Cybersecurity Module- Week 1: Introduction to Cybersecurity

Objective:

- Understand what cybersecurity is and why it is important.
- Identify common threats and risks in the digital world.
- Recognize the role of individuals and organizations in maintaining cybersecurity.

1. What is Cybersecurity?

Cybersecurity is the practice of protecting computers, networks, programs, and data from unauthorized access, attacks, or damage.

Key Concepts:

Confidentiality: Only authorized users can access data

Integrity: Data cannot be altered without permission

Availability: Data and systems are accessible when needed

Example:

Your online banking information should remain confidential, accurate, and always accessible when you log in.

Importance of Cybersecurity

- Protects sensitive information: personal, financial, and corporate data
- Prevents identity theft and fraud
- Maintains trust in online systems and digital services
- Ensures continuity of business operations

Real-Life Scenario:

A hospital stores patient records digitally. If these are hacked, patients' private information is exposed, violating confidentiality and trust.

Common Cybersecurity Threats

Threat	Description	Example	Prevention
Malware	Software designed to harm systems	Viruses, ransomware	Antivirus, software updates
Phishing	Fake messages to steal information	Emails claiming bank issues	Verify source, don't click links
Hacking	Unauthorized system access	Breaking into social media accounts	Strong passwords, firewalls
Social Engineering	Manipulating people to reveal info	Impersonating IT support	Educate users, verify identity
Insider Threat	Harm caused by employees	Employee leaking data	Access control, monitoring

Example Scenario:

Juan clicks a fake email link and his account is hacked. This is phishing combined with malware.

Types of Cybersecurity Threats

1. External Threats: Hackers, malware, phishing attacks

2. Internal Threats: Employees, contractors, or insiders misusing access

3. Advanced Persistent Threats (APT): Long-term attacks on organizations

4. Zero-Day Exploits: Attacks on previously unknown vulnerabilities

Activity / Exercise:

List 5 cybersecurity threats you have experienced online or know about and suggest one way to prevent each.

Case Study

Scenario:

A company receives a ransom-ware email. Employees click it, encrypting files.

Analysis:

Threat: Ransomware (malware)

Cause: Clicking suspicious link (human factor)

Prevention: Employee training, antivirus software, data backup

Discussion Questions:

1. How could the company have avoided the attack?
2. What immediate steps should be taken after infection?
3. What long-term security measures should be implemented?

Cybersecurity Roles for Individuals and Organizations

Individuals:

Use strong passwords and MFA

Keep software updated

Avoid suspicious links and emails

Organizations:

Implement firewalls, VPNs, and intrusion detection

Train employees regularly

Backup data regularly

Example:

Maria uses MFA on her email and a VPN on public Wi-Fi. The company installs intrusion detection systems to monitor network traffic.

Summary

- Cybersecurity protects data, networks, and systems from threats.
- Core principles: Confidentiality, Integrity, Availability (CIA)
- Threats include malware, phishing, hacking, social engineering, and insider threats.
- Both individuals and organizations play a role in maintaining cybersecurity.

Homework

1. Research a recent cybersecurity attack and explain:

Type of attack

Victim

Consequences

Prevention measures

2. Create a diagram showing 5 types of cybersecurity threats with examples.