جامعة بوليتكنك فلسطين

COMPUTER SECURITY AND PRIVACY

Prepared by:

Eng. Yousef Salah

Eng. Mohammad Jabari

This material developed under the objectives of FESTEM project funded by the EU.
https://festem.ps/

Co-funded by the Erasmus+ Programme of the European Union

CHAPTER FIVE
COMPUTER SECURITY AND PRIVACY

PREFACE:

This chapter shows an overview about computer security, risks and threats specially while involving online activities. It covers the primary tools and countermeasures on how to protect computing systems and ensure authorized accessed. The chapter also discusses malware programs and cyberattack techniques. Additionally, it emphases on certain topics and issues related to ethics, privacy and encryption.

INTENDED LEARNING OUTCOMES:

After completing this chapter students will be able to:

1) Provide introduction about computer security, attacks and crimes.
2) List several examples of unauthorized access and unauthorized use and explain several ways to protect against them.
3) Identify the main types of malware and differentiate among these types.
4) Describe some cybercrime ways, and provide examples of online protection systems.
5) Discuss related security topics terminologies like: computer ethics, encryption, mobile apps security and privacy.

FURTHER READING:

1) Discovering Computers ©2018: Digital Technology, Data, and Devices.
2) Computing Essentials 2017-McGraw-Hill (2017) Daniel O'Leary, Linda I. O'Leary, Timothy J O'Leary.
3) Understanding Computers Today And Tomorrow Comprehensive, Deborah Morley, Charles S. Parker - Cengage Learning, (2016).

WHAT IS A COMPUTER SECURITY

- ***Security*** involves protecting individuals and organizations from theft and danger.

- ***Computer security*** focuses on protecting information, hardware, and software from unauthorized use.

- ***Computer crime*** includes any illegal act involving a computer or a computer network.
- C***ybercrime*** is an Internet-based crime.

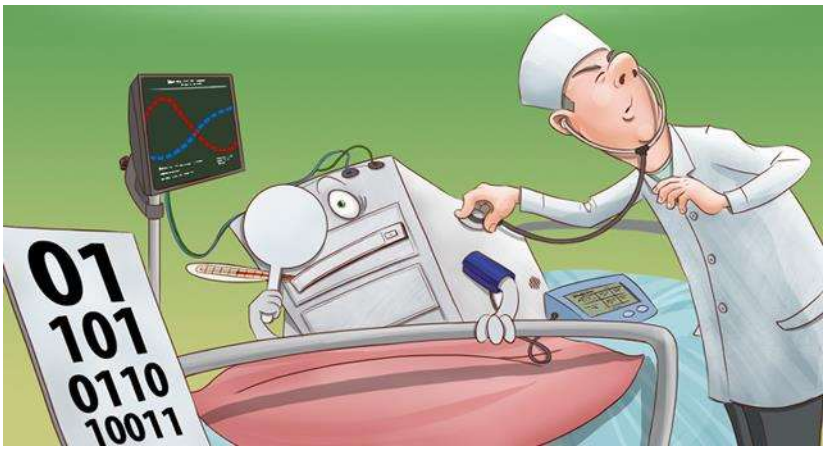
- A ***Hacker*** (or ***Attacker***) is a technically skilled person who tries to get unauthorized access or to perform illegal task within a computer system or a network.

- A hacker exploits the vulnerabilities and weaknesses of a computer system to harm a computer or perform illegal actions like:
  - Distributing malicious programs.
  - Stealing data and identity theft.
  - Internet scams.
  - Cyberbullying and blackmailing.
  - Sabotage a computer system.

MALWARE

- Malware is a program that has malicious intent.
- When a malware executes, it will damage or disrupt a computer system, or will steal private information.

- Some symptoms of malware infection:
  - Your computer is slowing down.
  - Annoying ads are displayed.
  - System Crashes.
  - Pop-up messages.
  - Internet traffic increases.
  - Lack of storage space.
  - Your browser homepage changed.
  - Unusual messages show unexpectedly.



Activity:

Had your system ever infected by a malware? What symptoms appeared to your system?

- The most common types of malware are:
  - Viruses.
  - Worms.
  - Trojan horses.
  - Spyware.
  - Ransomware.

Viruses

- A virus is a malware program that attaches and replicates itself to other programs or files.
- Computer viruses are often embedded into program or data files (such as software, games, videos, music files and documents).
- When a virus runs, it harms your system, causes damage, affects performance, or even monitors your activities.
- Most viruses comes through an infected removable storage medium, or via an email attachement or a webpage link clicked by the user.

