

Introduction to Information Technology IT111

Dr. Eng. Youssef Ntefeh

Lecture 9 - Network and Internet Security



جامعة الذكية
EVERYONE'S SMART UNIVERSITY

Learning Objectives

- Explain why computer users should be concerned about network and Internet security.
- List several examples of unauthorized access and unauthorized use.
- Explain several ways to protect against unauthorized access and unauthorized use, including access control systems, firewalls, and encryption.
- Provide several examples of computer sabotage.
- List how individuals and businesses can protect against computer sabotage.
- Discuss online theft, identity theft, spoofing, phishing, and other types of dot cons.

Learning Objectives

7. Detail steps an individual can take to protect against online theft, identity theft, spoofing, phishing, and other types of dot cons.
8. Identify personal safety risks associated with Internet use.
9. List steps individuals can take to safeguard their personal safety when using the Internet.

Why Be Concerned About Network and Internet Security?

- Security concerns related to computer networks and the Internet abound
- Computer Crime (cybercrime)
 - Any illegal act involving a computer, including:
 - Theft of financial assets
 - Manipulating data for personal advantage
 - Act of sabotage (releasing a computer virus, shutting down a Web server)
 - Phishing and Internet scams
- All computer users should be aware of security concerns and the precautions that can be taken

Unauthorized Access and Unauthorized Use

- Unauthorized Access
 - Gaining access to a computer, network, file, or other resource without permission
- Unauthorized Use
 - Using a computer resource for unapproved activities
- Both can be committed by insiders and outsiders
- Codes of Conduct
 - Used to specify rules for behavior, typically by a business or school

How to secure your network



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Encrypt your network with
a strong passphrase

Unauthorized Access and Unauthorized Use

- Hacking
 - Using a computer to break into another computer system
 - A serious threat for individuals, businesses, and the country (national security), i.e., cyberterrorism
- War Driving and Wi-Fi Piggybacking
 - War Driving
 - Driving around an area to find a Wi-Fi network to access and use without authorization

Unauthorized Access and Unauthorized Use

- Wi-Fi Piggybacking
 - Accessing an unsecured Wi-Fi network from the hacker's current location without authorization
- Interception of Communications
 - Unsecured messages, files, logon information, etc., can be intercepted using software designed for that purpose
 - New trend is to intercept credit card information during the card verification process
 - Packets sniffing software

Protecting Against Unauthorized Access and Unauthorized Use

- Access Control Systems
 - Used to control access to facilities, computer networks, databases, and Web site accounts
 - Identification Systems
 - Verify that the person trying to access the facility or system is an authorized user
 - Authentication Systems
 - Determine if the person is who he or she claims to be

Basics of Access Control



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Protecting Against Unauthorized Access and Unauthorized Use

- Possessed Knowledge Access Systems
 - Use information that only the authorized user should know
 - Passwords should be strong and changed frequently
 - Disadvantages
 - Passwords can be forgotten
 - If known, password can be used by someone who is not an authorized user

Protecting Against Unauthorized Access and Unauthorized Use

- Cognitive Authentication Systems
 - Use information the individual knows or can easily remember (birthplace, pet names, etc.)
 - Used in many password recovery systems
- Two-factor Authentication
 - Using two different methods to authenticate users
 - Biometric Feature – something you are
 - Possessed Object – something you have
 - Conventional username/password combination in conjunction with an access card that contains a one-time password

What is Two-Factor Authentication



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



Protecting Against Unauthorized Access and Unauthorized Use

– Possessed Object Access Systems

- Use a physical object an individual has in his/her possession to identify that individual
- Smart cards, magnetic cards
- RFID-encoded badges - USB security key
- Disadvantages: Can be lost or used by an unauthorized individual



SMART CARDS

Are read by a smart card reader to provide access to a facility or computer system.



USB SECURITY TOKENS

Are inserted into one of the computer's USB ports to provide access to that computer system.

