PRIVACY AND CYBER SECURITY

BY: MR. MOHAMMAD TAHA SULTAN

ASSISTANT LECTURER

PUBLIC ADMINISTRATION DEPARTMENT

BASIC GOALS

- Promote cyber security awareness
- Offer self-protection techniques
- Discuss methods to secure personal information
- Provide examples of protection

CONCERNS

- Kaspersky: More than 200,000 new malware items are detected every day.
- WebARX: A study was made that stated that there is an attack every 39 seconds.
- Cybercrime is the greatest threat to every company in the world (*IBM's chairman*)

IMPORTANCE OF CYBER SECURITY

- So much of our daily lives conducted online these days.
- Every day, cyber criminals victimize people who shop, bank and send or receive money online.
- Cyber Security Affects Everyone
  - The first instance of a cyber attack was in 1903, when magician Nevil disrupted John Ambrose demonstration by sending insulting Morse code messages that were projected onto the auditorium's screen.

ONLINE ATTACKS

- The internet allows an attacker to attack from anywhere on the planet.
- Tool and methods for hacking have increased as the internet has grown and it is now much easier to attack a business or an individual in this way.

MAIN RISKS

1. Identity Theft
2. Monetary Theft
3. Web Browser
4. IM Clients
5. Web Applications
6. Excessive User Rights

THE MAIN CYBERSECURITY FACTORS

Security: We must protect our computers and data in the same way that we secure the doors to our homes.

Safety: We must behave in ways that protect us against risks and threats that come with technology.

ONLINE POPULAR THREATS:

- ## PHISHING ATTACK

  Phishing: a ‘trustworthy entity’ asks via e-mail for sensitive information such as SSN, credit card numbers, login IDs or passwords.

OTHER ONLINE POPULAR THREATS:

- Brute-force attack
- Denial-of-service DOS attack

REQUIREMENTS

Minimum cyber security requirements for a network should be as follows:

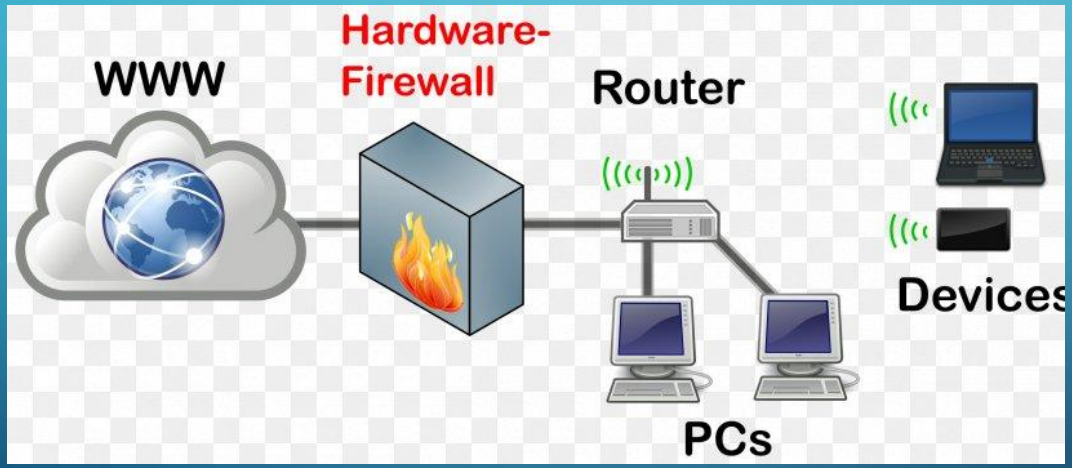
- Endpoint Protection (e.g. Passwords)
- Firewall
- Intrusion Detection System
- Encryption

PROTECTING DATA AND DEVICES

- Password:
  - DO NOT SHARE PASSWORD WITH OTHERS
  - DO NOT USE WORDS IN DICTIONARY
  - CHANGE THE PASSWORD REGULARLY
  - USE LONG PASSWORD 8 CHARACTERS AT LEAST
  - MIX
  - USE NUMBER INSTEAD OF LETTERS
    - ex: h4110 instead of hello

FIREWALL

- Barrier between the computer(s) and wider internet.



BACKUP AND UPDATE

- Backup is used to avoid data loss by making copies of the files on CDs or DVDs
- Why we use the Update?
  - New viruses created daily, antivirus must be updated.
  - Bugs(problem fixing)
  - Automatic update is used if you trust the vendor.

MALWARE

- **Malware:** Piece of Software designed with the intention of causing serious damage to the data in computer in which it is executed.

- *Forms of Malware:*

  1- Virus:

  - Small computer program that can attach it self to other program.
  - They called viruses because the act exactly as biological virus.(Hide and Spread)

FORMS OF MALWARE:

- 2-Trojan Horse:
  - Is an application, when it runs, it appears as something useful, but it will secretly perform malicious task.
- 3-Worm:
  - Similar to Trojan but it spreads across the networks.
  - Replicates it self.
  - Not necessary to attach it self to a program.

FORMS OF MALWARE

4- Spyware:

- Software that steals the data and sends it to third parties.

- Malware may infect the computer via:
  - E-mail Attachments
  - Distributing illegal software
  - Across network connections
  - Malicious web sites
  - Security holes in OS.

ANTI-VIRUS SOFTWARE

- Antivirus is used to detect and delete malware.
- The Process of removing a problem file is called disinfecting or cleaning.
- Viruses may modify important files.
- Sometimes it's impossible to remove the virus without damaging the original contents.


KASPERSKY
ANTI-VIRUS
AVG
McAfee
bitdefender
secure your every bit
F-Secure
INTERNET SECURITY SUITE 2010
Microsoft
Security Essentials
avast!
be free
AVIRA
eset
NOD32
antivirus

AVOID HACKER TRICKS

- Be sure to have a good firewall or pop-up blocker installed.
- Never click “yes,” “accept” or even “cancel.”
- Infected USB drives are often left unattended by hackers in public places.

TIPS FOR PROTECTING YOUR PRIVACY AND SECURITY

- Limit what you share on social media and online in general.
- Safeguard your data and devices.
- Become more aware of how your personal information, once shared online, is no longer in your control.

Questions?