

full one-shot videos on :JK Coding Pathshala YouTube channel

# JK Coding Pathshala

<https://youtube.com/@jayeshkande9215?feature=shared>



Unit VI	INTRODUCTION TO CYBER SECURITY	(06 hrs)
<b>Introduction to Cyber Security:</b> Basic Cyber Security Concepts, Layers of security, Vulnerability, Threat, Harmful Acts-Malware, Phishing, MIM Attack, DOS Attack, SQL Injection, Internet Governance – Challenges and Constraints, Computer Criminals, Assets and Threat, Motive of Attackers, Software attacks, hardware attacks, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber Stalking, Cyber Terrorism, Cyber Espionage, Comprehensive Cyber Security Policy		

- Q7)** a) What is cyber terrorism? How to identify and detect cyber stalking? [8]
- b) Explain various cyber crimes and Computer criminals. [9]

OR

- Q8)** a) Define & explain Vulnerability, Threat, Malware & Phishing. [8]
- b) Explain DoS Attack and SQL injection attack. [9]

**Q7) a)** What is cyber terrorism? Write in detail example of cyber terrorism. **[8]**

b) What is a man-in-the-middle attack (MIM)? Explain in detail. **[9]**

OR

**Q8) a)** Explain the term phishing & SQL Injection with suitable example. **[8]**

b) Explain the term cyber stalking & cyber espionage with suitable example. **[9]**

- Q7)** a) What is Cyber terrorism? What is an example of cyber terrorism? [8]  
b) Define Crime and Cybercrime. State Cybercrimes classification. [9]

OR

- Q8)** a) What Is Cyberstalking explain with an example. [8]  
b) Explain the term Phishing & SQL Injection with a suitable example. [9]

**Q7) a)** Write a short note on Software attacks & hardware attacks with example. **[8]**

**b)** Explain the threats and vulnerabilities of the information security system. **[9]**

OR

**Q8) a)** Explain Layers of Cyber Security in detail. **[8]**

**b)** What is a man-in-the-middle attack (MIM)? Explain in detail. **[9]**

**Q7) a)** Write short notes on

**[9]**

- i) Malware
- ii) Phishing
- iii) MITA attack

b) Elaborate different cyber security polycies in detail and explain different challenges in internet governance.

**[8]**

OR

**Q8) a)** Explain the term cyber stalking. How to iderty and detect cyber stalking.

b) Explain the types of cyber-crimes.

# Introduction to Cyber Security

## 1. Cyber Security kya hoti hai?

Cyber Security ka matlab hai — computer systems, mobile devices, networks aur data ko hackers, viruses aur unauthorized logon se bachana.

**Goal:** Aapki personal info, passwords, aur financial data ko safe rakhna.



## 2. Important Concepts:

### Asset :

Jo bhi cheez aapke liye valuable hai — jaise files, data, software, computer, etc.

**Example:** Aapka Gmail account, mobile phone, ya credit card info.

### Threat :

Koi bhi cheez ya person jo aapki asset ko nuksan pahucha sakta hai.

**Example:** Hacker jo aapka password chura sakta hai.

### Vulnerability :

System ke andar koi weakness jisse hacker easily attack kar sake.

**Example:** Old software jisme security update nahi hai.

### Attack :

Jab koi threat actual me action leta hai to wo attack kehlata hai.

**Example:** Virus attack, phishing email, website hack hona.

### Risk :

Threat aur vulnerability ke combination se hone wala possible nuksan.

**Example:** Agar aapka password weak hai (vulnerability) aur hacker try kare (threat), to aapka account hack ho sakta hai (risk).

