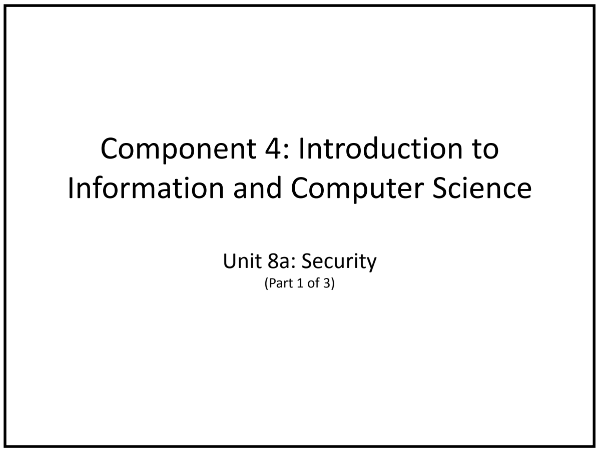
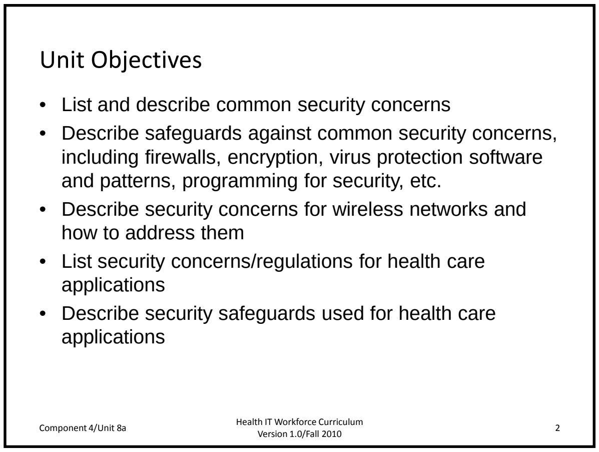


Component 4: Introduction to Information and Computer Science

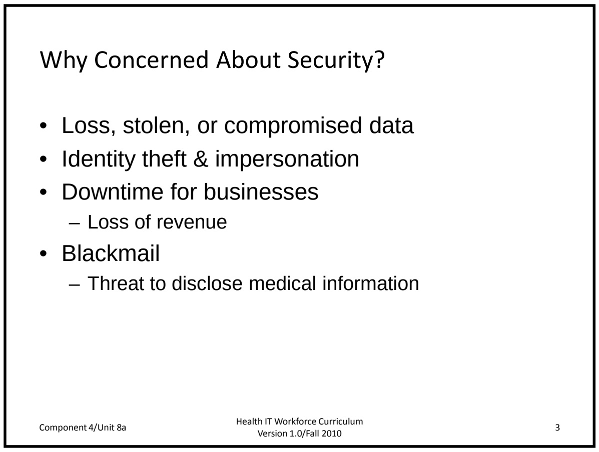
Unit 8a: Security

(Part 1 of 3)



Unit Objectives

- List and describe common security concerns
- Describe safeguards against common security concerns, including firewalls, encryption, virus protection software and patterns, programming for security, etc.
- Describe security concerns for wireless networks and how to address them
- List security concerns/regulations for health care applications
- Describe security safeguards used for health care applications



Why Concerned About Security?

- Loss, stolen, or compromised data
- Identity theft & impersonation
- Downtime for businesses
  - Loss of revenue
- Blackmail
  - Threat to disclose medical information

Common Threats to Security

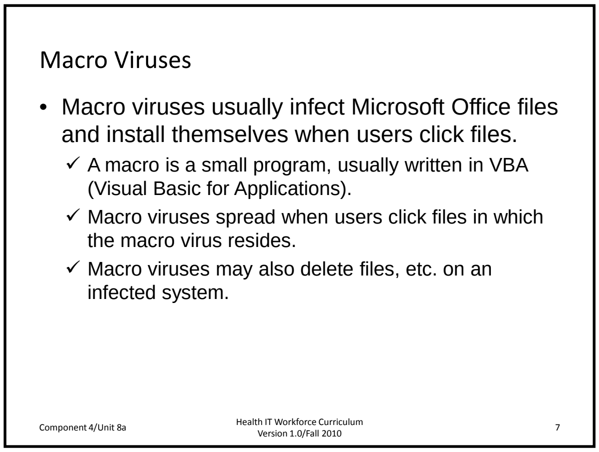
- Wikipedia:
  - “Malware, short for malicious software, is software designed to infiltrate a computer system without the owner's informed consent.”
- Types of malware include:
  - Trojans
  - Viruses
  - Hoaxes
  - Worms
  - Phishing
  - Macro viruses
  - Hackers

