MODERN DIGITAL SKILLS

CHAPTER 13: DIGITAL SAFETY & CYBER SECURITY

CONTENTS

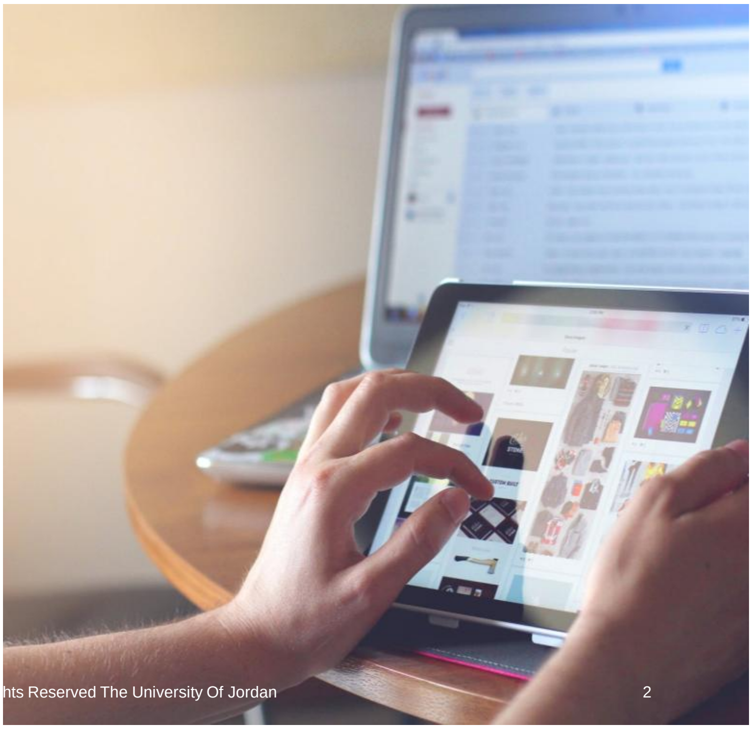
1. Introduction to cybersecurity
   - Definition and Goal
   - Basic Cybersecurity concepts
   - Cybercrime
   - Cyber Threats

2. Malware: definition and types

3. Cyber Security Breaches

4. Cyber Attacks

5. Digital / Cyber safety tips - Prevention Tips



Cyber Security
Introduction

With the rise of the **digital age** around the world, a large number of organizations are doing their business online via the internet .

- This makes processes **easier** and **more efficient**. ☺
- But may cause the following **security problems**: ☹
  - **Hacking** threats
  - **Unauthorized access** to sensitive information.

Therefore, the imperative for cybersecurity emerges.

***cybersecurity** is very important to prevent these problems and protect important data.*

Role of Cybersecurity: it acts as a protective shield between users and cybercriminals, ensuring data and systems remain safe from unauthorized access or changes

Definition and Goal

✓ **Cyber Security**

- is the collection of methods, tools, and procedures used to protect against threats, attacks, and unauthorized access to networks, computers, programs and data.

✓ **Cyber security Goal in the digital age** :

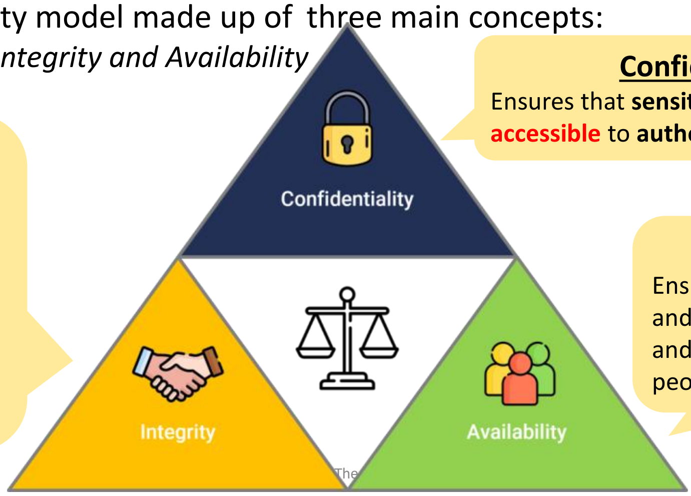
- Protecting Data from unauthorized access or alter
- Protecting resources(such as devices, staff, apps, services, and communication systems) from risks and keep them safe and secure.