### 3. 🎯 Cyber Security ke Main Goals

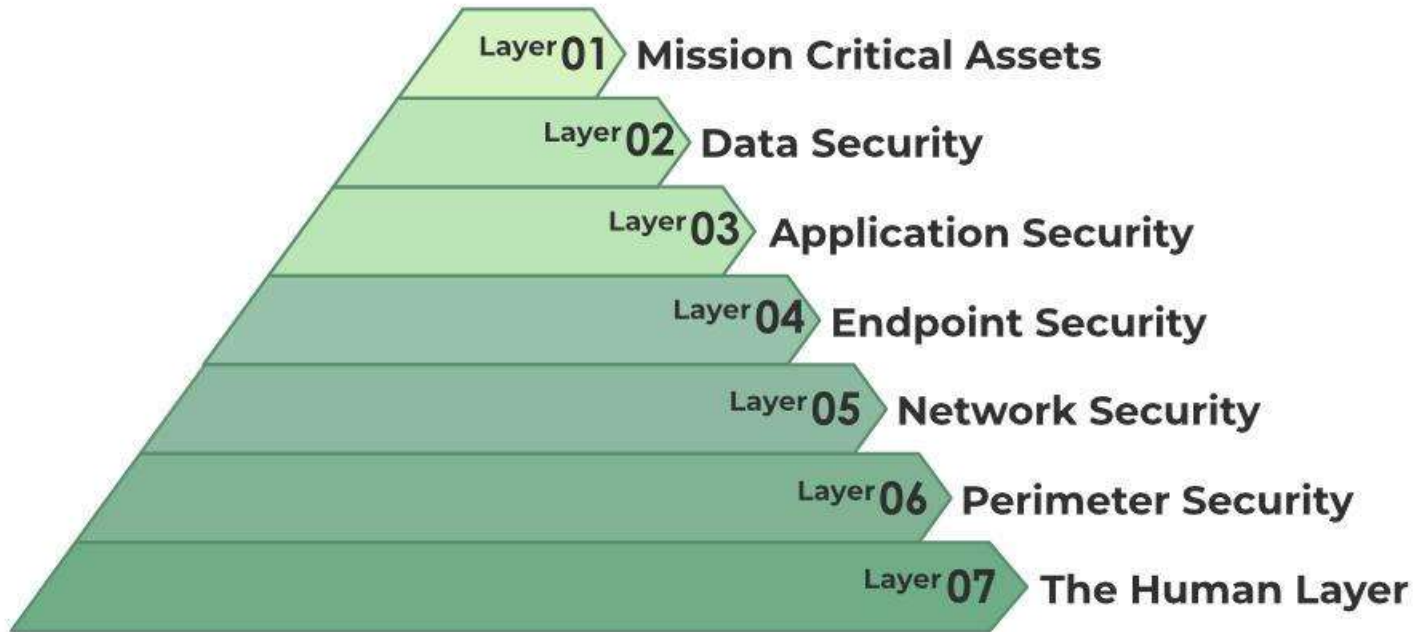
Goal	Explanation
<b>Confidentiality</b>	Data sirf authorized log hi dekh sakein.
<b>Integrity</b>	Data ko bina permission ke change nahi karna.
<b>Availability</b>	Jab zarurat ho, tab system aur data accessible ho.

#### **4.Real-Life Example:**

Agar aap online shopping karte ho:

- Aapka credit card info secure hona chahiye (Confidentiality).
- Payment amount galat na ho (Integrity).
- Website kaam kare jab aap use kar rahe ho (Availability).

# The Seven Layers of IT security



## ▲ The Seven Layers of IT Security

### □ Layer 01: Mission Critical Assets :

- Yeh sabse top layer hai — jisme aapke business ke most important data aur systems hote hain.
- Example:** Company ka financial data, customer records, trade secrets.
- Security:** Isko access karne ke liye highest level security chahiye (multi-factor authentication, encryption, etc).

### □ Layer 02: Data Security

- Is layer ka focus sirf **data ko protect** karne par hota hai — stored ya transmitted.
- Methods:** Encryption, data masking, secure backups.
- Example:** Passwords ko encrypted format me rakhna.

### □ **Layer 03: Application Security**

- Applications jaise mobile apps, websites, CRM systems ko secure rakhna.
- **Methods:** Code testing, patch updates, firewalls.
- **Example:** Bank app me login karne ke liye OTP lagana.

### □ **Layer 04: Endpoint Security**

- Yeh layer user ke devices (laptop, phone, PC) ko protect karti hai.
- **Tools:** Antivirus, anti-malware, encryption, mobile device management.
- **Example:** Laptop me BitLocker encryption lagana.

## □ **Layer 05: Network Security**

- Network ke through hone wale attacks ko block karta hai.
- **Tools:** Firewalls, intrusion detection systems, VPNs.
- **Example:** Office network me unauthorized user ko block karna.

## □ **Layer 06: Perimeter Security**

- External threats se protection deta hai – especially from internet-facing systems.
- **Tools:** DMZ, firewalls, proxies.
- **Example:** Public web servers ko secure karna.

## □ Layer 07: The Human Layer

- **Most vulnerable layer** — humans hi galti karte hain (jaise phishing emails par click karna).
- **Solution:** Awareness training, strong password policies.
- **Example:** Employees ko sikhana ki spam emails kaise pehchanein.



Layer No.	Name	Simple Explanation
01	Mission Critical Assets	Sabse important data/system jisko best security chahiye
02	Data Security	Data encryption, protection during use/transfer
03	Application Security	App ke bugs, loopholes se bachav
04	Endpoint Security	User ke devices jaise mobile/laptop secure karna
05	Network Security	Network par hone wale attacks ko rokna
06	Perimeter Security	External network boundary ko secure rakhna
07	Human Layer	Employee training aur phishing awareness

## ⚠️ Vulnerability kya hoti hai?

### ★ Definition:

Vulnerability ka matlab hota hai — **system ke andar koi weakness ya loophole** jiska फायदा hacker ya attacker utha sakta hai.

### □ Simple Explanation:

Agar aapke ghar ka darwaza purana hai aur lock thik se kaam nahi karta, to wo ek vulnerability hai — koi bhi usse easily ghus sakta hai.

## **Types of Vulnerabilities:**

### **1. Software Vulnerability:**

1. Old ya unpatched software jisme security bugs hote hain.
2. Example: Windows ka old version jo update nahi hua.

### **2. Weak Passwords:**

1. Jaise “123456” type ka password — easily guess ho sakta hai.

### **3. Misconfiguration:**

1. Server ya network settings sahi se configure na hona.

### **4. Lack of Encryption:**

1. Data bina encryption ke transfer ho raha ho.

## **Protection Tips:**

- Software ko regular update karo.
- Strong passwords use karo.
- Network aur apps ko properly configure karo.