Trojan Horse

- A Trojan horse is a malware program that usually impersonates a known good file installed on the system by replacing (deleting) the good file.
  - ✓ Gets its name from the Greek Trojan Horse myth.
  - ✓ The Trojan then does its dirty work on a certain date, through a user action, or on command.
  - ✓ Trojans can destroy or copy data, install adware, or install a browser toolbar.
  - ✓ Trojans can record keystrokes and send this to the attacker and scan computer ports.

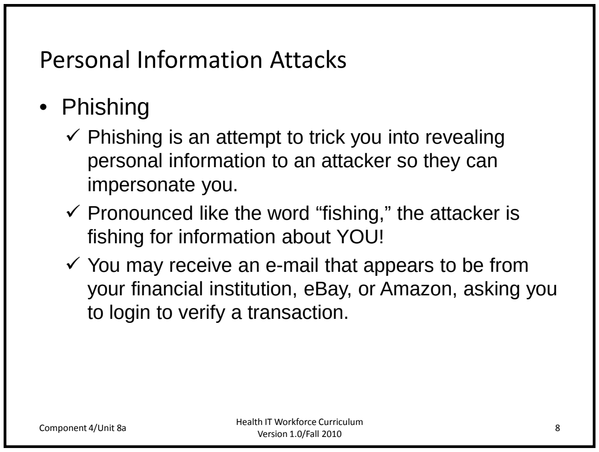
Viruses

- A virus is a computer program that can harm a computer and make it inoperable. Some viruses are only an annoyance.
  - ✓ Viruses usually do not replicate (make copies of) themselves on other computers.
  - ✓ Removing the virus usually cleans the computer.
  - ✓ Sending a virus via e-mail may replicate the virus.
  - ✓ In 2008, the Fun.exe virus spread itself via e-mail throughout the world and was very difficult to remove as it made many copies of itself on an infected computer.



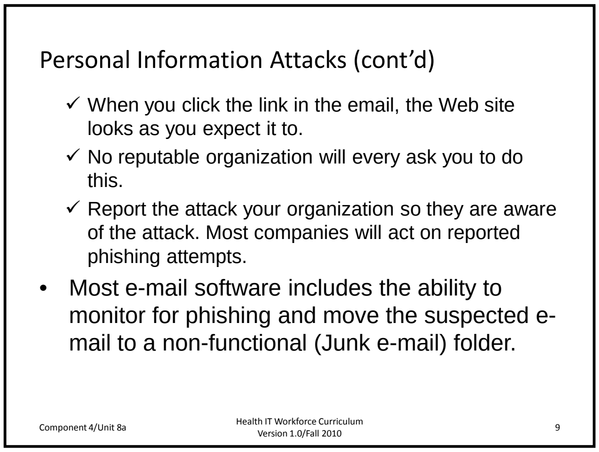
Macro Viruses

- Macro viruses usually infect Microsoft Office files and install themselves when users click files.
  - ✓ A macro is a small program, usually written in VBA (Visual Basic for Applications).
  - ✓ Macro viruses spread when users click files in which the macro virus resides.
  - ✓ Macro viruses may also delete files, etc. on an infected system.



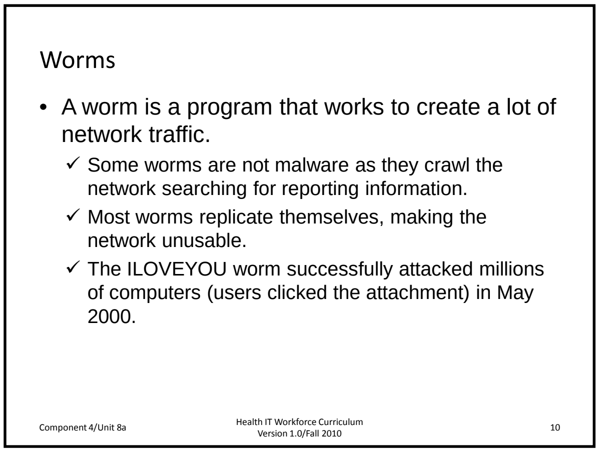
Personal Information Attacks

- Phishing
  - ✓ Phishing is an attempt to trick you into revealing personal information to an attacker so they can impersonate you.
  - ✓ Pronounced like the word “fishing,” the attacker is fishing for information about YOU!
  - ✓ You may receive an e-mail that appears to be from your financial institution, eBay, or Amazon, asking you to login to verify a transaction.



