Understanding Cyber Security Basics & Attack Surface

What Cyber security means:-

Cyber security means protecting computers, mobile phones, networks, servers, and data from digital attacks. These attacks usually try to steal information, damage systems, or disrupt services.

In simple words

Cyber security is like a lock and security guard for your digital world—it keeps your:-

Personal data safe (passwords, photos, bank details)

Devices secure (phones, laptops, computers)

Online activities protected (email, social media, payments)

What cyber security protects you from

Hacking – unauthorized access to systems

Viruses & malware – harmful software

Phishing – fake emails/messages to steal data

Identity theft – misuse of personal information

Online fraud & scams

Main areas of cyber security

Network Security – protects internet and Wi-Fi networks

Application Security – secures software and apps

Information Security – protects data from theft or loss

Cloud Security – secures data stored online

Cyber Awareness – teaching users safe online behavior

Why cyber security is important

Prevents financial loss

Protects privacy

Keeps government, businesses, and individuals safe

Ensures trust in digital services.

CIA Triad (Confidentiality, Integrity, Availability)

The CIA Triad is the foundation of cyber security. Every secure system—banks, social media, government portals—must protect these three principles.

1 : Confidentiality – Keep data secret

Meaning:-Only authorized people should be able to see sensitive information.

Banking example:- Your ATM PIN, net-banking password, and account balance must be visible only to you.

Banks use:-Passwords & PINs,OTPs,Encryption (data unreadable to hackers)

Social Media example:-Your private chats, saved photos, and email ID are visible only to you or people you allow & Privacy settings & encryption protect this data.

2. Integrity – Keep data correct & unaltered

Meaning:- Data should not be changed without permission.

Banking example:-Your account balance should change only when:

You deposit money

You withdraw money

Hackers must not be able to change:

₹10,000 → ₹1,00,000

Social Media example:- Your posts, profile name, bio, and messages should not be edited by someone else,Only you can delete or edit your posts.

3.Availability – Keep systems accessible:-

Meaning:-Systems and data should be available when needed.

Banking example:- ATM, UPI, and mobile banking should work 24/7.

Banks protect availability using:

Backup servers,Load balancing & Protection against DDoS attacks

Social Media example:-Apps like Instagram or WhatsApp should load anytime.

Servers must handle millions of users at once.

App crashes or stays offline for hours.

Types of cyber Attackers

Security experts usually classify attackers based on skill level, motivation, and resources. Below are the four most discussed attacker types, explained clearly with real-world style examples.

1.Script Kiddies (Beginners)

Low-skilled attackers

Use ready-made tools, scripts, or malware

Often motivated by fun, curiosity, or fame

What security blogs say:-

They don't understand how attacks work deeply

Mostly rely on YouTube tutorials, GitHub tools, or leaked scripts

2.Insider Threats (Most Dangerous)

Employees, ex-employees, or contractors

Already have authorized access

Attacks can be intentional or accidental

What security blogs say:-

One of the top causes of data breaches

Hard to detect because access looks legitimate

3.Hacktivists (Ideology-Driven)

Attack for political, social, or religious reasons

Goal is public attention, not money

What security blogs say:-

Attacks increase during political conflicts

Use website defacement, DDoS, and data leaks

4.Nation-State Actors (Advanced & Powerful)

Government-sponsored hackers

Highly skilled with huge funding

Operate silently for years

What security blogs say:-

Known for Advanced Persistent Threats (APTs)

Targets include banks, power grids, defense, telecom

Attack surfaces

An attack surface is the total set of entry points where an attacker can try to exploit a system. Below is a clear, real-world oriented breakdown of the most common attack surfaces you mentioned, with typical weaknesses and examples.

1.Web Application Attack Surface

What it includes

Login & signup pages

Forms (search, contact, payment)

Cookies & sessions

Admin panels

File upload/download features

Common vulnerabilities

SQL Injection (SQLi) – manipulating database queries

Cross-Site Scripting (XSS) – injecting malicious scripts

Cross-Site Request Forgery (CSRF)

Broken Authentication & Session Management

Insecure File Uploads

Real-world example

A banking website allowing attackers to steal user data through SQL Injection.

A social media site where XSS steals session cookies.

