

Cyber Security

Cyber security is the practice of protecting systems, networks, and data from digital attacks.

Its main goal is to ensure that information remains secure, accurate, and accessible even in the presence of threats.

The foundation of cyber security is built on the CIA Triad.

CIA Triad

The CIA Triad consists of three key principles:

Confidentiality

Confidentiality ensures that information is accessed only by authorized users.

Examples:

Password-protected email accounts

Encrypted bank transactions

Two-factor authentication (OTP)

Threats:

Data breaches

Phishing attacks

Unauthorized access

Integrity

Integrity ensures that data is accurate and not altered without permission.

Examples:

Exam results stored in a university database

Transaction records in banking systems

Security Measures:

Hashing

Digital signatures

Access control mechanisms

Availability

Availability ensures that systems and data are accessible when required.

Examples:

Hospital management systems

Online banking services

Threats:

Denial of Service (DoS/DDoS) attacks

Server failures

Ransomware

Types of Attackers

Different attackers have different motivations and skill levels.

Script Kiddies

Beginners using pre-made hacking tools

Attack systems for fun or attention

Insider Threats

Employees or authorized users

May leak data intentionally or accidentally

Hactivists

Motivated by political or social causes

Attack websites to spread messages or protest

Nation-State Attackers

Government-sponsored hackers

Highly skilled and well-funded

Target critical infrastructure and defense systems

Attack Surfaces

An attack surface is any point where an attacker can try to exploit a system.

Web Applications

SQL Injection

Cross-Site Scripting (XSS)

Weak authentication

Mobile Applications

Insecure data storage

Excessive permissions

Weak encryption

APIs

Broken authentication

Exposed endpoints

Poor rate limiting

Network Infrastructure

Open ports

Man-in-the-Middle attacks

Packet sniffing

Cloud Infrastructure

Misconfigured storage buckets

Weak access policies

Publicly exposed services

Data Flow & Attack Points

Typical data flow in daily-use applications:

User → Application → Server → Database

Possible attack points:

Login phase (Phishing, credential theft)

Data transmission (MITM attacks)

Server/database (Malware, data breaches)