

1/15/2026

# Basics of Cyber Security

- ★ The CIA triad in Cyber Security
- ★ Types of Attacks
- ★ Attack surfaces

# The CIA Traids In Cybersecurity

The CIA Triad is a core concept in Cyber Security. It represents the three main principles used to protect information systems.

The CIA in cyber security are:

- Confidentiality
- Integrity
- Availability

## 1. Confidentiality

Only authorized people can access data

**Purpose:**

Prevents unauthorized access to sensitive information

### **Examples:**

Passwords & PINs

Encryption (AES, RSA)

Access control (Login, OTP, biometrics)

### **Real-life example:**

Only you can read your WhatsApp messages

## **2. Integrity**

Data must be accurate and not altered

### **Purpose:**

Ensures data is not changed or tampered with

### **Examples:**

Hashing (SHA-256)

Digital signatures

Checksums

**Real-life example:**

Bank balance should not change without a valid transaction

### **3. Availability**

Data and systems must be accessible when needed

**Purpose:**

Ensures systems are up and running

**Examples:**

Backup systems

Load balancing

Protection against DDoS attacks

**Real-life example:**

ATM should work anytime you need cash

# Attackers In Cybersecurity

In Cyber Security, attackers are classified based on skill, intent, and access level.

## Types of Attackers

### 1 Script Kiddies

- ◆ Beginners who use ready-made tools
- ◆ No deep technical knowledge

Example: Using free hacking apps to deface websites

### 2 Black Hat Hackers

- ◆ Hack for personal gain or damage

- ◆ Illegal activities

**Example:** Stealing passwords, spreading malware

### 3 White Hat Hackers (Ethical Hackers)

- ◆ Hack legally to find vulnerabilities
- ◆ Work for companies

**Example:** Penetration testers

### 4 Gray Hat Hackers

- ◆ Mix of white & black hat
- ◆ May break rules but not for personal harm

**Example:** Finding a bug and informing the company without permission

## 5 Insiders

- ◆ Employees or trusted people
- ◆ Already have system access

**Example:** Employee leaking company data

## 6 Hacktivists

- ◆ Politically or socially motivated
- ◆ Attack to spread a message

**Example:** Website defacement for protests



## 7 Cyber Criminals

- ◆ Organized groups
- ◆ Financial motivation

**Example:** Ransomware gangs, credit card fraud

## 8 State-Sponsored Attackers

- ◆ Government-backed
- ◆ Highly skilled & well funded

**Example:** Cyber espionage, cyber warfare

# Attack Surface in Cyber Security

Attack Surface refers to all possible points where an attacker can try to enter, attack, or extract data from a system.

## Types of Attack Surfaces

### 1 Network Attack Surface

◆ Points exposed through a network

#### Examples:

Open ports

IP addresses

Firewalls & routers

Wi-Fi networks

**Example:** Open port 21 (FTP) can be attacked

### 2 Application Attack Surface

## ◆ Vulnerabilities in software and applications

### **Examples:**

Web applications

APIs

Login forms

SQL Injection, XSS

**Example:** Weak login page in a website

## 3 Physical Attack Surface

### ◆ Physical access to devices

### **Examples:**

USB ports

Laptops

Servers

Unlocked systems

**Example:** Attacker plugs in a malicious USB

#### 4 Human Attack Surface

◆ Weakness due to human behavior

**Examples:**

Phishing emails

Weak passwords

Social engineering

**Example:** Employee clicks fake email link

---

DAY-TO-DAY APPS

# Basics of Cyber Security

- ★ The CIA triad in Cyber Security
- ★ Types of Attackers
- ★ Attack surfaces