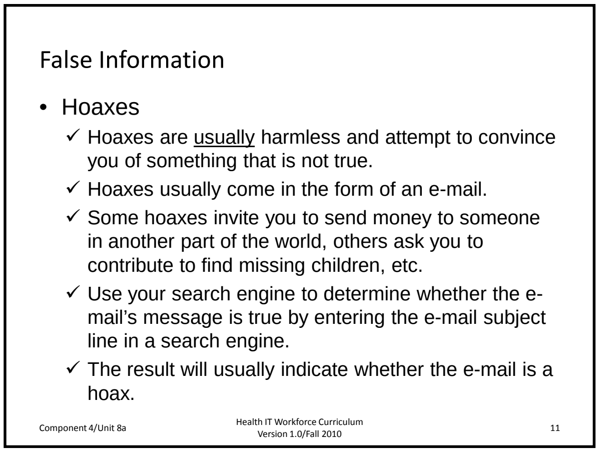
Personal Information Attacks (cont’d)

  - ✓ When you click the link in the email, the Web site looks as you expect it to.
  - ✓ No reputable organization will every ask you to do this.
  - ✓ Report the attack your organization so they are aware of the attack. Most companies will act on reported phishing attempts.
- Most e-mail software includes the ability to monitor for phishing and move the suspected e-mail to a non-functional (Junk e-mail) folder.



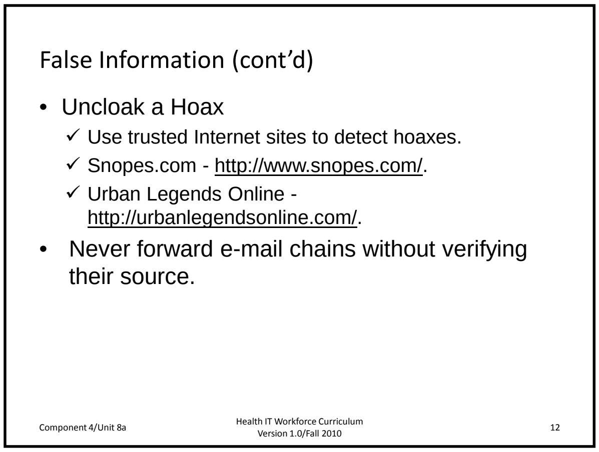
Worms

- A worm is a program that works to create a lot of network traffic.
  - ✓ Some worms are not malware as they crawl the network searching for reporting information.
  - ✓ Most worms replicate themselves, making the network unusable.
  - ✓ The ILOVEYOU worm successfully attacked millions of computers (users clicked the attachment) in May 2000.



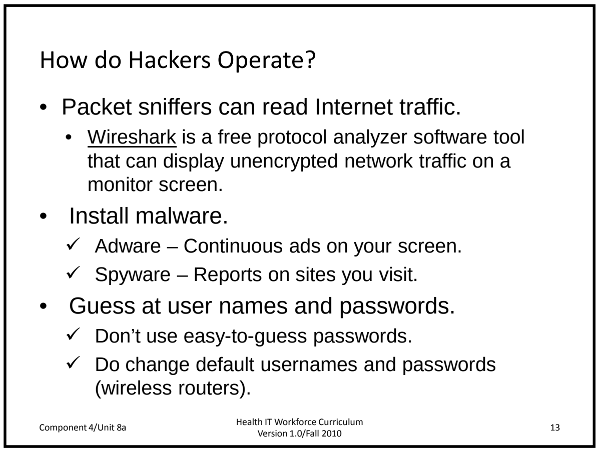
False Information

- Hoaxes
  - ✓ Hoaxes are usually harmless and attempt to convince you of something that is not true.
  - ✓ Hoaxes usually come in the form of an e-mail.
  - ✓ Some hoaxes invite you to send money to someone in another part of the world, others ask you to contribute to find missing children, etc.
  - ✓ Use your search engine to determine whether the e-mail's message is true by entering the e-mail subject line in a search engine.
  - ✓ The result will usually indicate whether the e-mail is a hoax.