## 🔥 Threat (खतरा) kya hota hai?

### ★ Definition:

Threat ka matlab hota hai — **koi bhi cheez ya person jo system ko damage, access ya misuse karne ki koshish kare.**

### □ Simple Explanation:

Agar koi chor aapke ghar ka purana darwaza dekh kar andar aane ki sochta hai — wo threat hai.

## **Types of Threats:**

### **1.Malware:**

1. Virus, Trojan, Ransomware — system ko corrupt karta hai.

### **2.Phishing:**

1. Fake email ke zariye personal info churaana.

### **3.Hackers:**

1. Unauthorized access karne wale attackers.

### **4.Insider Threats:**

1. Company ke hi log jo jaan bujhkar nuksan pahunchayein.

### **5.Natural Threats:**

1. Earthquake, flood se servers ya data destroy ho sakta hai.

## **Protection Tips:**

- Anti-virus install karo
- Phishing emails se bacho
- Access controls lagao
- Employee training do

## **Harmful Acts:**

- Malware
- Phishing
- MIM (Man-In-the-Middle) Attack
- DOS (Denial of Service) Attack
- SQL Injection



## ❑ **Malware:**

### 📖 **Definition**

**Malware** ka full form hota hai "**Malicious Software**" — ye aise software ya program hote hain jo aapke computer, mobile ya network ko **nuksan pahunchane ke liye banaye jaate hain**.

## ❑ **Simple Language mein:**

Malware ek **bura software** hota hai jo chhup kar system me ghus jata hai aur:

- data chura leta hai
- system ko slow ya corrupt kar deta hai
- unauthorized control le leta hai

## Types of Malware

Type	Explanation (HiEnglish)	Example
<b>Virus</b>	Khud ko dusre files/programs me copy karta hai aur phailta hai	File virus, macro virus
<b>Worm</b>	Network ke through automatically spread hota hai	Internet worms
<b>Trojan Horse</b>	Useful software jaisa dikhta hai but andar se harmful hota hai	Fake game ya cracked software
<b>Ransomware</b>	Aapka data encrypt karke paise (ransom) maangta hai	WannaCry, Petya
<b>Spyware</b>	Chupke se user activity record karta hai	Keyloggers, adware
<b>Adware</b>	Bar-bar unwanted ads dikhata hai	Popup ads, redirect viruses
<b>Rootkit</b>	Hacker ko hidden access deta hai system ke andar	Deep system control malware

## ✦ Malware ka Real-Life Example:

### WannaCry Ransomware Attack (2017):

Is malware ne duniya bhar ke hospitals, companies aur governments ke computers ko lock kar diya tha. Attackers ne files ko unlock karne ke liye **Bitcoin ransom** maanga tha.

## □ **Malware se Protection kaise karein?**

1. **Antivirus Software** use karo (jaise Quick Heal, Avast, Kaspersky)
2. **Regular updates** karo operating system aur software ka
3. Unknown links ya email attachments **click na karein**
4. **Strong passwords** rakhein
5. Secure websites (https://) ka hi use karein
6. Pirated software install **na karein**


## Phishing:

### Definition :

**Phishing** ek cyber attack technique hai jisme attacker aapko **fake email, message ya website** ke through **personal ya financial information churaane ki koshish karta hai**. Ye ek type ka **social engineering attack** hota hai.

### ☐ Simple Language mein:

Phishing matlab hota hai "jhooth bol kar ya ullu bana kar" aapka sensitive data (jaise password, bank details) chura lena — jaise ek machhli ko bait de kar pakadna.

 "Phishing = Fake message + Real damage"

## ✉️ **Phishing kaise hota hai? (Common Methods)**

### **1.Fake Emails :**

1. Email aata hai jaise bank, Paytm ya Google ki taraf se.
2. Message hota hai: "Aapka account suspend hone wala hai, turant login karein."

### **2.Fake Websites:**

1. Link click karne par aapko ek **fake website** par le jaya jata hai — original website jaisi dikhne wali.
2. Aap wahan login karte ho aur attacker aapka username-password chura leta hai.

### **3.SMS Phishing (Smishing):**

1. SMS ke through bhi aise messages aate hain:  
"Click this link to claim your free gift "

### **4.Voice Phishing (Vishing):**

1. Fake phone calls: "Main aapke bank se bol raha hoon, OTP batayein..."

### 🎯 Real-Life Example:

#### **RBI Bank Fake Email Scam:**

Logon ko ek email aaya tha jisme likha tha:

“Your RBI refund is ready, click here to claim ₹50,000”.

Jab logon ne link par click kiya, unka bank login chura liya gaya.

