Introduction to Cyber Security

Cybersecurity is the practice of protecting computer systems, networks, programs, and data from unauthorized access, attacks, or damage.
It ensures that digital information remains **confidential, accurate, and available** to authorized users.

It covers protection from:

a. Hacking

- Definition: The act of exploiting system vulnerabilities to gain unauthorized access to computers or networks.
- Goal: Steal data, alter files, or use systems for further attacks.

---

b. Phishing

- Definition: A social engineering attack where cybercriminals trick users into revealing personal information (like passwords or credit card details) by pretending to be a trusted entity (e.g., bank, company, friend).

- Example: A fake email from “PayPal” asking you to verify your account.
  Goal: Steal credentials, financial data, or install malware.

---

c. Ransomware

- Definition: A type of malware that encrypts a victim's data and demands payment (ransom) to restore access.

- Example: The WannaCry attack (2017) affected hospitals, banks, and companies worldwide.

d. Data Breaches

- Definition: Unauthorized access, disclosure, or theft of confidential data from a system or network.

- Causes: Weak passwords, malware, insider threats, or poor security configurations.

- Example: Personal information like credit card numbers or health records leaked online.

e. Service Disruption (DDoS Attacks)

- **Definition: Distributed Denial of Service (DDoS)** attacks flood a target's server or network with massive traffic, making it slow or unavailable.
- **Example:** A website crash during a DDoS attack using thousands of infected computers (botnets).

Cybersecurity operates across multiple layers and they have different scopes :

1. Network Security – Protecting Data During Transmission

- **Definition:** Safeguards the integrity, confidentiality, and availability of data as it moves across networks.
- **Focus:** Prevent unauthorized access, misuse, or disruption of network resources.
- **Techniques: Firewalls, intrusion detection/prevention systems (IDS/IPS), VPNs, encryption, and network segmentation.**
-
- **Example:** Using SSL/TLS to secure data transfer between a browser and a web server.

---

2. Application Security – Securing Apps from Vulnerabilities

- **Definition:** The process of making applications more secure by finding, fixing, and preventing security flaws.
- **Focus:** Protect software from attacks such as SQL injection, XSS (Cross-Site Scripting), or buffer overflows.
- **Techniques:** Secure coding practices, input validation, authentication, and regular patching.
- **Example:** Implementing two-factor authentication in a web app.

---

3. Information Security – Protecting Data Storage and Integrity

- **Definition:** Ensures data confidentiality, integrity, and availability, whether it's stored digitally or physically.
- **Focus:** Prevent unauthorized access, alteration, or destruction of data.
- **Techniques:** Encryption, access control, backup systems, and data classification.
- **Example:** Encrypting sensitive files on a company server.

---

4. Cloud Security – Protecting Cloud-Stored Data and Infrastructure

- **Definition:** A set of technologies and policies designed to protect cloud-based systems, data, and infrastructure.
- **Focus:** Prevent data breaches and unauthorized access in cloud environments.
- **Techniques:** Encryption, identity and access management (IAM), secure APIs, and compliance checks.
- **Example:** Using AWS Identity and Access Management (IAM) to control user permissions.

---

5. IoT Security – Securing Connected Devices

- **Definition:** Protecting Internet of Things (IoT) devices and the networks they connect to from cyber threats.
- **Focus:** Secure data communication and prevent exploitation of device vulnerabilities.
- **Techniques:** Device authentication, firmware updates, data encryption, and network monitoring.

- **Example:** Securing smart home devices like cameras or thermostats from remote hacking.

---

6. Cyber Law and Policy – Legal Frameworks Governing Cyberspace

- **Definition:** The set of laws, regulations, and policies that define legal behavior in cyberspace.

Sample Questions & Answers

Q1. What is Cybersecurity?
A: Cybersecurity is the practice of defending computers, servers, mobile devices, networks, and data from malicious attacks or unauthorized access.

Q2. Why is cybersecurity important today?
A: Because our personal, financial, and business activities are heavily dependent on digital technologies, and any breach can lead to massive losses and privacy violations.

Q3. Mention three main areas where cybersecurity is applied.
A: Network security, information security, and application security.

CIA Triad: Core Principles of Cyber Security

The **CIA Triad** represents the **three foundational principles** of information security:

- **Confidentiality**

- **Integrity**
- **Availability**

These principles guide security policies and strategies in every organization.

---

1. Confidentiality

Definition:
Ensuring that information is **accessible only to authorized users** and kept secret from unauthorized access.

Example:
Encryption, user authentication, and access control lists protect confidentiality.

---

2. Integrity

Definition:
Ensuring the **accuracy, completeness, and consistency** of data over its entire lifecycle.

Example:
Hash functions, digital signatures, and checksums verify data has not been altered.

---

3. Availability

Definition:
Ensuring that information and systems are **accessible and functional** when required by authorized users.

Example:
Redundant systems, backups, and DDoS protection improve availability.

In short :

Confidentiality → Who can see the data

Integrity → Is the data correct and unchanged

Availability → Can authorized users access it when needed

Sample Questions & Answers :

Give one example of a threat to integrity.

Ans : Unauthorized modification of financial data by a hacker.

Overview of Cybercrime

Cybercrime refers to criminal activities that involve a computer, network, or digital device as the target, tool, or both.

Goal :Damage systems or data, Spread malware, Disrupt services

Cybercrimes can be categorized into:

1.Crimes against Individuals : Identity theft, cyberstalking, phishing, online harassment.

2.Crimes against Property: Hacking, data theft, malware attacks, ransomware.

3.Crimes against Government or OrganizationsCyberterrorism, espionage, denial of service attacks.