- Antivirus Software:

- A software that detects and removes viruses.
- The antivirus software should be updated continuously to be notified by latest viruses in the world, so that it can discover virus threats when get into your computer.
- Most common antivirus programs are: Kaspersky, Avast, McAfee, ….

Activity:

What other Antivirus software are common? Are they free software?

Worms

- Worm is a malicious program that copies itself repeatedly, for example in memory or on a network, using up computing resources and possibly shutting down the computer, device, or network.
- Worms differ from viruses in that they do not need to attach themselves to other files or programs. Worms are stand-alone malicious programs that can self-replicate and propagate independently as soon as they have breached the system.

Trojan Horses

- Do you know the Story of Troy?
- Trojan horse is a malicious program that hides within or looks like a legitimate program. Unlike a virus or worm, a trojan horse does not replicate itself to other computers or devices.
- Many recent Trojans trick the user by inviting him to a normal ongoing activities (such as the Windows Update service or a warning from a security program or buying a useless program).
- A Trojan horse uses Social Engineering to trick the user.

- What is Social Engineering?

- Social Engineering is a psychological action used by a hacker to deceive the user by offering him an appealing service to get private information, or to catch his acceptance to run a malware program.

- Social Engineering uses emotional aspects to let a user reveals his private information like usernames, passwords, credit card numbers, …..

Activity:

What Social Engineering examples you faced through the Internet?

Spyware

- A spyware is a malware program that monitors and spies on his victim.
- It secretly collects information about the user and sends it to outside source while the user is online.
- A Spyware runs in the background to record user keystrokes (what a user types on the keyboard), which means that the attacker can view passwords that the victim enters into the computer.
- There are Antispyware programs that can detect and remove spyware.

Ransomware

- Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid.

MORE ON CYBERATTACKS

- Cyberattack is any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to an online system.
- We'll cover some of cyberattacks like:
  - Phishing Attacks.
  - DoS attacks.
  - Passwords Attacks.

Phishing

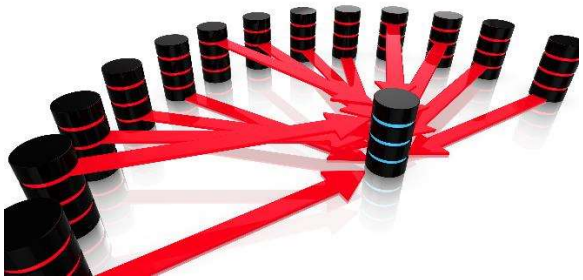
- Phishing is a way of deceiving a user through fake website or email that looks well-known or legitimate.
- Phishing is an Internet scam which tries to steal financial private data, login information, or sensitive personal information.

- Phisher may design a website that look official to let you input or update your private information to steal you.

- To avoid Phishing, when inputting sensitive information, be care of the URL of the webpage you are browsing, and make sure it is the official trusted site.

DoS (Denial of Service) Attacks

- Denial of Service (DoS) Attack overwhelms a server by requests to stop the service and shuts it down for the legitimate users.
- Usually requests come from thousands of computers at the same time.



Password Attacks

- A Password Attack involves trying to steal user's login information.
- Common approaches of Password Attack are:
  - **Brute-force attacks**

    A hacker uses a computer program or script to try to log in with possible password combinations, usually starting with the easiest-to-guess passwords.

  - **Dictionary attacks**

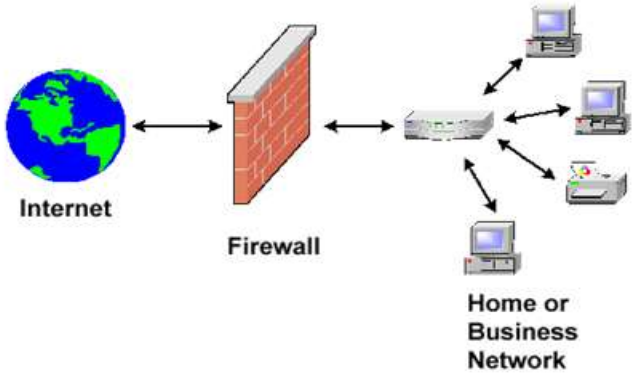
    A hacker uses a program or script to try to login by cycling through combinations of common words from a dictionary.

