intrusion detection software automatically analyzes all network traffic, assesses system vulnerabilities, identifies any unauthorized intrusions, and notifies network admins.

Honeypots

- A honeypot is a vulnerable computer that is set up to entice an intruder to break into it.
- They appear real to the intruder but are separated from the organization’s network.
- They are used to learn how intruders are exploiting their network.

UNAUTHORIZED ACCESS AND USE AND INFORMATION PRIAVACY

What is **“Unauthorized Access”?**

Unauthorized Access is when a person who does not have permission to connect to or use a system gains entry in a manner unintended by the system owner. The popular term for this is “hacking”.

UNAUTHORIZED ACCESS AND USE AND INFORMATION PRIAVACY

How did this happen?

The specifics are different for each individual event but it could happen in any number of ways. Usually access is gained via unpatched software or other known vulnerabilities.

UNAUTHORIZED ACCESS AND USE AND INFORMATION PRIAVACY

What should I do?

The University will notify you in some manner of the incident and provide you with more detailed information about the incident.The university encourages all persons impacted by an Unauthorized Access incident to contact one of the three credit reporting agencies to place a 90-day fraud alert on their credit report. If there is reason to believe more stringent action should be taken, it will be noted in the letter (or other notification) you receive.

UNAUTHORIZED ACCESS AND USE AND INFORMATION PRIAVACY

What is a Fraud Alert?
From the TransUnion website:

A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit
reporting companies. As soon as that company processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.

UNAUTHORIZED ACCESS AND USE AND INFORMATION PRIAVACY

How to Prevent Unauthorized Computer Access

1.Install all Security Patches.

2.Browsing the Internet? Pay Due Attention to File Sharing.

3.Keep the Firewall On.

4.Carefully Read Your Email MEssages and Know the Senders.

5.Maintain a Proper Backup of Your Data Online.

6.Make Use of Strong Passwords.

UNAUTHORIZED ACCESS AND USE AND INFORMATION PRIAVACY

What is unauthorized access to information?

Unauthorized access is when a person gains entry to a computer network, system, application software, data, or other resources without permission. Any access to an information system or network that violates the owner or operator's stated security policy is considered unauthorized access.

UNAUTHORIZED ACCESS AND USE AND INFORMATION PRIAVACY

What are some examples of unauthorized access?

Unauthorized access is when someone gains access to a website, program, server, service, or other system using someone else's account or other methods. For example, if someone kept guessing a password or username for an account that was not theirs until they gained access, it is considered unauthorized access.

The first step for any organization to prevent unauthorized data access is to keep current on allthe security patches.

Prevent Unauthorized Data Access: 9 Tips to Help You Boost Your Cybersecurity

1. Keep Current on all Security Patches
2. Detect and Respond to Intrusions Quickly
3. Implement Principle of Least Privilege (Minimize Data Access)
4. Use Multi-Factor Authentication
5. Implement IP Whitelisting
6. Encrypt Network Traffic Inside the System
7. Encrypt Data-at-Rest
8. Ensure Anti-Malware Protection/Application Whitelisting
9. Track and Manage Your Risks

Software Theft & Information Privacy

Software Theft

- The unauthorized or illegal copying, sharing or usage of copyright-protected software programs. Software theft may be carried out by individuals, groups or, in some cases, organizations who then distribute the unauthorized software copies to users.
- Software theft can make many forms from someone physically stealing a DVD-ROM, or floppy disk to intentional piracy of software.

Software Theft & Information Privacy

Safeguard Against Software Theft

- To protect media from being stolen, owners should keep original software boxes in a secure location.
- All computer users should backup their files regularly.
- Escort terminated employees immediately to protect their softwares and programs (in big companies).

Software Theft & Information Privacy

Information Privacy

- Also known as Data Privacy or Data Protection.
- Refers to the right of individuals and companies to deny or restrict the collection and use information about them.
- The relationship between the collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them.