Protecting Against Unauthorized Access and Unauthorized Use

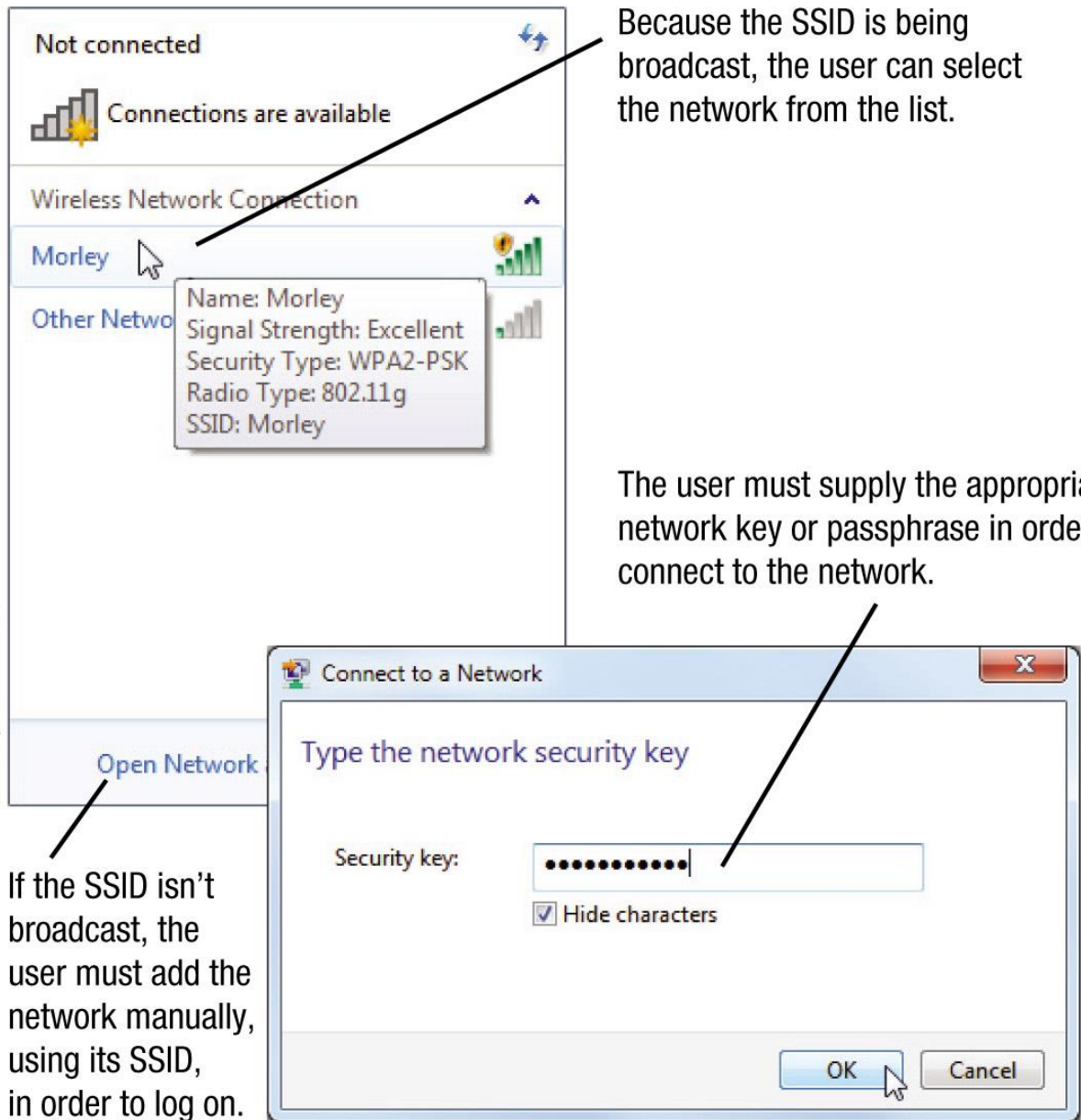
– Biometric Access Systems

- Identifies users by a particular unique biological characteristic
 - Fingerprint, hand, face, iris, voice, etc.
- Data read by biometric reader must match what is stored in a database
- Often used to
 - Control access to secure facilities
 - Log on to computers, punch in/out at work, law enforcement, etc.
- Advantages
 - Can only be used by the authorized individual
 - Cannot be lost or forgotten
- Disadvantages
 - Cannot be reset if compromised
 - Hardware and software are expensive