✓ **Cybersecurity is also known as**:

- Information security (INFOSEC),
- Information assurance (IA)
- System security.

Basic Cyber Security Concept

- The foundation of cybersecurity basics lies in the **CIA** triad which refers to an information security model made up of three main concepts:
  - *Confidentiality, Integrity and Availability*



Integrity:
Maintain the accuracy, consistency, and reliability of data and systems by **Protecting** them from being **altered, modified** or **corrupted** by **unauthorized** people

Confidentiality:
Ensures that **sensitive information** is **only accessible** to **authorized** individuals.

Availability:
Ensures that information and systems are **available** and **accessible** by right people when needed.

Cybercrime

What is Cybercrime?

- **Cybercrime:** the illegal use of communication devices to commit or help in committing illegal acts.
- **Cybercrime examples**:
  - Hacking
  - Identity theft
  - Fraud
  - Phishing
  - Malware distribution
  - Cyberstalking
  - Online harassment

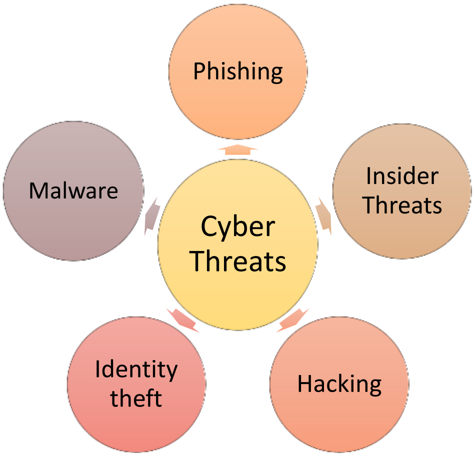
Who are Cybercriminals?

- **Cybercriminals:** people who use technical skills to commit illegal acts.
- **Examples:**
  - Hackers
  - Stalkers
  - Scammers

Cyber Threats

Cyber threats:
A wide range of risks that can:

1. **Exploit weaknesses** in computer systems, networks, or data.
2. Make it **possible to harm** or disrupt digital assets.
3. **Lead to actual cyberattacks**, depending on whether there are preventive tools in place to reduce or eliminate the threat.



Cyber Threats

Phishing

Insider Threats

Hacking

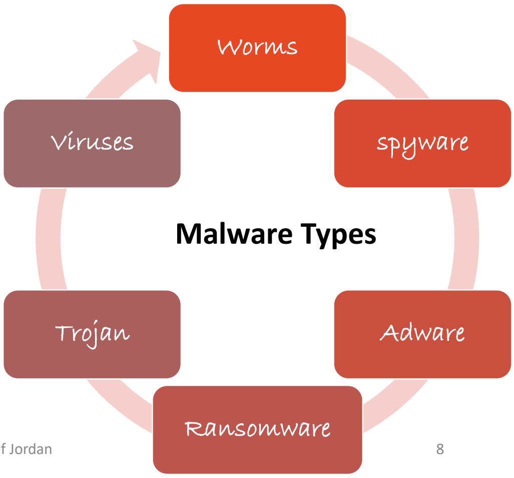
Identity theft

Malware

Types of Cyber threats:

Cyber Threats
Malware Definition

- **Malware** (or "**Malicious Software**.“) : It is a type of software created by cybercriminals to **disrupt** or **damage** a user's computer.
- **Cybercriminals use malware to:**
  - Make money (e.g., through theft or fraud)
  - Conduct politically motivated cyber-attacks.
- **Common Distribution Methods of Malware**:
  - *Unwanted or unexpected Email* ***Attachments****.*
  - *Hidden in Legitimate-Looking* ***Downloads*** *(Downloads that appear safe).*



Worms

spyware

Adware

Ransomware

Trojan

Viruses

Malware Types

Cyber Threats
Malware Types

1. **Viruses:** programs that cause corrupting data, stealing information ,deleting files, forcing reboots or damaging the system.

2. **Worms:** Worms infect systems directly and reside in memory, where they self-replicate and spread to other systems on the network.

3. **Trojans:** are malware disguised as legitimate software or files to trick users into downloading and executing them.

4. **Ransomware** :locks down a user’s files and data, with the threat of erasing it unless a ransom is paid.

5. **Spyware :** secretly monitor and collect information about a user's activities, such as keystrokes, browsing history, and personal data.

