What is Cyber security?

Cyber security is the practice of protecting computers, servers, mobile devices, networks, and data from digital attacks, theft, and unauthorized access. It involves implementing technologies, processes, and controls to secure systems and mitigate cyber threats.

Key Objectives of Cyber security

1. **Confidentiality** – Ensuring that data is accessible only to authorized users.
2. **Integrity** – Preventing unauthorized changes to data.
3. **Availability** – Ensuring that systems and data remain accessible when needed.

Types of Cyber security

1. **Network Security** – Protecting networks from unauthorized access, malware, and attacks.
    - Example: Firewalls, Intrusion Detection Systems (IDS).
2. **Information Security** – Safeguarding sensitive data from breaches and leaks.
    - Example: Encryption, Access Control.
3. **Application Security** – Securing software and applications from cyber threats.
    - Example: Secure coding practices, penetration testing.
4. **Cloud Security** – Protecting cloud-based applications and services.
    - Example: Multi-factor authentication (MFA), Data encryption.
5. **Operational Security** – Managing data access and security policies.
    - Example: Role-based access control (RBAC).
6. **IoT Security** – Protecting internet-connected devices from cyber threats.
    - Example: Secure firmware updates, Authentication mechanisms.

Common Cyber Threats

1. **Malware** – Harmful software like viruses, ransom ware, and spyware.
2. **Phishing** – Fake emails or websites that steal user credentials.
3. **Denial of Service (DoS) Attacks** – Overloading a system to make it inaccessible.

4. **Man-in-the-Middle (MitM) Attacks** – Intercepting communication between users.
5. **SQL Injection** – Injecting malicious SQL code to access databases.
6. **Zero-Day Exploits** – Attacking software vulnerabilities before they are patched.

Cyber security Best Practices

1. Use **strong passwords** and enable **multi-factor authentication (MFA)**.
2. Keep **software and systems updated** with security patches.
3. Install **antivirus and firewall** for protection against threats.
4. Avoid **clicking on suspicious links** or downloading unknown files.
5. Encrypt sensitive data and use **secure backups**.
6. Use **VPNs** when accessing public Wi-Fi.

Cyber security is crucial in today's digital world to protect individuals, businesses, and governments from cyber-attacks and data breaches.