Protecting Against Unauthorized Access and Unauthorized Use

- Controlling Access to Wireless Networks
 - In general, Wi-Fi is less secure than wired networks
 - Security is usually off by default; wireless networks should be secured
 - Wireless network owners should:
 - Enable encryption (WPA2, WPA3)
 - Not broadcast the network name (SSID)

Courtesy of Microsoft



Not connected
Connections are available

Wireless Network Connection

Morley

Other Networks

Name: Morley
Signal Strength: Excellent
Security Type: WPA2-PSK
Radio Type: 802.11g
SSID: Morley

Open Network

Connect to a Network

Type the network security key

Security key:

☒ Hide characters

OK Cancel

Because the SSID is being broadcast, the user can select the network from the list.

The user must supply the appropriate network key or passphrase in order to connect to the network.

If the SSID isn't broadcast, the user must add the network manually, using its SSID, in order to log on.

Protecting Against Unauthorized Access and Unauthorized Use

- Firewalls, Encryption, and Virtual Private Networks (VPNs)
 - Firewalls
 - A collection of hardware and/or software intended to protect a computer or computer network from unauthorized access
 - Block access to the computer from hackers
 - Block access to the Internet from programs on the user's computer unless authorized by the user
 - Important for home computers that have a direct Internet connection, as well as for businesses
 - Work by closing down external communications ports

Understanding Encryption



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



Protecting Against Unauthorized Access and Unauthorized Use

–Encryption

- Method of scrambling contents of e-mail or files to make them unreadable if intercepted
- Private Key Encryption (symmetric key encryption)
 - Uses a single key
 - Most often used to encrypt files on a computer
 - If used to send files to others, the recipient and sender must agree on the private key to be used