### ❑ **Phishing se kaise bachen?**

1. **Unknown links/email par click na karein**
2. **Website URL check karein:** Always use **https://**
3. **Spelling mistakes aur urgent tone se alert ho jao**
4. **Sender ka email address carefully check karo**
5. Bank ya company kabhi bhi OTP ya password **nahi maangti**
6. **Two-factor authentication (2FA) enable karo**

## ☐♂☐ **MIM Attack (Man-In-The-Middle Attack):**

### 📖 **Definition:**

**Man-in-the-Middle (MIM) Attack** ek aisa cyber attack hota hai jisme attacker do logon ke beech ki communication ko secretly intercept (बीच में सुनना या बदलना) karta hai — bina unke pata chale. Yani attacker dono ke **beech me ghus jata hai** jaise ek "middleman".



### □ Simple Example (Real-life jaisa):

Socho aap bank ki website par login kar rahe ho.  
Aapka data jaa raha hai → 🗝️ Bank ke server tak.  
Agar beech me koi attacker aa gaya —  
jo aapka **username, password ya OTP** secretly capture kar le —  
to **yehi hota hai Man-in-the-Middle attack**.

🗣️ “You think you’re talking to the bank, but you’re actually talking to the hacker.”

## 🔍 How MIM Attack Works (Kaise hota hai):

1. User ek secure website (jaise bank) par login karta hai
2. Attacker beech me ghus kar traffic capture karta hai
3. Wo aapki info (passwords, messages) dekh bhi sakta hai aur change bhi kar sakta hai

## 🔒 Types of MIM Attacks:

Type	Explanation
<b>Wi-Fi Eavesdropping</b>	Public Wi-Fi par attacker network sniffing karta hai
<b>HTTPS Spoofing</b>	Fake SSL certificate ke through secure site jaisa page dikhata hai
<b>Session Hijacking</b>	Logged-in session ko hijack karke user ban jaata hai
<b>Email Hijacking</b>	Emails ko intercept karke reply ya data chura leta hai
<b>DNS Spoofing</b>	Real website ki jagah fake site dikhata hai

□ **Protection from MIM Attacks:**

1. Hamesha **HTTPS** secure websites ka use karo
2. **Public Wi-Fi** avoid karo (ya VPN use karo)
3. **SSL certificate** check karo site visit karte waqt
4. Unknown emails, popups, suspicious sites se savdhaan raho
5. Use **two-factor authentication (2FA)**
6. VPN (Virtual Private Network) ka use karo secure browsing ke liye

## ☀ DoS Attack (Denial of Service Attack):

### 📖 Definition:

**DoS attack** ek aisa cyber attack hota hai jisme attacker kisi website, server, ya system par itni zyada traffic bhejta hai ki **wo system crash ya slow ho jaata hai**, aur real users usse access nahi kar paate.

🗣 “Denial of Service” = Service bandh ho jaati hai (public ke liye)

### ❏ Simple Example (Socho aise):

Sochiye ek restaurant me 10 logon ke liye jagah hai.

Lekin 1 attacker 100 fake customers ko bhej deta hai sirf seats occupy karne ke liye — asli customers andar hi nahi aa paate.

**Yehi DoS attack hai.**

## 🔄 Types of DoS Attacks:

Type	Explanation (HiEnglish)
<b>Volume-based</b>	Server ko zyada requests bhej kar bandwidth full kar dete hain
<b>Protocol-based</b>	Network ke rules/protocols ka misuse karke system confuse karte hain
<b>Application-level</b>	Website/app ke specific functions par attack karte hain

## 🔥 DDoS Attack (Distributed Denial of Service):

**DoS attack ka upgraded version = DDoS attack**

- DDoS me attacker sirf ek machine se nahi — **multiple systems (botnet)** use karta hai.
- Zyada powerful hota hai, kyunki attack **multiple locations se ek saath hota hai**.
- **Example:** Netflix, Amazon, or Govt websites ka down ho jaana due to sudden traffic.

## 🎯 Real-Life Example:

### **GitHub DDoS Attack (2018):**

- GitHub par 1.35 Tbps se zyada data bheja gaya
- World ka one of the **biggest DDoS attack**
- GitHub temporarily down ho gaya tha

### □ **Protection from DoS/DDoS Attacks:**

1. **Firewall & Anti-DDoS tools** install karo (like Cloudflare, AWS Shield)
2. Suspicious traffic ko monitor karo
3. **Rate limiting** lagao — ek IP se kitni baar request allowed hai
4. Load balancer use karo to distribute traffic
5. Fake bot traffic ko detect karne ke tools use karo

## ❑ **SQL Injection:**

### 📖 **Definition:**

**SQL Injection** ek **code injection attack** hota hai jisme attacker **malicious SQL code** (Structured Query Language) ko input field ke through database me bhejta hai — **jisse wo unauthorized data access ya damage kar sakta hai.**

👉 “Attacker SQL code daal kar database ka control le leta hai.”



### □ Simple Example (Real-life jaisa):

Aap login page par jaate ho aur username/password daalte ho.  
Normal query hoti hai:

```
SELECT * FROM users WHERE  
username = 'user' AND password = '1234';
```

Agar attacker ne password ki jagah likh diya:

```
' OR '1'='1
```

To query ban jaayegi:

```
SELECT * FROM users WHERE username = 'user' AND password = " OR '1'='1';
```

'1'='1' hamesha true hota hai — to **login bypass ho jaata hai!**

✗ Authentication fail hone ke bajaye, attacker **bina password ke login kar jaata hai!**

## ★ What Attackers Can Do Using SQL Injection:

Attack Objective	What Happens
🔒 Login Bypass	Unauthorized login without password
📁 Data Leakage	Database se sensitive data nikal lete hain (email, card, etc.)
🗑️ Data Deletion	Delete/modify kar dete hain important tables
🖥️ Admin Access	Admin panel access le lete hain
🔧 Server Control	Backend system ka control mil sakta hai

## ❑ SQL Injection Se Kaise Bachein? (Protection Tips)

- ✔ **Input Validation:**

- User input ko sanitize karo — special characters (like ', ", --) remove karo.

- ❑ **Use Prepared Statements (Parameterized Queries):**

- Hardcoded SQL ke bajaye secure query functions use karo.

Example (in PHP):

- `$stmt = $pdo->prepare("SELECT * FROM users WHERE username = ? AND password = ?");`

- 🔒 **Use ORM (Object Relational Mapping):**

- Like Hibernate, Sequelize, Django ORM – jo SQL queries ko safely handle karta hai.

- ❑ **Error Messages Hide Karo:**

- Attackers ko backend error dikha ke hint mat do (e.g., "SQL syntax error").

- ⊘ **Avoid Dynamic SQL:**

- Avoid karo SQL queries jisme directly user input include ho.

🔗 **SQL Injection Real-Life Example:**


**2012 – Yahoo SQL Injection Attack:**

Hackers ne SQL injection ke zariye 450,000+ users ke login credentials chura liye the

## **Internet Governance: What is it?**

### **Definition:**

**Internet Governance** ka matlab hai **rules, policies, and decisions** jo internet ke use, development, aur security ko **globally manage karne ke liye banaye jaate hain**.

 “Internet governance ensures the internet is open, secure, and accessible for all.”

## ⚠️ Challenges & Constraints in Internet Governance

### ◆ 1. Cybersecurity Threats :

- Hackers, ransomware, phishing, DDoS attacks increase ho rahe hain.
- Global rules aur coordination ki kami hai.

### ◆ 2. Lack of Global Agreement :

- Har country ka internet policy alag hai.
- U.S., China, Russia jaise countries ki policies clash karti hain.

### ◆ 3. Data Privacy and Protection :

- Personal data misuse, surveillance, unauthorized access — sab concern hai.
- GDPR (Europe), PDP (India) jaise rules bhi ek jaisi nahi hain.

### ◆ 4. Digital Divide :

- Rural vs urban areas, rich vs poor countries ke beech internet access me farak.
- Education aur digital literacy bhi barrier hai.

### ◆ 5. Misuse of Social Media :

- Fake news, hate speech, election interference — social platforms par control mushkil hai.
- Content regulation ka clear global framework nahi hai.

### ◆ 6. Jurisdiction Issues :

- Kisi ek country ke law doosri country me kaise apply honge?
- Internet borderless hai, par laws national hote hain.

Challenge	Explanation
Cybersecurity Threats	Increasing attacks, less global coordination
Global Policy Conflict	Different countries, different rules
Privacy Concerns	Data misuse and surveillance risks
Digital Divide	Unequal access to internet and technology
Social Media Misuse	Fake news, hate speech, political manipulation
Jurisdiction Issues	Which law applies where? Internet is borderless
Tech Monopoly	Big tech dominance raises fairness concerns
Representation Gaps	Less voice for poor nations and small stakeholders

## **Computer Criminals: Introduction**

### **Definition:**

**Computer Criminals** ya **Cyber Criminals** wo log hote hain jo computers, networks, aur internet ka use karke **illegal activities** karte hain — jaise data churaana, systems ko hack karna, ya fraud karna.

🌀 “Ye log technology ka misuse karke crime karte hain — bina physically present huye.”



## 🔍 Types of Computer Criminals

### 1. 🧑💻 Hackers :

- Unauthorized access lete hain kisi system ya network ka.
- Do types hote hain:
  - **Black Hat** – criminal intent ke saath hacking
  - **White Hat** – ethical hacking (security testing ke liye)
  - **Grey Hat** – mix of both

### 2. 🧑🔓 Crackers:

- Software ko illegally break karte hain (e.g., license bypass).
- **Pirated software** create ya distribute karte hain.

### 3. 💣 Cyber Terrorists:

- Political ya ideological motive se computer systems par attack karte hain.
- Example: National power grid ya govt websites par attack.

#### 4. **Corporate Spies (Industrial Spies):**

- Competitor companies ka data churaane ke liye hired hote hain.
- Trade secrets, client data, product codes etc. churaate hain.

#### 5. **Insiders:**

- Company ya organization ke hi log jo andar se data leak ya damage karte hain.
- Most dangerous, kyunki inhe system ka full access hota hai.

#### 6. **Phishers:**

- Fake emails, websites, SMS bhej kar logon se passwords, OTP ya credit card info churaate hain.

### 7. 🕸️ Cyber Fraudsters:

- Online shopping scams, fake lottery, investment frauds jaise kaam karte hain.
- Bank frauds, UPI scams bhi inhi mein aate hain.

## ⚠️📌 Motives of Computer Criminals:

Motive	Explanation
💰 Financial Gain	Paise kamaane ke liye (fraud, theft)
👑 Power/Control	Systems ko control karne ka interest
🔐 Challenge	Skill dikhane ke liye (mostly young hackers)
😡 Revenge	Kisi se badla lene ke liye (insiders)
🔥 Political Agenda	Govt system disrupt karne ke liye (cyber terrorists)

### ❑ **How to Stay Safe from Computer Criminals:**

1. 🔒 Use strong passwords and 2FA
2. ⚠️ Unknown links/emails par click na karein
3. 🖥️ Antivirus and firewall use karo
4. 🔄 Software regular update karo
5. ❑ Cyber awareness aur training zaroori hai

# Assets and Threats







## What Are Assets in Cyber Security?

### Definition:

**Assets** wo sab kuch hota hai **jo kisi organization ya person ke liye valuable hota hai**, aur jise protect karna zaroori hota hai.

 "Assets are anything of value that needs protection."

## □ Types of Assets:

Type	Example
 <b>Data</b>	Personal data (Aadhaar, passwords), business records, emails
 <b>Software</b>	Applications, operating systems, licensed tools
 <b>Hardware</b>	Servers, computers, routers, mobile devices
 <b>Network</b>	Internet connections, Wi-Fi systems
 <b>Documents</b>	Contracts, reports, ID proofs, invoices
 <b>People</b>	Employees, users, stakeholders — jinke paas sensitive access ho








## ⚠️ What Are Threats in Cyber Security?

### 📖 Definition:

**Threats** wo actions, events ya log hote hain jo kisi **asset ko damage, misuse, ya destroy** karne ka **risk** ban jaate hain.

🗣️ “Threat is anything that can harm your digital assets.”

## □ Types of Threats:





Type	Explanation + Example
 <b>Malware</b>	Virus, worm, ransomware — data corrupt ya chura sakta hai
 <b>Phishing</b>	Fake emails/websites se personal info churaana
 <b>DDoS Attack</b>	Website ya server ko crash kar dena traffic bhej ke
 <b>Unauthorized Access</b>	Kisi ke system me bina permission ghus jaana
 <b>Insider Threats</b>	Employee ya user jo jaan bujh ke system ko harm kare
 <b>Natural Threats</b>	Fire, flood, earthquake — hardware damage ho sakta hai
 <b>Social Engineering</b>	Logon ko trick kar ke passwords, OTPs nikalna



## □ How to Protect Assets from Threats?

Step	What to Do
🔍 Identify Assets	Important data, systems, people pe focus karo
⚠️📋 Analyze Threats	Kis type ke attacks ho sakte hain, unka risk samjho
🛡️ Use Security Tools	Antivirus, firewalls, encryption, backups etc.
👤📚 Train Users	Cyber awareness training for staff and users
🔒 Access Control	Sirf authorized logins allow karo

## Motive of Attackers

 No.	 Motive	 Explanation (HiEnglish)	 Example
1	Financial Gain	Paisa kamane ke liye system hack/fraud karte hain	Bank fraud, ransomware, card cloning
2	Revenge	Personal ya professional badla lene ke liye attack karte hain	Ex-employee ne system crash kar diya
3	Political/Ideological	Govt systems ko disrupt karna ya message dena	Cyber terrorism, hacktivism
4	Cyber Espionage	Competitor ya dusri country ka secret data churaana	Industrial spying, military data hacking
5	Challenge/Thrill	Sirf apni skills dikhane ke liye — maza ke liye	Young hacker ne unauthorized login kiya
6	Notoriety/Fame	Hacker community me naam banane ke liye	Website defacement with hacker's name
7	Destruction	Sirf system ko damage ya disrupt karne ka irada	Delete karna, website crash karna
8	Insider Benefit	Organization ke andar ka banda jo internal data misuse karta hai	Data leak, credentials sell karna
9	Access to Resources	Powerful systems, servers ya networks ka access chahiye	Botnet creation, crypto mining from others' systems

## **Types of Attacks:**

- Software Attacks
- Hardware Attacks

## ★ **Types of Attacks in Cyber Security**

Cyber attacks do major categories mein divide hote hain:

**1. Software Attacks**

**2. Hardware Attacks**

## ❏ 🖥️ 1. Software Attacks

### 📄 Definition:

Software attacks wo hote hain jisme attacker **malicious code ya programs** ka use karke system, application ya data ko damage, access ya control karta hai.

🗣️ “Software ke through hone wale attacks — jaise virus, malware, phishing, etc.”

## Common Types of Software Attacks:

● Attack Type	💬 Explanation	🔗 Example
📄 <b>Virus/Worm</b>	Apne aap spread hone wale programs jo files damage karte hain	Email attachment virus
🐞 <b>Trojan Horse</b>	Fake useful software, lekin secretly damage karta hai	Free game with hidden malware
🎣 <b>Phishing</b>	Fake email/website se user ka data churaana	Bank login page clone
🔒 <b>Ransomware</b>	Files lock karke paise maangna	WannaCry, Locky attacks
🕵️ <b>Spyware/Keylogger</b>	Secretly user ki activity record karta hai	Password churaana
💣 <b>DoS/DDoS</b>	Website/server par traffic overload bhejna	Website crash due to fake traffic
📄 <b>SQL Injection</b>	Malicious code daal kar database hack karna	Login bypass using ' OR '1'='1










## □ 2. Hardware Attacks

### 📖 Definition:

Hardware attacks wo hote hain jisme attacker **physical devices ya hardware components** ko damage, manipulate, ya misuse karta hai.









🗣️ “Yeh attacks system ke physical parts ko target karte hain — jaise motherboard, USB, hard drive, etc.”

## □ Common Types of Hardware Attacks:

 Attack Type	 Explanation	 Example
 <b>Physical Tampering</b>	Computer parts ko todna ya physically alter karna	System ke ports disable kar dena
 <b>Hardware Trojans</b>	Hardware me malicious chip ya circuit daal dena	Infected chip in mobile device
 <b>Keyloggers (Hardware)</b>	External device jo keyboard strokes record karta hai	USB keylogger device
 <b>USB/Removable Attacks</b>	Malicious USB devices ke through attack	USB worm like Stuxnet
 <b>Power Analysis Attack</b>	Device ke power use ka analysis karke secrets nikaalna	Cryptographic key leak
 <b>Signal Interference</b>	Wireless signal jam karna ya intercept karna	Wi-Fi jamming



## Comparison Table: Software vs Hardware Attacks

Feature	  Software Attacks	 Hardware Attacks
 Medium Used	Code, programs, online methods	Physical devices, circuits
 Target	OS, apps, files, data	Devices, chips, circuits
 Installation Way	Downloads, emails, websites	USB, chips, physical access
 Example	Ransomware, phishing, viruses	Keylogger device, Trojan chip
 Protection	Antivirus, firewall, updates	Physical security, secure supply chain

## **Cyber Threats:**

- Cyber Warfare
- Cyber Crime
- Cyber Stalking
- Cyber Terrorism
- Cyber Espionage

## Cyber Threats: Overview

### Definition:

**Cyber Threats** are malicious activities carried out using computers, networks, or the internet that aim to **harm individuals, organizations, or nations**.

🗣️ "Cyber threats kisi bhi digital system ko damage, disturb ya misuse karne ki koshish hoti hai."

## 1 Cyber Warfare

### 📖 What is it?

Nation-level digital attack to damage or disable another country's infrastructure (like military, electricity, communication, etc.).

### ☐ Real Example:

**Stuxnet Worm** – US & Israel ne banaya tha to slow down **Iran ka nuclear program** by infecting their centrifuges.

### ☐ Protection Measures:

- Government-level **cyber defense teams** (like India's CERT-In)
- Secure national infrastructure with **strong firewalls & encryption**
- **AI & threat intelligence** to detect foreign attacks
- Regular **security audits** of critical systems

## 2 Cyber Crime

### What is it?

Illegal online activities for money, data theft, fraud, etc.

#### Real Example:

A hacker sends a **fake bank login page** via email. Jab user login karta hai, attacker uska **username-password chura leta hai**.

#### Protection Measures:

- Use **multi-factor authentication (MFA)**
- Never click on **unknown links** or **email attachments**
- Keep **antivirus & software** updated
- Educate users on **phishing awareness**
- Report incidents to **cyber police** (In India: <https://cybercrime.gov.in>)

### 3 Cyber Stalking

#### What is it?

Internet par kisi ko repeatedly monitor, message, harass, ya threaten karna.

#### Real Example:

Someone creates **fake social media profiles**, sends daily messages, comments on every post, and even tries to find your location.

#### Protection Measures:

- **Report & block** stalkers on social media
- **Restrict privacy settings** (Only friends can view)
- Never share **personal info (address, phone)** publicly
- Use **strong passwords** and change regularly
- File complaint with **cyber crime cell** or police

## 4 Cyber Terrorism

### ■ What is it?

Internet ka use to create **fear**, **chaos**, or damage public services for political/religious motives.

### □ Real Example:

A terrorist group launches a **DDoS attack** on hospitals and emergency services to create panic during a festival.

### □ Protection Measures:

- Use **DDoS protection systems** (like Cloudflare, AWS Shield)
- **Backups** of critical systems and offline alternatives
- **Incident response teams** ready with SOPs
- Collaborate with **law enforcement and CERTs**
- Continuous **monitoring and traffic analysis**

## 5 Cyber Espionage

### ■ What is it?

Secretly collect karna **confidential info** from governments, militaries, ya companies.

### □ Real Example:

Hackers target a company working on a new vaccine and **steal their research data** to sell to competitors or foreign states.

### □ Protection Measures:

- Implement **Zero Trust Architecture** (trust no device or user by default)
- Use **data encryption** and **endpoint protection**
- Limit access to **sensitive files (role-based access)**
- Conduct **employee background checks**
- Train employees on **phishing & suspicious links**



Threat Type	Real-Life Example	How to Protect
Cyber Warfare	Iran nuclear centrifuges infected (Stuxnet)	National cyber defense, AI detection, secure infrastructure
Cyber Crime	Fake bank site to steal login	MFA, phishing awareness, report to cyber police
Cyber Stalking	Fake profiles & repeated threats online	Block/report, strong privacy, police complaint
Cyber Terrorism	DDoS attack on hospitals	DDoS protection tools, backup plans, coordination with CERT
Cyber Espionage	Vaccine research stolen	Encryption, access control, staff training




### ❑ **Comprehensive Cyber Security Policy**

**Purpose:** Is policy ka objective hai organization ke digital assets (data, devices, systems) ko protect karna from unauthorized access, cyber attacks, and misuse.

## 1. Scope

Ye policy apply hoti hai sabhi employees, vendors, contractors, aur anyone jo organization ke IT systems ya data use karta hai.

## 2. Organizational Roles & Responsibilities

Role	Responsibility (Zimmedari)
 Management	Policy implementation, funding, compliance monitoring
 IT Team	Systems security, network monitoring, threat response
 All Employees	Policy follow karna, secure behavior adopt karna

### 3. Key Policy Components

#### A. Access Control

- Har employee ka **unique login ID** hoga
- Use of **strong passwords & Multi-Factor Authentication (MFA)**
- **Access based on role (RBAC)** — sirf jitna zarurat ho, utna access

#### B. Data Protection

- Important data should be **encrypted (AES 256-bit)**
- Regular **data backup** (local & cloud both)
- Confidential files marked as "**Restricted**"

#### C. Device & Network Security

- Only **authorized devices** can connect to office network
- Install **firewalls, antivirus & endpoint protection software**
- Use of **VPN** for remote access

#### **D. Email & Internet Use**

- No opening of **unknown email attachments or links**
- Personal social media use discouraged** on official systems
- Block malicious websites using **Web Filtering**

#### **E. Incident Response Plan**

- Har attack ka **response protocol** ready hona chahiye
- Incident Response Team (IRT)** banayi jaati hai
- Logs maintain kiye jaate hain for investigation

#### **F. Training & Awareness**

- Sabhi employees ka **cyber security training quarterly** hota hai
- Phishing simulations** and awareness posters

#### **G. Third-Party Access**

- Vendors ko **NDA sign** karna hoga
- Minimal data sharing with **end-to-end encryption**

## ⚠️ 4. Penalties for Policy Violation

Type of Violation	Consequence
Weak password, repeated phishing	Training + warning letter
Unauthorized access	Account suspension + investigation
Intentional data breach	Legal action, termination



## 5. Policy Review Cycle

- Ye policy **har 6 mahine mein review/update** ki jaayegi
- Cyber security team aur management dono review karenge

**jayesh\_kande\_** ▾ ●

What's  
on your  
playlist?



**Jayesh Kande**

**16**  
posts

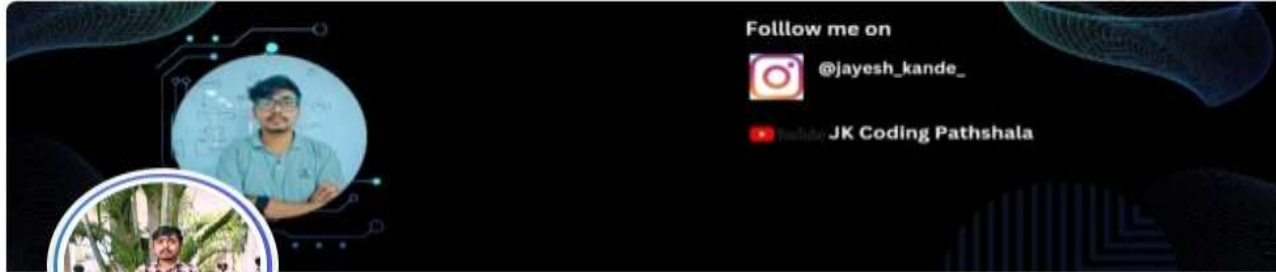
**275**  
followers

**276**  
following

23

रास्ते बदलो, मंजिल नहीं

[yt.openinapp.co/0y0qd](https://yt.openinapp.co/0y0qd)



## Jayesh Kande

Third-Year IT Engineering Student | Aspiring Web Developer  
| Java Enthusiast | Data Structures & Algorithms Learner |  
Proficient in C, C++, Java, and MERN Stack | AI + Web  
Development Project Enthusiast

Nashik, Maharashtra, India · [Contact Info](#)

494 followers · 495 connections



[See your mutual connections](#)

[Join to view profile](#)

[Message](#)



Kbt engineering college nashik



✦✦ **Thank You for Watching!** ✦✦

➔📱 Follow us on Instagram: **@jayesh\_kande\_**

🔗 Connect with us on LinkedIn: **[Jayesh Kande]**