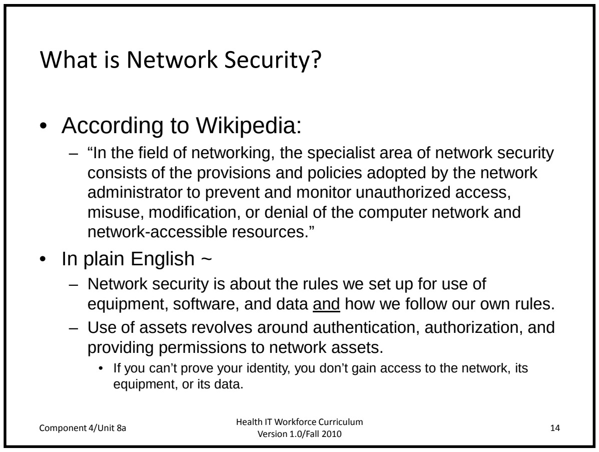
False Information (cont'd)

- Uncloak a Hoax
  - ✓ Use trusted Internet sites to detect hoaxes.
  - ✓ Snopes.com - http://www.snopes.com/.
  - ✓ Urban Legends Online - http://urbanlegendsonline.com/.
- Never forward e-mail chains without verifying their source.



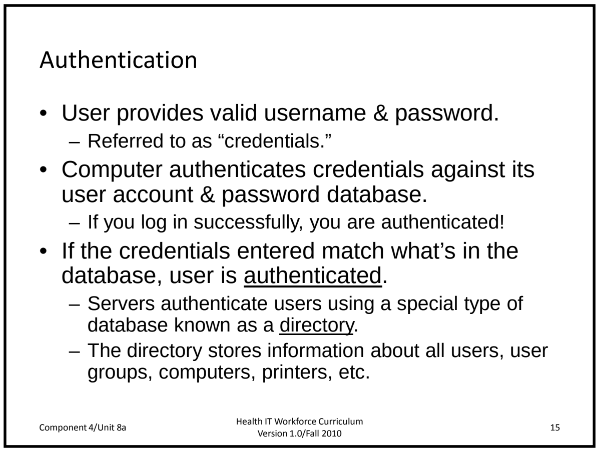
How do Hackers Operate?

- Packet sniffers can read Internet traffic.
  - Wireshark is a free protocol analyzer software tool that can display unencrypted network traffic on a monitor screen.
- Install malware.
  - ✓ Adware – Continuous ads on your screen.
  - ✓ Spyware – Reports on sites you visit.
- Guess at user names and passwords.
  - ✓ Don't use easy-to-guess passwords.
  - ✓ Do change default usernames and passwords (wireless routers).



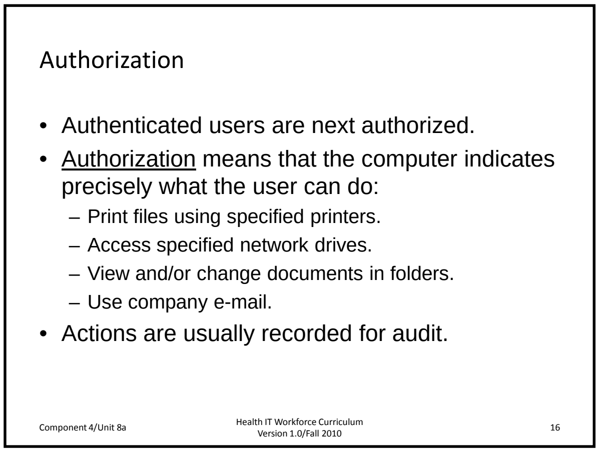
What is Network Security?

- According to Wikipedia:
  - "In the field of networking, the specialist area of network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources."
- In plain English ~
  - Network security is about the rules we set up for use of equipment, software, and data and how we follow our own rules.
  - Use of assets revolves around authentication, authorization, and providing permissions to network assets.
    - If you can't prove your identity, you don't gain access to the network, its equipment, or its data.