6. **Adware** is software that displays unwanted advertisements or pop-up windows on a user's computer which compromise user privacy.

Cyber Attacks

Cyber attacks:

- deliberate and malicious actions carried out by individuals or organizations with the intent to compromise, disrupt, damage, or gain unauthorized access to computer systems, networks, or data.
- are the actual execution of cyber threats.

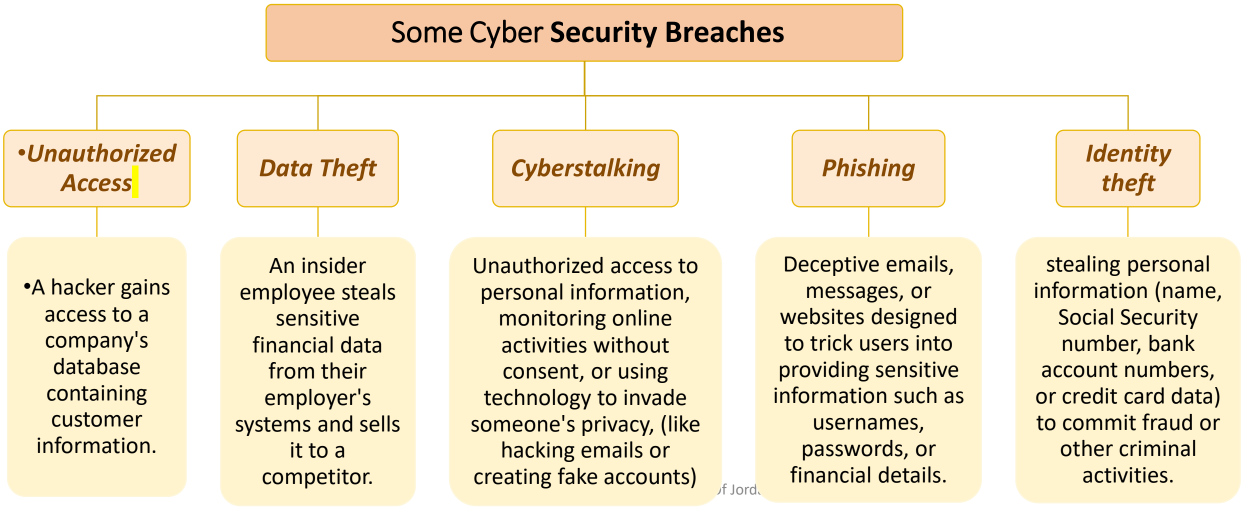
Example:
Man-in-the-Middle (MitM) attacks : The attacker is positioned in the “middle” of the two parties. He can spy on their communication and modify messages before sending them.

Cyber Security Breaches

- **Cyber security breach** is a case where an unauthorized person gains access to a computer system, network, or data without permission.

- Breaches can happen **because of Malwares** that takes advantage of weaknesses in systems or software. This allows attackers to:
  - *Gain unauthorized access*
  - *Steal sensitive information*
  - *Compromise the integrity of the system*

Cyber Security Breaches



Some Cyber **Security Breaches**

•Unauthorized Access

•A hacker gains access to a company's database containing customer information.

Data Theft

An insider employee steals sensitive financial data from their employer's systems and sells it to a competitor.

Cyberstalking

Unauthorized access to personal information, monitoring online activities without consent, or using technology to invade someone's privacy, (like hacking emails or creating fake accounts)

Phishing

Deceptive emails, messages, or websites designed to trick users into providing sensitive information such as usernames, passwords, or financial details.

Identity theft

stealing personal information (name, Social Security number, bank account numbers, or credit card data) to commit fraud or other criminal activities.

Digital / Cyber safety tips - Prevention Tips

Cyber safety tips:

- ✓ **Use Secure Wi-Fi Networks:** Reduces the risk of data interception and unauthorized access.
- ✓ **Practice Safe Social Media Usage:** Adjusting privacy settings and being cautious about sharing personal information on social media.
- ✓ **Backup Your Data Regularly:** ensures that important files can be recovered in case of data loss or ransomware attacks.
- ✓ **Use Strong and Unique Passwords:** creating strong passwords to protect accounts from unauthorized access.
- ✓ **Do not open email attachments from unknown senders:** These could be infected with malware.
- ✓ **Use anti-virus software**.