  - **Social Engineering attacks**

    Someone might be trying to know your password by socializing with you emotionally to get it.

WHAT IS A FIREWALL

- A firewall is a network security system, it protects network resources from intrusions.
- Based on a set of rules, a firewall checks all incoming (from the Internet) and outgoing (to the Internet) traffic, and allows only authorized traffic to pass through the firewall.
- A firewall may be hardware system or software.



SECURITY COUNTERMEASURES

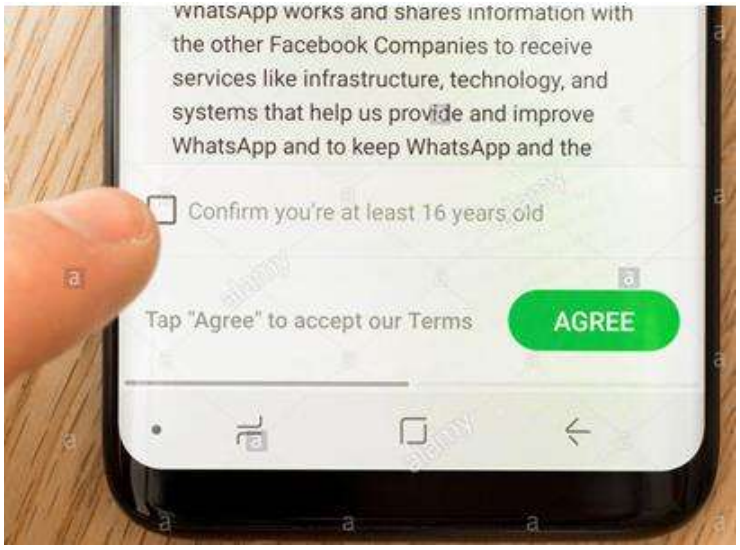
- Countermeasures are preventive procedures and awareness tips that guide the user to be protected and safe against a danger or a threat.
- Main security countermeasures are:
  - Secure your computer: update your operating system and use up-to-date security (antivirus, antispyware, firewall, etc.) software.
  - Be suspicious of unsolicited email attachments.
  - Scan removable media for malware before using it.
  - Back up your data regularly.
  - Use strong passwords, change them regularly, and never give it to others.
  - Download files from trusted websites or mobile stores.
  - Verify sources before sharing sensitive information—never respond to e-mail or phone requests for sensitive information.
  - Avoid putting too many personal details on your Web site or a social media site.
  - Avoid using location-based services that share your location information with strangers.
  - When using a public computer, make sure to delete any personal data or settings before leaving a computer.

PRIVACY

- Privacy is related to what information about individuals is available, how it is used, and by whom.
- **Information privacy** refers to the right of individuals and companies to deny or restrict the collection, use, and dissemination of information about them.

MOBILE APPS SECURITY AND PRIVACY

- The widespread use of mobile devices "apps" raises some serious security and privacy concerns.
- Some Mobile apps may collect data about their users with or without their consent.
- "apps" if given permission, can collect data about your contact list, photos, location, etc..
- It's important to take into account the permission every app asks for before installation.



Activity:

How mobile apps may violate user privacy?

How social media affects privacy?

- Social media sites like Facebook, Twitter, and Instagram, know about you more than you can imagine.
- It knows where you live, whom are your friends, when you plan your next trip, what you like and not like, what you have bought, and much much more!
- You are giving away all these information about yourself for free.
-

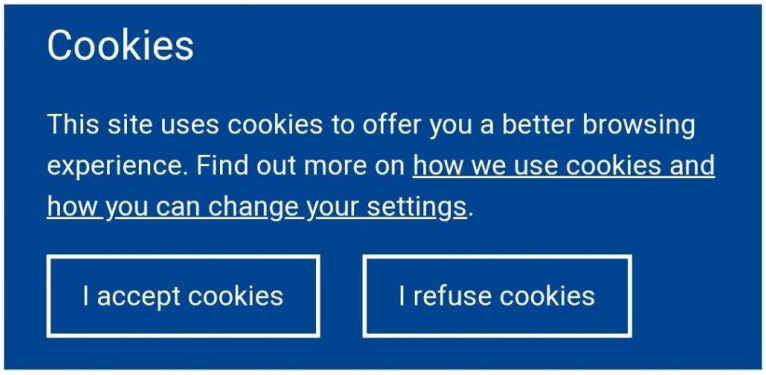
Part of Facebook Privacy Statement

- **Networks and connections.** We collect information about the people, Pages, accounts, hashtags and groups you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups you are part of. We also collect contact information if you choose to upload, sync or import it from a device (such as an address book or call log or SMS log history), which we use for things like helping you and others find people you may know and for the other purposes listed below.
- **Your usage.** We collect information about how you use our Products, such as the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your activities. For example, we log when you're using and have last used our Products, and what posts, videos and other content you view on our Products. We also collect information about how you use features like our camera.

