




# Cybersecurity Module- Week 2: Types of Cybersecurity

## Objective:

-  Understand the different types of cybersecurity.
-  Identify how each type protects systems and data.
-  Apply knowledge to real-world scenarios.

## Introduction

Cybersecurity is not a single solution but a combination of strategies protecting networks, devices, applications, and data. Each type of cybersecurity focuses on a specific area.

## Key Concept:

A layered approach is essential for robust protection.

Visual Diagram:

## Types of Cybersecurity

1. Network Security
2. Information Security (InfoSec)
3. Application Security
4. Cloud Security
5. Endpoint Security

### 1. Network Security

Definition: Protects computer networks from unauthorized access, attacks, and misuse.

Key Tools:

Firewalls: Block unauthorized access

Intrusion Detection Systems (IDS): Monitor suspicious activity

Virtual Private Networks (VPN): Encrypt data transmission

Example:

A company uses a firewall and VPN so employees can safely access files remotely without exposing sensitive data.

Scenario:

Hacker attempts to access the company's internal network. The firewall blocks the intrusion, preventing a data breach.

## **2. Information Security (InfoSec)**

Definition: Protects the confidentiality, integrity, and availability of information, whether digital or physical.

Key Practices

Encryption: Converts data into unreadable format for unauthorized users

Access Control: Grants permissions only to authorized personnel

Backup: Maintains copies of data in case of loss

Example:

Banks encrypt customer account information so even if intercepted, it cannot be read by hackers.

Scenario:

Maria's school stores student grades in a secure database. Only authorized staff can access it, ensuring privacy and accuracy.

## **3. Application Security**

Definition: Protects software applications from vulnerabilities throughout their lifecycle.

Key Practices:

Secure coding: Avoids common security flaws

Regular updates and patches: Fixes vulnerabilities

Application firewalls: Protects apps from attacks

Example:

An online shopping website regularly updates its software to prevent hackers from exploiting outdated features.

Scenario:

A hacker tries SQL injection to access a database. Proper input validation in the application prevents unauthorized access.

#### **4. Cloud Security**

Definition: Protects data stored in cloud services from cyber threats and unauthorized access.

Key Practices:

Strong authentication and passwords

Encryption for data in transit and at rest

Regular monitoring and audits

Example:

A company storing customer files on Google Drive uses two-factor authentication and file encryption to ensure safety.

Scenario:

Hackers attempt to steal cloud data, but multi-factor authentication prevents them from logging in.

## **5. Endpoint Security**

Definition: Protects devices such as computers, smartphones, and IoT devices from attacks.

Key Practices:

Antivirus and anti-malware software

Device encryption

Regular updates and patches

Example:

Juan installs antivirus software on his laptop and phone to detect and prevent malware.

Scenario:

Malware targets an employee's laptop, but endpoint security software detects and isolates the threat before spreading to the company network.

### **Case Study**

Scenario:

A multinational company experienced a data breach after an employee used an unprotected device to access the internal network.

Analysis:

Threat: Malware on unprotected endpoint device

Solution: Implement endpoint security, network firewalls, and employee training

Lesson: Multiple layers of cybersecurity are essential

### **Discussion Questions:**

1. Which types of cybersecurity could have prevented this breach?
2. How do network and endpoint security complement each other?
3. Why is encryption important in both InfoSec and cloud security?

## **Summary**

- Cybersecurity is multi-layered; each type protects a specific area.
- Network Security: Protects data in transit and connections
- InfoSec: Protects data's confidentiality, integrity, and availability
- Application Security: Secures software from vulnerabilities
- Cloud Security: Protects online stored data
- Endpoint Security: Secures individual devices
- A combination of these types forms a strong defense against cyber threats.

## **Homework**

1. Create a diagram showing 5 types of cybersecurity, with one example of a tool or practice for each.
2. Research a real-world data breach and identify which types of cybersecurity could have prevented it.
3. Write a one-paragraph reflection on which type of cybersecurity you think is most important for daily use and why.