Software Theft & Information Privacy

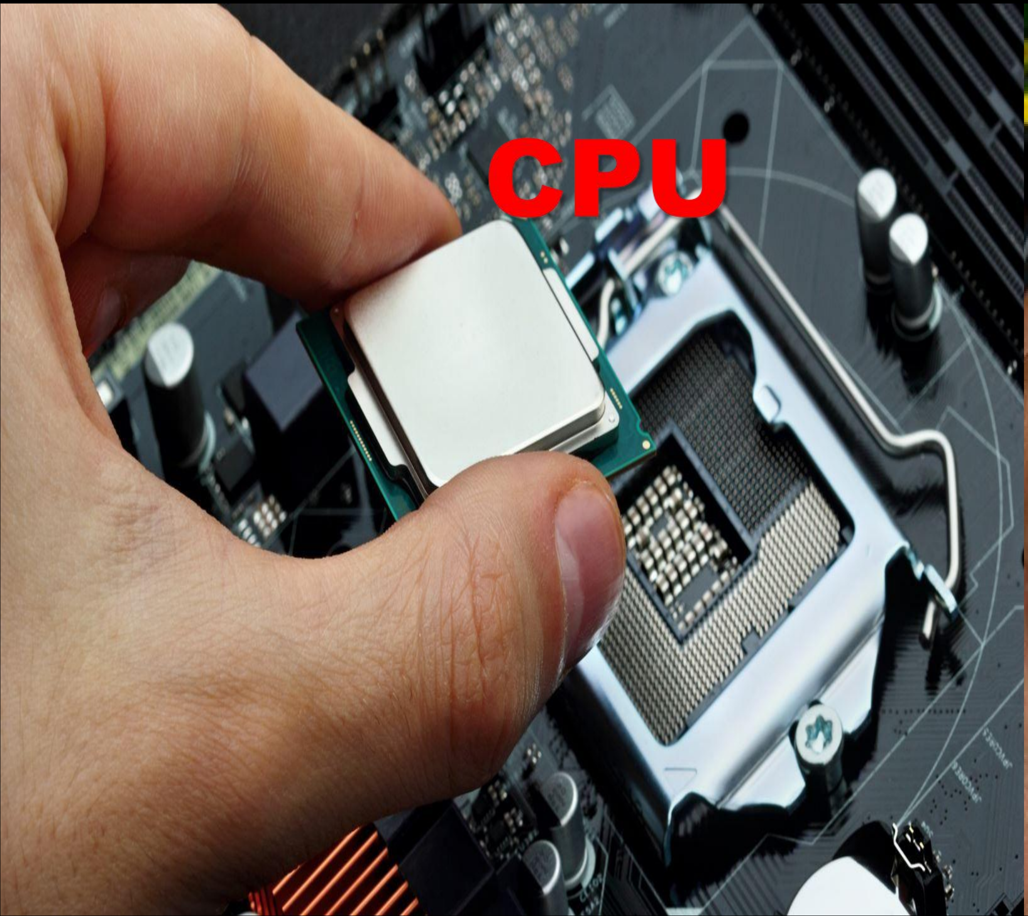
Some ways to Safeguard Personal Information

- Fill in only necessary information on rebate, warranty, and registration forms.
- Install a personal firewall.
- Do not reply to spam for any reason.
- Sign up for email filtering through your ISP or use an anti- spam program.

HARDWARE THEFT, VANDALISM, AND FAILURE

HARDWARE THEFT - the act of stealing digital equipment

HARDWARE THEFT, VANDALISM, AND FAILURE



HARDWARE THEFT, VANDALISM, AND FAILURE

HARDWARE VANDALISM- Is the act of defacing or destroying digital equipment.

HARDWARE THEFT, VANDALISM, AND FAILURE

- To help reduce the chances of theft, companies and schools use variety of security measures

Hardware theft and Vandalism Safeguards

➢ Physical Access Control (i.e. locked doors and windows) • Alarm System • Physical Security Devices (i.e., cables and locks) • Device-tracking app

Hardware theft and Vandalism Safeguards

➢ Physical Access Control (i.e. locked doors and windows)

➢Alarm System

➢Physical Security Devices (i.e., cables and locks)

➢ Device-tracking app

HARDWARE THEFT, VANDALISM, AND FAILURE

BACKING UP- the ultimate safeguard

BACK-UP - is a duplicate of a file, program, or media can be used if the original is lost, damaged, or destroyed.

