# CYBER SECURITY BASICS

## 1. What is Cybersecurity?

Cybersecurity is the practice of **protecting computers, networks, and data** from:

- Hackers (unauthorized access)
- Viruses and malware
- Data leaks/loss
- Cyberattacks (like phishing, ransomware, etc.)

## 2. Main Areas in Cybersecurity:

| Area | Description |
|---|---|
| **Network Security** | Protecting data as it travels across networks |
| **Information Security** | Keeping sensitive info safe (like passwords, Aadhar, etc.) |
| **Ethical Hacking** | Hacking legally to find and fix security flaws |
| **Malware Analysis** | Studying viruses, worms, trojans to prevent spread |
| **Cyber Law & Forensics** | Catching cybercriminals and presenting digital evidence |

## 3. Common Threats You'll Learn About:

- **Phishing** – Fake emails/websites to steal info
- **Malware** – Harmful software like virus, worms, ransomware
- **DDoS Attack** – Overloading a website to make it crash
- **Man-in-the-Middle (MITM)** – Hacker intercepts data between two people

## 4. Important Concepts:

| Concept | Explanation |
|---|---|
| **Encryption** | Converting data into unreadable form (secure) |
| **Authentication** | Proving who you are (like password, OTP) |
| **Firewall** | A barrier that blocks unauthorized access |
| **Antivirus/Antimalware** | Software that detects and removes viruses |

## 5. Tools You'll Use Later:

- **Wireshark** – Network analyzer
- **Kali Linux** – Ethical hacking OS
- **Burp Suite** – Web security testing
- **Nmap** – Port scanner
- **Metasploit** – Hacking tool for learning purposes

## Tips to Get Started:

- Learn **basic networking** (IP, DNS, Ports, Protocols)
- Get good with **Linux commands**
- Start small with **simple hacking labs** like TryHackMe or Hack The Box

# FUNDAMENTAL OF CYBERSECURITY

## 1. Definition of Cybersecurity

Cybersecurity is the practice of protecting computer systems, networks, software, and data from cyberattacks or unauthorized access.

Goal: Maintain Confidentiality, Integrity, and Availability - known as the CIA Triad.

## 2. CIA Triad – The Core of Cybersecurity:

| Term | Meaning |
|---|---|
| **Confidentiality** | **Only authorized users should access data (e.g., passwords)** |
| **Integrity** | **Data should not be changed by unauthorized people** |
| **Availability** | **Systems & data should be available when needed (no downtime)** |

## 3. Types of Cybersecurity:

| Type | Description |
|---|---|
| **Network Security** | Protects networks (like Wi-Fi, LAN) from intruders |
| **Application Security** | Protects software/apps from threats |
| **Information Security** | Keeps data safe (like Aadhar, passwords, etc.) |
| **Operational Security** | Controls who can access what inside an organization |
| **Cloud Security** | Protects data stored in cloud platforms (Google Drive, AWS) |

## 4. Common Cyber Threats:

| Threat | Description |
|---|---|
| **Phishing** | Fake messages/emails to trick users and steal info |
| **Malware** | Harmful software (virus, worm, trojan, ransomware) |
| **Spyware** | Secretly spies on your device activity |
| **DDoS Attack** | Overloading servers to shut down a website |
| **Social Engineering** | Tricking humans into giving away passwords/info |

## 5. Basic Cybersecurity Tools & Concepts:

| Tool/Concept | Use |
|---|---|
| **Firewall** | Blocks unauthorized access to/from networks |
| **Antivirus** | Detects & removes malicious software |
| **Authentication** | Confirms user identity (password, fingerprint, OTP) |
| **Encryption** | Converts data into secret code to protect it |
| **VPN** | Virtual network to keep your online activity private |

## 6. Need for Cybersecurity:

- Digital India = More internet usage
- Online banking, UPI, Aadhaar, healthcare = More targets
- Businesses, colleges, government = All store sensitive data
- So, Cybersecurity = National & personal safety

## 7. Cyber Laws (India):

- IT Act 2000 – Indian law to punish cybercrime
- Covers hacking, identity theft, data theft, cyberstalking, etc.