2. Mobile Application Attack Surface

What it includes

Mobile app code (APK / IPA)

Local storage (SQLite, shared preferences)

App permissions

Backend APIs

Communication with servers

Common vulnerabilities

Hardcoded credentials & API keys

Insecure local storage

Weak encryption

Improper certificate validation (MITM attacks)

Excessive permissions

Real-world example

A food delivery app storing user tokens in plaintext.

Attackers reverse-engineering APKs to extract API keys.

3. API Attack Surface

What it includes

REST / GraphQL endpoints

Authentication tokens (JWT, OAuth)

Input parameters

Rate limits

Common vulnerabilities

Broken Object Level Authorization (BOLA)

Broken Authentication

Excessive data exposure

Lack of rate limiting

Mass assignment

Real-world example

Changing a user ID in an API request to access another user's data.

No rate limit → brute-force OTP attacks.

4. Network Attack Surface

What it includes

Routers & switches

Open ports & services

Firewalls

Wi-Fi networks

VPNs

Common vulnerabilities

Open or unused ports

Weak passwords

Outdated protocols (FTP, Telnet)

Man-in-the-Middle (MITM) attacks

Misconfigured firewalls

Real-world example

Public Wi-Fi sniffing passwords.

Open SSH port brute-forced by attackers.

5. Cloud Infrastructure Attack Surface

What it includes

Cloud servers (VMs)

Storage buckets

IAM roles & permissions

Containers & Kubernetes

Cloud APIs

Common vulnerabilities

Misconfigured storage (public buckets)

Over-privileged IAM roles

Exposed cloud keys

Unpatched virtual machines

Insecure container images

Real-world example

A public cloud storage bucket leaking customer data.

Stolen AWS keys used for crypto-mining.

OWASP Vulnerabilities

The OWASP Top 10 is a globally recognized list of the most critical security vulnerabilities affecting web applications. It's published by OWASP and is widely used by developers, testers, and security teams.

OWASP Top 10 Vulnerabilities

1. Broken Access Control

What it means:

Users can access data or actions they shouldn't.

Example:

Changing /user/123 to /user/124 and seeing someone else's data.

Impact:

Data theft, account takeover

2.Cryptographic Failures

What it means:

Sensitive data is not properly encrypted.

Example:

Passwords stored in plain text

Website using HTTP instead of HTTPS

Impact:

Data leaks, privacy violations

3. Injection

What it means:

Untrusted input is sent to an interpreter (SQL, OS, LDAP).

Example:

SQL Injection to bypass login

' OR '1'='1

Impact:

Database compromise, full system access

4. Insecure Design

What it means:

Security is missing at the design level.

Example:

No account lockout after failed login attempts

Impact:

Logic abuse, fraud

5.Security Misconfiguration

What it means:

Improper or default security settings.

Example:

Admin panel exposed

Default passwords still active

Impact:

Unauthorized system access

6. Vulnerable & Outdated Components

What it means:

Using old libraries or frameworks with known flaws.

Example:

Old WordPress plugins

Unpatched Apache server

Impact:

Remote code execution, data breach

7. Identification & Authentication Failures

What it means:

Weak login and session handling.

Example:

Weak passwords

No MFA

Session IDs not expiring

Impact:

Account hijacking

8. Software & Data Integrity Failures

What it means:

Untrusted software updates or CI/CD pipelines.

Example:

Compromised updates

Malicious third-party plugins

Impact:

Supply chain attacks

9.Security Logging & Monitoring Failures

What it means:

Attacks are not detected or logged.

Example:

No alerts on multiple failed login attempts

Impact:

Attackers stay hidden longer

10. Server-Side Request Forgery (SSRF)

What it means:

Server is tricked into making malicious requests.

Example:

Attacker accesses internal cloud metadata services

Impact:

Cloud takeover, internal data exposure

Summary

Cybersecurity is the practice of protecting data, systems, and applications from attacks. Its main goal is to maintain the CIA Triad:

Confidentiality (data stays private), Integrity (data stays accurate), and Availability (systems stay accessible).

Every system has attack surfaces such as web apps, mobile apps, APIs, networks, and cloud services where attackers can try to break in. Many attacks exploit common weaknesses listed in the OWASP Top 10.

Data flows from user → application → server → database, and security is required at each step. Different attackers—script kiddies, insiders, hacktivists, and nation-states—target these weaknesses for different reasons.

In short: cybersecurity is about identifying weak points and protecting every layer of a system.