- To back up files means to make copy of it.

- Off-site back ups are stored in location separate from the computer or mobile device site.

HARDWARE THEFT, VANDALISM, AND FAILURE

CLOUD STORAGE

-is a technology that allows you to save files in the storage, and then access those files via cloud.

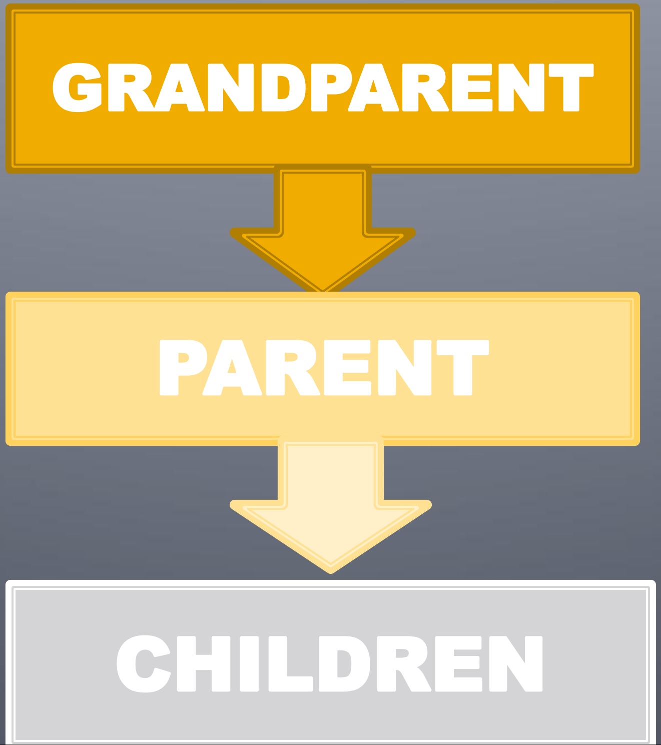
- the CLOUD represents the internet

- Categories of backups:

