📘

Unit 1: Overview of Cyber Security

---

1. Concept of Cyber Security

Cyber Security is the practice of protecting computers, servers, networks, mobile devices, electronic systems, and data from malicious digital attacks. In the modern era, where almost every activity—banking, shopping, education, healthcare, and governance—is digitized, ensuring the security of digital information has become a critical requirement.

- Definition:

  Cyber Security refers to a set of techniques and practices designed to safeguard digital systems from unauthorized access, theft, or damage.

- Main Goals of Cyber Security are represented by the CIA Triad:

  1. Confidentiality → Protecting information from unauthorized users.

     Example: Only authorized employees should access company salary details.

  2. Integrity → Ensuring that data remains accurate, consistent, and unaltered.

     Example: Bank transactions should not be tampered with during processing.

  3. Availability → Ensuring systems and data are accessible when required.

     Example: A hospital's patient records must always be available during emergencies.

---

2. Significance of Cyber Security

The importance of Cyber Security can be understood by analyzing its impact on individuals, businesses, and governments.

1. For Individuals:

    - Protects personal data (Aadhaar, PAN, credit card details, medical records).
    - Prevents identity theft and online scams.
2. For Businesses:
    - Prevents financial losses due to hacking or ransomware.
    - Ensures business continuity.
    - Builds customer trust in online transactions.
3. For Governments:
    - Protects national security and defense networks.
    - Safeguards critical infrastructure like power grids, airports, and railways.
    - Prevents cyber warfare and espionage.

💡 Example: In 2017, the WannaCry ransomware attack affected over 200,000 computers in 150 countries, including banks, hospitals, and railway systems. This highlighted the global significance of strong cyber defenses.

---

3. Fundamentals of Cyber Security

Every Cyber Security framework is based on certain fundamental principles:

- Authentication → Verifying a user's identity before granting access (e.g., passwords, biometrics, OTP).
- Authorization → Granting specific rights to authenticated users (e.g., a student can view marks but not change them).
- Non-repudiation → Ensuring that a sender cannot deny sending a message or transaction (achieved through digital signatures).
- Data Protection → Encrypting and securing sensitive information from theft.
- Risk Management → Identifying, assessing, and minimizing potential threats.

---

4. Cyber Security Techniques

(a) Cryptography

- Science of converting information into a secure format.
- Provides confidentiality, integrity, and authentication.
- Types:
    - Symmetric Cryptography → Same key used for encryption & decryption. Fast, but key distribution is difficult. (Example: DES, AES)
    - Asymmetric Cryptography → Uses two keys: Public Key (shared openly) and Private Key (kept secret). (Example: RSA, ECC)

(b) Encryption

- Definition: Process of converting plaintext (readable text) into ciphertext (unreadable format).
- Widely used in securing emails, files, and network communication.
- Example: WhatsApp uses end-to-end encryption, meaning only sender and receiver can read the messages.

(c) Firewalls

- Firewalls act as security guards of computer networks.
- Monitor incoming and outgoing traffic and block unauthorized access.
- Types of Firewalls:
    - Packet Filtering Firewall
    - Proxy Firewall
    - Next-Generation Firewall (NGFW)

(d) Passwords

- Most basic and widely used authentication method.
- A strong password should have:
    - Minimum 8–12 characters
    - Mix of uppercase, lowercase, numbers, symbols
    - No dictionary words or personal information
- Problems: People reuse weak passwords or write them down. Hence, advanced methods like multi-factor authentication (MFA) are recommended.

(e) Privacy

- Cyber Security also ensures data privacy—keeping personal and organizational information safe from misuse.
- Privacy is protected by laws like:
    - GDPR (General Data Protection Regulation) – Europe
    - IT Act 2000 & IT Rules 2011 – India

Example: Companies like Google and Facebook must protect users' data and cannot share it without permission.

(f) Digital Signatures

- A mathematical technique used to validate the authenticity and integrity of digital data.
- Provides Authentication + Integrity + Non-repudiation.
- Widely used in:
    - Online contracts
    - Income Tax e-filing in India

- E-Governance

---

5. Issues and Challenges in Cyber Security

Despite advancements, several challenges remain:

1. Hacking and Malware: Hackers use viruses, worms, spyware, and ransomware to attack systems.
2. Phishing Attacks: Fake emails/websites trick users into giving personal details.
3. Insider Threats: Employees misusing access rights for personal gain.
4. Advanced Persistent Threats (APT): Long-term, highly targeted attacks by skilled hackers.
5. IoT Vulnerabilities: Smart devices (CCTV, Alexa, Smart TVs) often lack strong security.
6. Cloud Security Issues: Data stored in the cloud can be leaked if not protected.
7. Shortage of Skilled Professionals: Global demand for cyber experts is rising, but trained manpower is limited.
8. Legal and Ethical Issues: Different countries have different cyber laws, making international cybercrime hard to control.