Protecting Against Unauthorized Access and Unauthorized Use

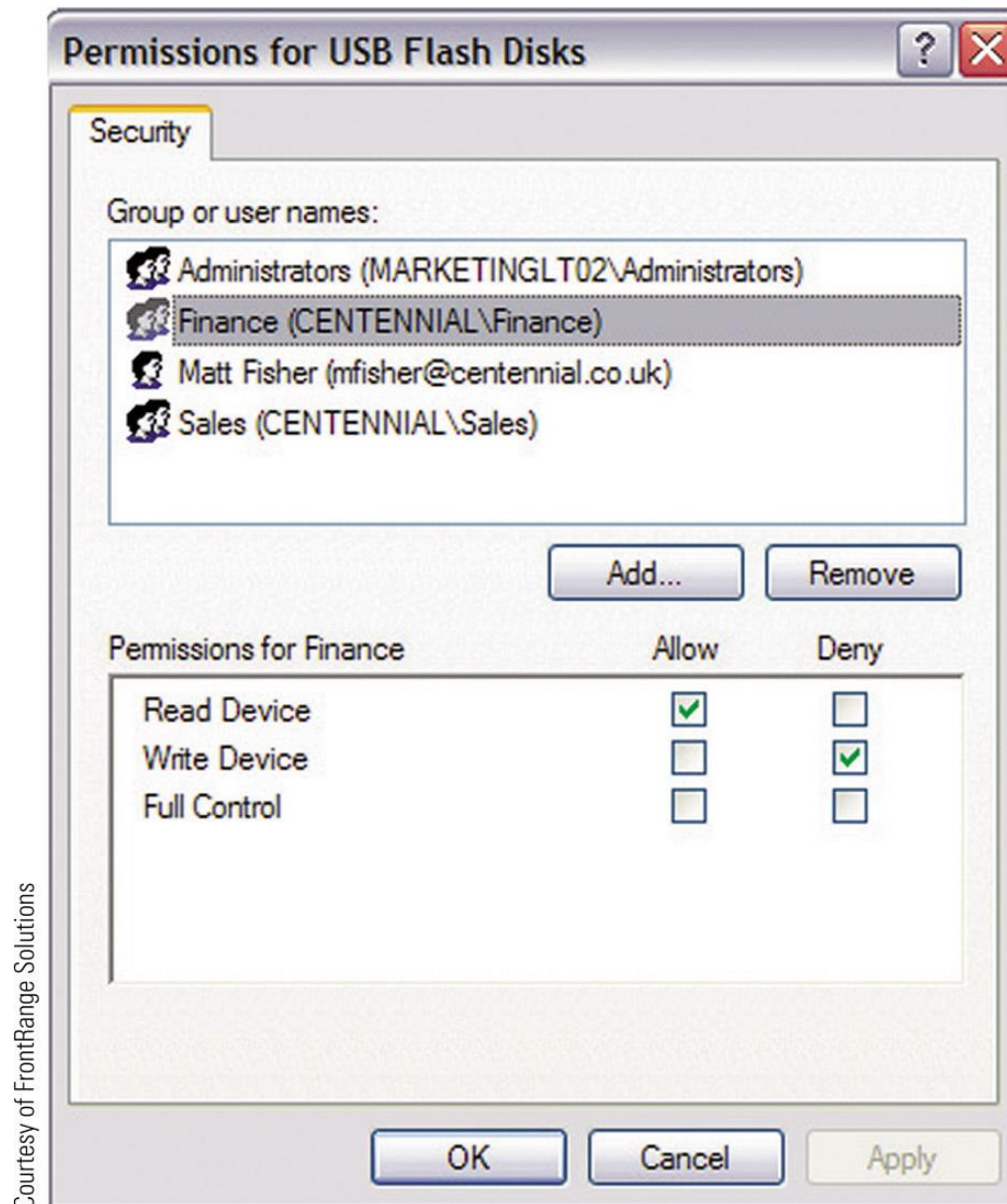
- Public Key Encryption (asymmetric key encryption)
 - Uses two keys (a private key and a public key) to encrypt and decrypt documents
 - Public key can be given to anyone
 - Key pairs can be obtained through a Certificate Authority
- Various strengths of encryption available
 - Stronger is more difficult to crack
 - Strong = 128-bit (16-character keys)
 - Military = 2,048-bit (256-character keys)

Protecting Against Unauthorized Access and Unauthorized Use

- Virtual Private Networks (VPNs)
 - A private secure path over the Internet
 - Allows authorized users to securely access a private network via the Internet
 - Much less expensive than a private secure network since it uses the Internet
 - Can provide a secure environment over a large geographical area
 - Typically used by businesses to remotely access corporate networks via the Internet
 - Personal VPNs can be used by individuals to surf safely at a wireless hotspot

Protecting Against Unauthorized Access and Unauthorized Use

- Sensible Employee Precautions
 - Screen Potential New Hires Carefully
 - Watch for Disgruntled Employees and Ex-Employees
 - Develop Policies and Controls
 - Ask Business Partners to Review Their Security



Courtesy of FrontRange Solutions

DIFFERENCE BETWEEN

Viruses

Malware

Trojans

Ransomware

Spyware

& Worms!

Computer Sabotage

- Computer Sabotage
 - Acts of malicious destruction to a computer or computer resource
 - Launching a computer virus
 - Denial of Service attack
 - Botnet
 - A group of bots (computers controlled by a hacker) that are controlled by one individual and work together in a coordinated fashion
 - Used by criminals to send spam, launch Internet attacks and malware, etc.