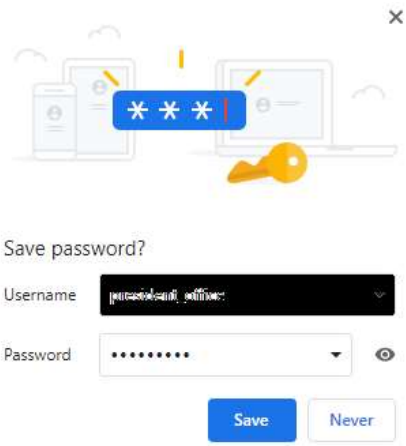
- Be care about what you provide on the Internet.
- You are liable about the content you put while you are online, and you may be consequently prosecuted.

- Even if you used an anonymous way of hiding yourself, then you for sure are religiously questionable.

Cookies and Privacy:

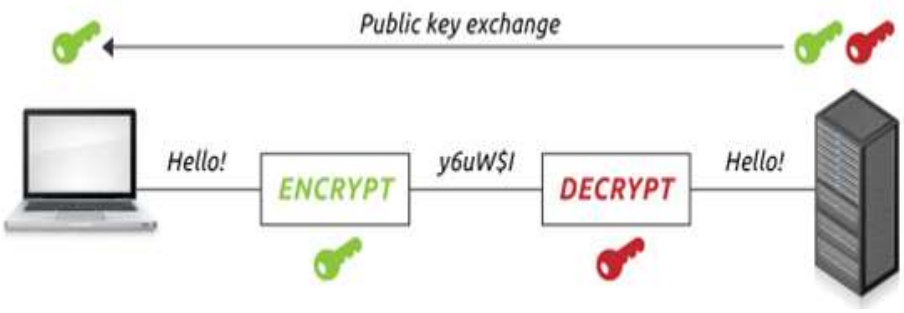


- Cookies are small data files that are saved on your hard disk from websites you have visited.
- Cookies allow these websites to remember you when you visit them next time.
- Based on your browser's settings, these cookies can be accepted or blocked.
- For example, they do not ask you for your "username" and "password" if you check the box "keep me logged in" previously.
- Cookies are useful, but sometimes they are dangerous.
- Some Websites use Cookies to track users browsing history, behavior and preferences.
- Tracking cookies can be used to display Web page ads based on your browsing activities.
- For example if you visited a website that sells Cameras, next time, when you visit Facebook or other websites you will see ads about Cameras, or even your will see ads about the same Camera model you were looking for on that site.



Encryption:

- Data over the Internet, is by default, sent as unencrypted plaintext (*human readable*).
- ***Encryption*** is the process of converting data that is readable by humans into encoded characters to prevent unauthorized access.
- For example, users may specify that an email application encrypt a message before sending it securely.



Activity:

How **"https"** protocol differs from **"http"** protocol?

COMPUTER ETHICS

- Computer ethics are guidelines for the morally acceptable use of computers in our society.
- Common computer ethics involved in:
  - Intellectual Property rights.
  - Internet and Information Privacy.
  - Code of conduct.
  - Green Computing.
  - Plagiarism.

Sample IT Code of Conduct

1. Technology may not be used to harm other people.
2. Employees may not meddle in others' files.
3. Employees may use technology only for purposes in which they have been authorized.
4. Technology may not be used to steal.
5. Technology may not be used to bear false witness.
6. Employees may not copy or use software illegally.
7. Employees may not use others' technology resources without authorization.
8. Employees may not use others' intellectual property as their own.
9. Employees shall consider the social impact of programs and systems they design.
10. Employees always should use technology in a way that demonstrates consideration and respect for fellow humans.

Discussion:

- How do companies like Google and Facebook make money?

- How a firewall protect my computer against intruders?

- If you received an email from your bank asking you to change your password for security reasons, what should you do?

- What is **CAPTCHA**, and what is supposed to achieve?