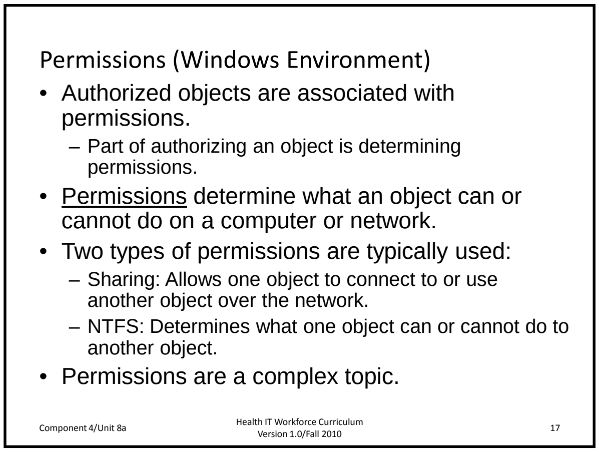
Authentication

- User provides valid username & password.
  - Referred to as "credentials."
- Computer authenticates credentials against its user account & password database.
  - If you log in successfully, you are authenticated!
- If the credentials entered match what's in the database, user is authenticated.
  - Servers authenticate users using a special type of database known as a directory.
  - The directory stores information about all users, user groups, computers, printers, etc.



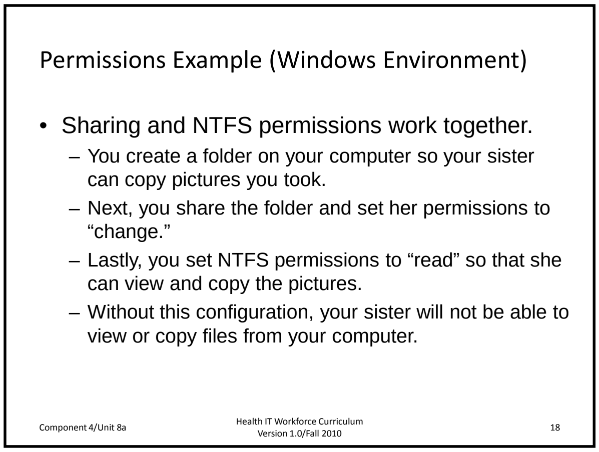
Authorization

- Authenticated users are next authorized.
- Authorization means that the computer indicates precisely what the user can do:
  - Print files using specified printers.
  - Access specified network drives.
  - View and/or change documents in folders.
  - Use company e-mail.
- Actions are usually recorded for audit.



Permissions (Windows Environment)

- Authorized objects are associated with permissions.
  - Part of authorizing an object is determining permissions.
- Permissions determine what an object can or cannot do on a computer or network.
- Two types of permissions are typically used:
  - Sharing: Allows one object to connect to or use another object over the network.
  - NTFS: Determines what one object can or cannot do to another object.
- Permissions are a complex topic.

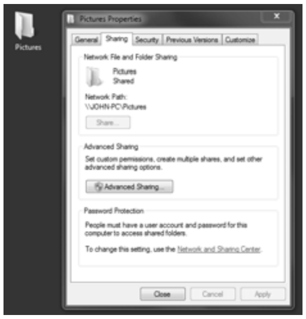


Permissions Example (Windows Environment)

- Sharing and NTFS permissions work together.
  - You create a folder on your computer so your sister can copy pictures you took.
  - Next, you share the folder and set her permissions to “change.”
  - Lastly, you set NTFS permissions to “read” so that she can view and copy the pictures.
  - Without this configuration, your sister will not be able to view or copy files from your computer.

Permissions Example

- Right-click the folder and select Properties from the menu.
- The Pictures folder is shared.
- Click Advanced Sharing to configure sharing permissions for this folder.



Network File and Folder Sharing

Pictures
Shared

Network Path:
\\JOHN-PC\Pictures

Advanced Sharing

Set custom permissions, create multiple shares, and set other advanced sharing options.

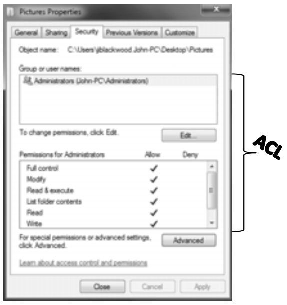
Password Protection

People must have a user account and password for this computer to access shared folders.

To change this setting, use the Network and Sharing Center.

Permissions Example (cont'd)

- Click the Security tab to configure NTFS permissions.
- Group or user names are listed in what is called an access control list, or ACL.
- Administrators have Full Control over this folder and its contents.
  - This means that a user who is a member of the Windows Administrator's group can do anything to this folder and its contents.
  - Anything means view, add new files, delete existing files, change existing files, create new sub-folders, etc.



Object name: C:\Users\jblackwood.John-PC\Desktop\Pictures

Group or user names:

Administrators (John-PC\Administrators)

To change permissions, click Edit.

Permissions for Administrators	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions