Cyber security 101 :

Thursday, January 1, 2026 1:48 PM

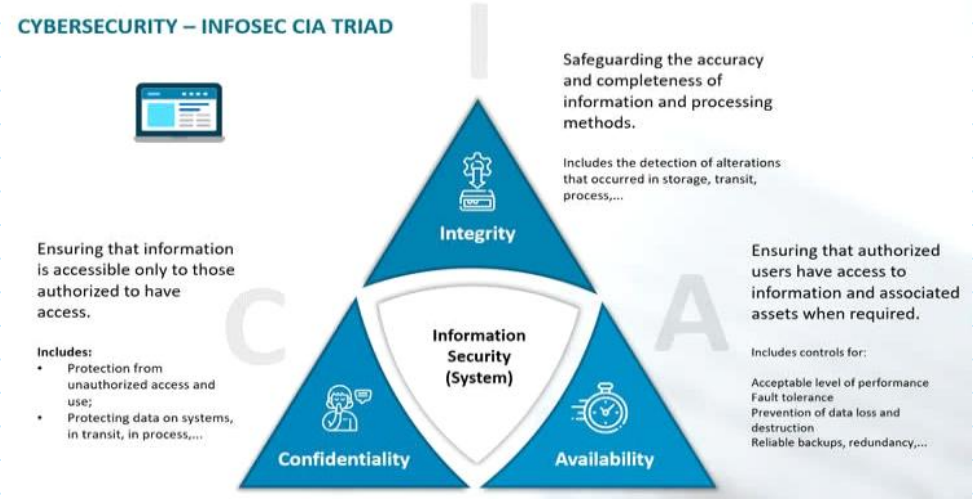
What Is Cybersecurity :

Cybersecurity is the practice of protecting computers, networks, servers, mobile devices, and data from attacks, damage, or unauthorized access.

Core Pillars of Cybersecurity :

1 CIA TRIAD :

The CIA Triad is a fundamental cybersecurity model that ensures data confidentiality, integrity, and availability to protect information from unauthorized access, modification, and disruption.



CONFIDENTIALITY :

- **Confidentiality means protecting information from unauthorized access.**
- **Only authorized users should be able to see or use the data.**

Why Confidentiality is Important :

- **Prevents data leaks**
- **Protects personal and sensitive information**
- **Avoids identity theft and fraud**

How Confidentiality is Achieved :

- **Passwords**
- **Encryption**
- **Access control**
- **Biometrics (fingerprint, face ID)**

INTEGRITY :

- **Integrity ensures that data remains accurate, complete, and unchanged unless modified by an authorized person.**

Why Integrity is Important :

- **Prevents unauthorized modification**
- **Maintains trust in data**

Real-Life Examples :

- Exam marks should not be altered
- Bank balance must remain correct
- Legal documents must stay original

How Integrity is Maintained :

- File hashes
- Checksums
- Digital signatures

AVAILABILITY :

- Availability ensures that data and systems are accessible to authorized users whenever they are needed.

Real-Life Examples :

- Banking system working 24/7
- Company website not crashing
- Hospital systems available during emergencies

How Availability is Ensured :

- Regular backups
- DDoS protection
- Load balancing

2 IA (INFORMATION ASSURANCE):

- Ensures information is trustworthy throughout its life cycle.

IA focuses on:

- Protecting data
- Managing risks
- Ensuring reliability

IA Includes:

- Confidentiality
- Integrity
- Availability
- Authentication
- Non-repudiation

3 IAAA (SECURITY FRAMEWORK) :

IAAA = Identification, Authentication, Authorization, Accounting

Identification :

Who are you?

User claims identity
No verification yet

Examples:

Username
Email ID
Employee ID

Authentication :

Prove who you are

System verifies identity

- Happens after identification

Examples:

Password
OTP
Fingerprint
Face ID

🎯 Authorization :

👉 *What are you allowed to do?*

Defines permissions
Happens after authentication
Examples:
Student → View marks
Teacher → Edit marks
Admin → Full access

📊 Accounting (Auditing) :

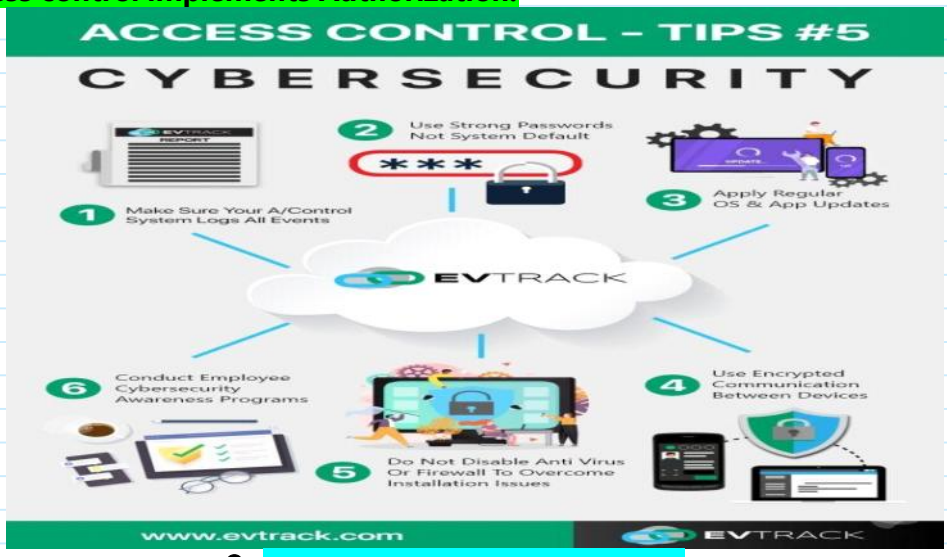
👉 *Tracking user activities*

Logs user actions
Used for monitoring & investigation

Examples:
Login time
Files accessed
Changes made

4️⃣ ACCESS CONTROL :

- Mechanism that decides who can access what resources.
- Access control implements Authorization.



🔐 Types of Access Control :

1️⃣ Mandatory Access Control (MAC) :

- Controlled by system
- Very strict
- Used in military

Example: Classified government files

2️⃣ Discretionary Access Control (DAC):

- Owner decides permissions

Example: File sharing in Windows

3 Role-Based Access Control (RBAC) :

- Access based on job role

Example:

- HR → employee data
- Finance → payment data

⭐ *Most commonly used in organizations*

4 Attribute-Based Access Control (ABAC) :

- Access based on attributes

Attributes:

- Time
- Location
- Device
- Role

📌 Access Control Components :

- Policies
- Rules
- Permissions
- Access enforcement

5 RISK MANAGEMENT :

Possibility of loss or damage

Risk = Threat × Vulnerability × Impact

🔐 Risk Management :

Identifying, analyzing, and reducing risks

🔁 Risk Management Steps :

- Identify assets
- Identify threats
- Identify vulnerabilities
- Assess risk
- Apply controls
- Monitor continuously.

5 PRIVACY :

- ***Protecting personal data and user rights.***

Personal Data Examples :

- **Name**
- **Phone number**
- **Aadhaar / SSN**
- **Email**
- **Location**
- **Biometric data**

Privacy Principles :

1. **Data minimization – Collect only needed data**
2. **Consent – User permission required**
3. **Transparency – Inform data usage**
4. **Purpose limitation – Use data only for stated reason**
5. **Data protection – Secure the data**

COMMON CYBER THREATS :

1 MALWARE :

- Malware is any software designed to harm, damage, or gain unauthorized access to a computer or network.
- Malware – Viruses, worms, trojans, ransomware

◇ Types of Malware :

Virus :

- Attaches itself to files.
- Spreads when infected file is opened.
- Can corrupt or delete data.

Example: Infected USB drive.

Worm :

- Spreads automatically over networks
- Does not need user action

Example: Rapidly spreading network infection

Trojan :

- Looks like a legitimate program
- Performs malicious activity secretly

Example: Fake software download

Ransomware :

- Encrypts files
- Demands money to unlock them

Example: "Pay money or lose your data"

2 PHISHING :

- Phishing is a cyber attack where attackers send fake emails, messages, or websites to trick users into revealing sensitive information.

◇ Common Phishing Targets :

Passwords
Bank details
Credit card numbers
OTPs

Example :

You receive an email saying:

"Your bank account is blocked. Click here to verify."

The link is fake and steals your details.

Types of Phishing :

- Email phishing
- SMS phishing (Smishing)
- Voice phishing (Vishing)

3 HACKING :

Hacking is the act of gaining unauthorized access to systems, networks, or data.

How Hackers Gain Access :

- Weak passwords
- Software vulnerabilities
- Unpatched systems
- Social engineering

Example :

Breaking into someone’ s email account.
Accessing company servers illegally.

4 DDoS ATTACKS (Distributed Denial of Service) :

- A DDoS attack floods a server or website with huge traffic, making it slow or unavailable for legitimate users.

How DDoS Works :

- Thousands of infected systems send requests at once
- Server becomes overloaded
- Website crashes

Example

Online shopping website goes down during sale
Bank website unavailable

Impact of DDoS :

Website downtime
Loss of customers
Revenue loss

5 INSIDER THREATS :

- An insider threat occurs when employees or trusted users misuse their access, intentionally or unintentionally.

Types of Insider Threats :

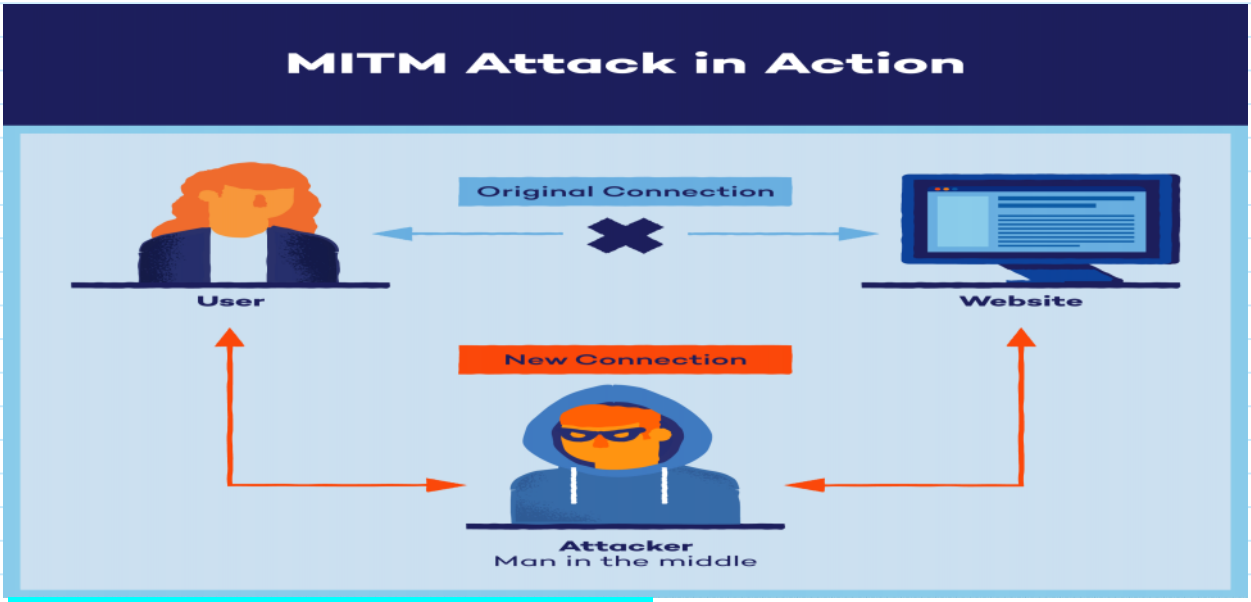
Malicious employee stealing data
Careless employee clicking malicious links
Former employee still having access

Example :

Employee copying confidential company data
Sharing passwords with others

6 MAN-IN-THE-MIDDLE (MITM) ATTACK :

- A Man-in-the-Middle (MITM) attack occurs when an attacker secretly places themselves between two communicating parties (user and server) and intercepts, reads, or alters the communication without their knowledge.



How MITM Attack Works (Step-by-Step) :

1. User sends data (login details)
2. Attacker intercepts the data
3. Attacker forwards it to the server
4. Neither user nor server knows about the attacker

Real-Life Example :

- You connect to free public Wi-Fi at a café
- You log in to your bank website
- Attacker captures your username and password

Common Types of MITM Attacks :

- Wi-Fi Eavesdropping
- Session hijacking
- ARP spoofing
- DNS spoofing
- SSL stripping

Impact of MITM Attacks :

- Password theft
- Bank fraud
- Identity theft
- Data manipulation

Prevention Methods :

- Use HTTPS websites
- Avoid public Wi-Fi for sensitive work
- Use VPN
- Enable encryption
- Keep systems updated

7 ZERO-DAY ATTACK :

A Zero-Day attack exploits a software vulnerability that is unknown to the software developer and for which no patch or fix exists yet.

Why Is It Called "Zero-Day"?

- Developers have zero days to fix the vulnerability

- Attackers discover and exploit it before anyone else knows

🔁 How a Zero-Day Attack Works (Step-by-Step) :

1. Unknown vulnerability exists in software
2. Attacker discovers the flaw
3. Attacker exploits it secretly
4. Damage occurs before a fix is released

❌ Why Zero-Day Attacks Are Dangerous :

- No immediate defense available
- Antivirus may not detect it
- High success rate
- Can cause massive damage

🔐 Prevention of Zero-Day Attacks :

- Regular software updates
- Use intrusion detection systems
- Behavior-based security tools
- Network monitoring
- Least-privilege access

Basic Cybersecurity Protection Methods :

Protection Methods :

- ⭐ Strong, unique passwords
- ⭐ Two-Factor Authentication (2FA)
- ⭐ Firewalls
- ⭐ Antivirus / Anti-malware
- ⭐ Encryption
- ⭐ Regular software updates
- ⭐ Data backups

CYBERSECURITY DOMAINS :

Cybersecurity is divided into different domains, where each domain focuses on protecting a specific part of IT systems.

1️⃣ NETWORK SECURITY :

- ⭐ Network Security focuses on protecting computer networks and the data moving through them from unauthorized access, attacks, and misuse.

🧠 What Does It Protect :

Routers
Switches
Servers
Network traffic
Internet connections

⚠️ Common Network Threats :

Hacking
Man-in-the-Middle attacks
DDoS attacks
Packet sniffing

Network Security Tools & Methods :

Firewalls
Intrusion Detection Systems (IDS)
Intrusion Prevention Systems (IPS)
VPN (Virtual Private Network)
Network monitoring

2 APPLICATION SECURITY :

★ Application Security involves protecting software and applications from vulnerabilities and attacks throughout their lifecycle.

What Does It Protect :

Web applications
Mobile apps
Software programs
APIs

⚠ Common Application Threats :

SQL Injection
Cross-Site Scripting (XSS)
Broken authentication
Software bugs

Application Security Techniques :

Secure coding practices
Regular patching and updates
Application testing
Web Application Firewalls (WAF)

3 INFORMATION SECURITY :

★ Information Security (InfoSec) focuses on protecting data and information from unauthorized access, modification, or destruction.

What Does It Protect:

Digital data
Physical documents
Databases
Emails
Files

⚠ Common Information Threats :

Data breaches
Unauthorized access
Data leaks
Insider threats

Information Security Measures :

Encryption
Access control
Data classification
Backup and recovery

4 CLOUD SECURITY :

★ Cloud Security refers to protecting data, applications, and services stored in cloud environments.

What Does It Protect :

Cloud servers
Online storage
Cloud-based applications
Virtual machines

⚠ Common Cloud Threats :

Data exposure
Misconfigured cloud settings
Account hijacking
Insecure APIs

Cloud Security Techniques :

Identity and Access Management (IAM)
Encryption
Secure configurations
Continuous monitoring

5 ENDPOINT SECURITY :

★ Endpoint Security protects end-user devices that connect to a network.

What Does It Protect :

Desktop computers
Laptops
Mobile phones
Tablets

⚠ Common Endpoint Threats :

Malware
Ransomware
Phishing attacks
USB-based attacks

Endpoint Security Measures :

Antivirus software
Device encryption
Regular updates
Endpoint Detection and Response (EDR)