- Full
- Differential
- Incremental
- Selective
- Continuous data protection

HARDWARE THEFT, VANDALISM, AND FAILURE

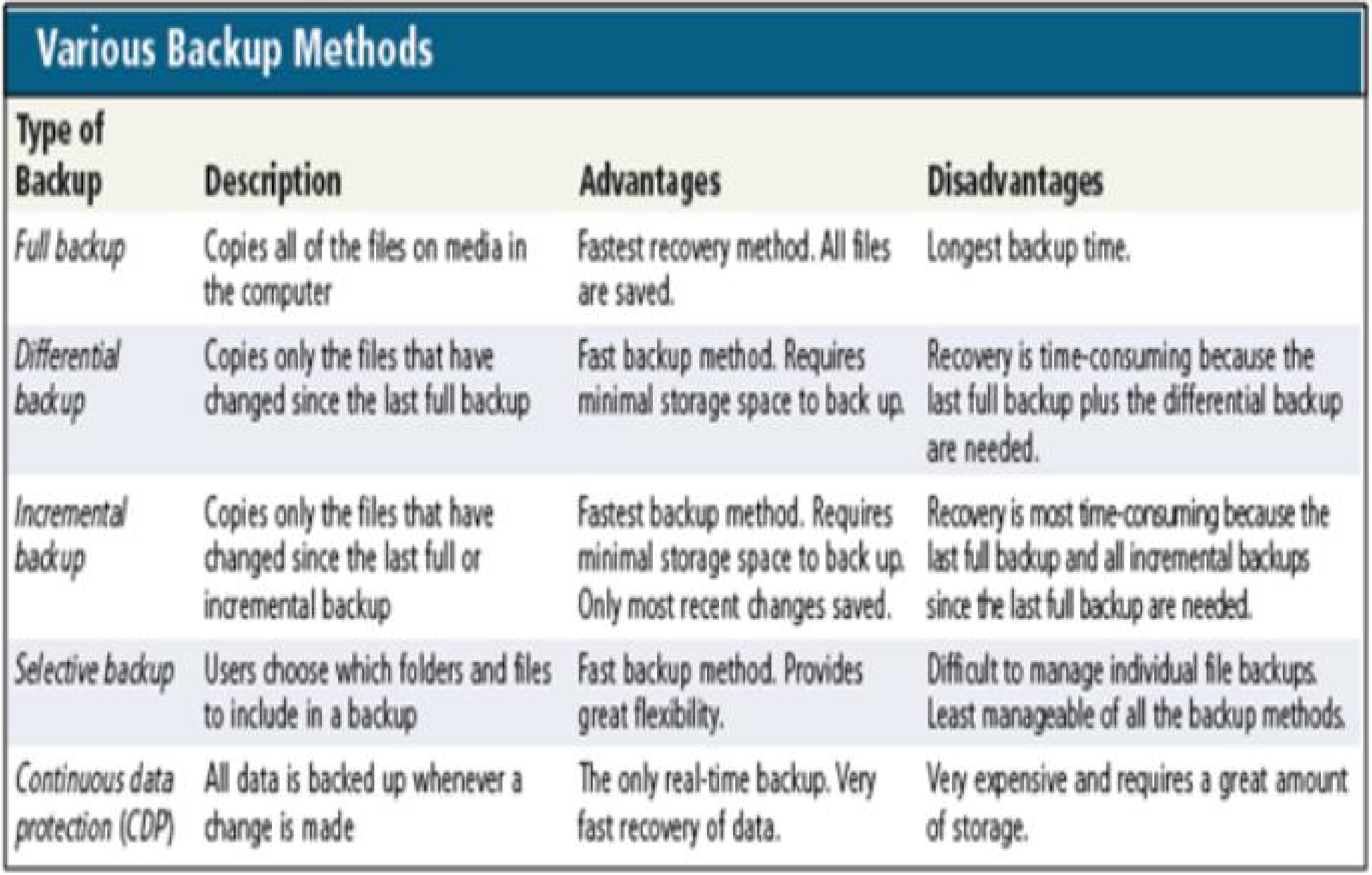
THREE GENERATION BACK-UP POLICY



GRANDPARENT

PARENT

CHILDREN



Various Backup Methods

Type of Backup	Description	Advantages	Disadvantages
Full backup	Copies all of the files on media in the computer	Fastest recovery method. All files are saved.	Longest backup time.
Differential backup	Copies only the files that have changed since the last full backup	Fast backup method. Requires minimal storage space to back up.	Recovery is time-consuming because the last full backup plus the differential backup are needed.
Incremental backup	Copies only the files that have changed since the last full or incremental backup	Fastest backup method. Requires minimal storage space to back up. Only most recent changes saved.	Recovery is most time-consuming because the last full backup and all incremental backups since the last full backup are needed.
Selective backup	Users choose which folders and files to include in a backup	Fast backup method. Provides great flexibility.	Difficult to manage individual file backups. Least manageable of all the backup methods.
Continuous data protection (CDP)	All data is backed up whenever a change is made	The only real-time backup. Very fast recovery of data.	Very expensive and requires a great amount of storage.

WIRELESS SECURITY & ETHICS AND SOCIETY

Wireless security

-is the prevention of unauthorized access or damage to computers or data using wireless networks, which include Wi-Fi networks.

-there are four types of wireless protocols, which include:

- Wired equivalent privacy (WEP)
- Wi-Fi protected access (WPA)
- Wi-Fi protected access 2 (WPA 2)
- Wi-Fi protected access 3 (WPA 3)

WIRELESS SECURITY & ETHICS AND SOCIETY

Ethics and society

Computer ethics are a set of moral standards that govern the use of computers. It is society's views about the use of computers, both hardware and software.

Information accuracy is a concern.

WIRELESS SECURITY & ETHICS AND SOCIETY

Ethics and Society

Digital rights management (DRM) is the use of technology and systems to restrict the use of copyrighted digital materials.

SUMMARY

- Variety of digital security risks
- Cybercrime and cybercriminals
- Risks and safeguards associated with Internet and network attacks, unauthorized access and use, software theft, information theft, and hardware theft, vandalism, and failure
- Ethical issues in society and various ways to protect the privacy of personal information
- Various backup strategies and methods of securing wireless communications