Computer Sabotage

- Computer Viruses and Other Types of Malware
 - Malware
 - Any type of malicious software
 - Written to perform destructive acts (damaging programs, deleting files, erasing drives, etc.)
 - Writing malware is considered unethical; distributing is illegal

Computer Sabotage

- Computer Viruses
 - A software program installed without the user's knowledge and designed to alter the way a computer operates or to cause harm to the computer system
 - Often embedded in downloaded programs and e-mail messages (games, videos, music files)
- Computer Worm
 - Malicious program designed to spread rapidly by sending copies of itself to other computers via a network
 - Typically sent as an e-mail attachment

Computer Sabotage

– Trojan Horse

- Malicious program that masquerades as something else
- Usually appears to be a game or utility program
- Cannot replicate themselves; must be downloaded and installed

• Denial of Service (DoS) Attacks

- Act of sabotage that attempts to flood a network server or Web server with so much activity that it is unable to function
- Distributed DoS Attacks target popular Web sites (like Twitter) and use multiple computers

Denial of Service (DoS) Attack

1. Hacker's computer sends several simultaneous requests; each request asks to establish a connection to the server but supplies false return information. In a distributed DoS attack, multiple computers send multiple requests at one time.

Hello? I'd like some info...

2. The server tries to respond to each request but can't locate the computer because false return information was provided. The server waits for a short period of time before closing the connection, which ties up the server and keeps others from connecting.

I can't find you, I'll wait and try again...

3. The hacker's computer continues to send new requests so, as a connection is closed by the server, a new request is waiting. This cycle continues, which ties up the server indefinitely.

Hello? I'd like some info...

Hello? I'd like some info...

I'm busy, I can't help you right now.

LEGITIMATE COMPUTER

4. The server becomes so overwhelmed that legitimate requests cannot get through and, eventually, the server usually crashes.

WEB SERVER



HACKER'S COMPUTER





Attack Types

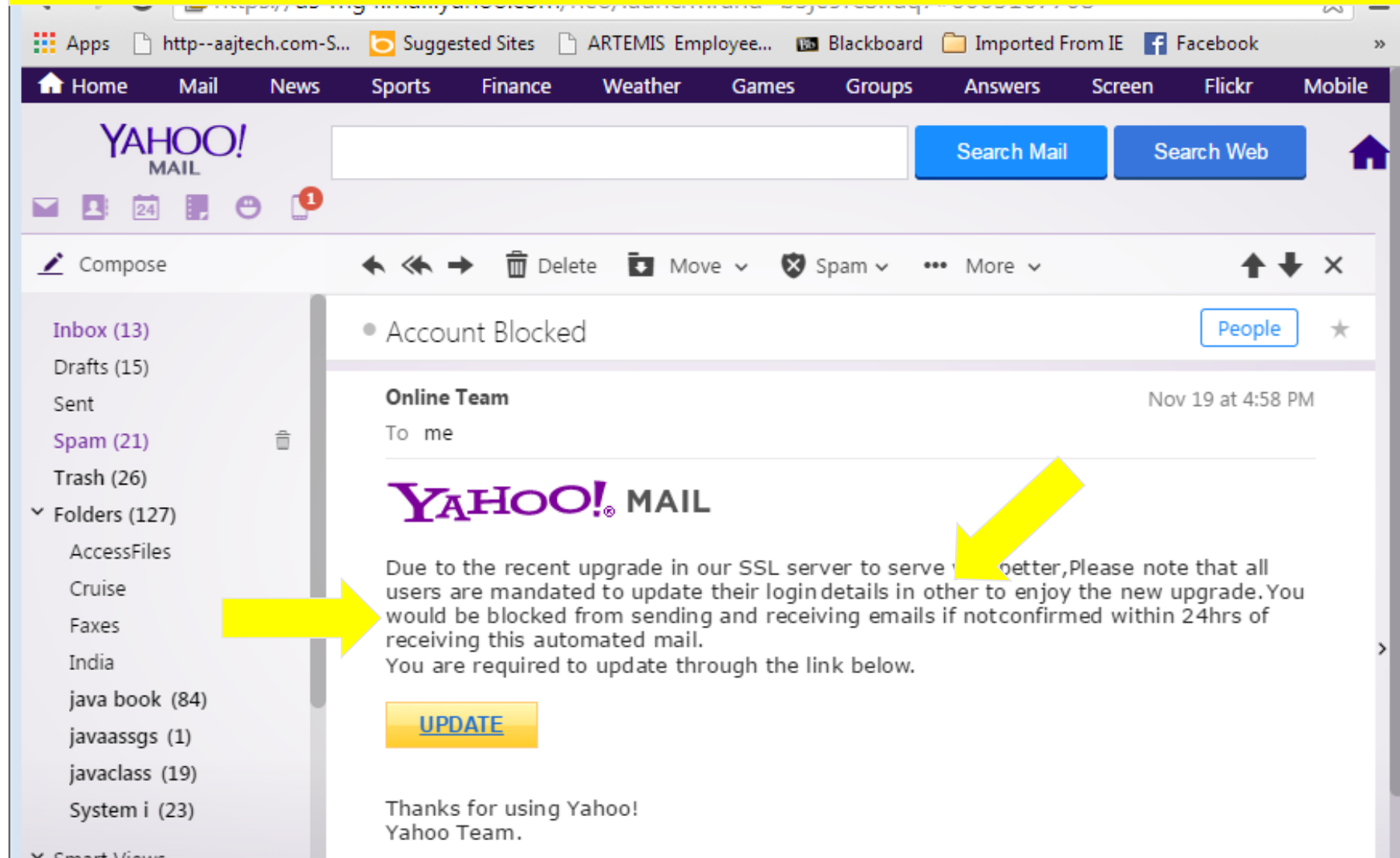
- Backdoors: access that circumvents security

