Cybersecurity Module- Week 4: Cybersecurity Best Practices

Objective:

- Learn how to protect devices, data, and networks.
- Implement strong cybersecurity habits in daily life.
- Reduce the risk of cyber attacks through preventive measures.

Introduction

Cybersecurity is only effective when users actively apply best practices. Technology alone is not enough—human behavior and proper procedures are equally important.

Key Concept:

- Cybersecurity is a combination of technology, policies, and awareness.

Cybersecurity's Best Practices

1. Password Management

Definition: Using strong, unique passwords to protect accounts and devices.

Tips:

- Include letters, numbers, symbols
- Avoid common words or dates
- Use a different password for each account
- Use password managers to securely store credentials

Example:

Strong: S3cure!P@ss2025

Weak: password123

Scenario:

Maria uses a strong password for her email and a unique one for her online bank. A hacker cannot guess both, reducing risk of account compromise.

2. Multi-Factor Authentication (MFA)

Definition: Adds an extra layer of verification beyond just a password.

Examples:

SMS codes

Authentication apps

Biometric verification (fingerprint, facial recognition)

Scenario:

Juan logs into his work email. After entering his password, he receives a code on his phone. Even if a hacker knows his password, they cannot access his account without the code.

Diagram:

Login Process with MFA

[Password] → [Verification Code / Biometric] → Access Granted

3. Software Updates

Definition: Regularly updating operating systems, apps, and security software to fix vulnerabilities.

Importance:

Prevents exploitation of outdated software

Improves system performance and security

Example:

A company updates its email client to fix a security flaw. Hackers cannot exploit the old vulnerability.

Scenario:

Juan ignores update prompts for his laptop. Malware targets a known vulnerability and infects his system.

4. Secure Networks

Definition: Ensuring that internet connections are safe from intruders.

Tips:

Avoid public Wi-Fi for sensitive transactions

Use Virtual Private Networks (VPNs) for encryption

Enable firewalls to filter malicious traffic

Example:

Maria works from a café. She uses a VPN to encrypt her internet traffic, preventing hackers on public Wi-Fi from intercepting her data.

5. Data Backup

Definition: Keeping copies of important data to prevent loss from attacks or accidents.

Types of Backup:

Cloud Backup: Stores data online (Google Drive, Dropbox)

External Backup: Uses USB drives, external hard drives

Example:

Juan's laptop is infected by ransomware. Because he has a cloud backup, he restores his files without paying the ransom.

Scenario:

A small business performs daily backups to prevent loss of client data during system crashes or cyber attacks.

Case Study

Scenario:

A company suffers a ransomware attack. Systems are encrypted, and employees panic. Because the company has:

1. Regular backups
2. MFA on all accounts
3. Updated antivirus software

They restore operations quickly without paying the ransom.

Discussion Questions:

1. Which best practices helped mitigate the attack?
2. How could employee training further prevent such incidents?
3. What lessons can individuals learn from this case?

Summary

- Cybersecurity best practices protect against threats proactively.
- Key practices include:
- Password management: strong, unique password
- Multi-factor authentication (MFA): extra layer of security
- Software updates: patch vulnerabilities
- Secure networks: VPNs, firewalls, avoid public Wi-Fi
- Data backup: recover from attacks without loss
- Combining technology, awareness, and discipline reduces cyber risks significantly.

Homework

1. Create a personal cybersecurity checklist with at least 5 best practices you will implement.
2. Research a ransomware incident and explain:

How backups and MFA could have minimized the impact

Lessons for businesses and individuals

3. Draw a diagram showing the layered approach to cybersecurity, including devices, networks, applications, and data.