- Programmer created when s/w written
- Installed after initial illegal access
 - Certain key combination
 - Create a new user id and pw



- Spoofing: make your computer resources look like someone else's

Got this email from "Yahoo"



Notice typo, bad grammar, and short time frame – trying to scare me into making a bad choice

How?

- User tries to open an infected file
 - Opens what they think is a picture.
- User inadvertently runs it
 - Thinks they're running a game.
- Uses an infected secondary storage media
 - Where has that thumb drive been?
- Connects to an infected network

Prevention?

- Never open a file from an unknown source.
- Don't use unknown secondary storage media.
- Don't open email attachments unless they are expected.
 - Even if it is from someone you trust
- Install antivirus s/w
 - Most computers come with some.
 - Lots of free stuff available.

Antivirus S/W

- Initially will scan all files looking for malware
 - If found will delete
 - If can't delete will quarantine
- Thereafter will check any downloaded files.
- Update s/w often
 - Updates will protect against the latest threats.



Personal Safety Issues

- Cyberbullying and Cyberstalking
 - Cyberbullying
 - Children or teenagers bullying other children or teenagers via the Internet
 - E-mails
 - Social networking sites
 - Blogs

Personal Safety Issues

- Cyberstalking
 - Repeated threats or harassing behavior between adults carried out via e-mail or another Internet communication method
 - Sending harassing e-mail messages to the victim
 - Sending unwanted files to the victim
 - Posting inappropriate messages about the victim
 - Signing the victim up for offensive material
 - Publicizing the victim's contact information
 - Hacking into victim's social networking pages
 - Sometimes escalates to personal Includes personal data, proprietary corporate information, and money



Summary

- Why Be Concerned About Network and Internet Security?
- Unauthorized Access and Unauthorized Use
- Protecting Against Unauthorized Access and Unauthorized Use
- Computer Sabotage
- Protecting Against Computer Sabotage
- Online Theft, Online Fraud, and Other Dot Cons
- Protecting Against Online Theft, Online Fraud, and Other Dot Cons

Reference



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

