Understanding Cyber Security Basics & Attack Surface

Cybersecurity is the practice of protecting computers, networks, systems, and data from cyber threats such as hacking, viruses, malware, and unauthorized access.
Its purpose is to keep information safe, accurate, and accessible only to authorized users.
Cybersecurity helps prevent data theft, fraud, system damage, and service disruptions.

In simple terms:
👉 Cybersecurity means staying safe and protected when using digital technology and the internet.

Examples include:
* Securing online banking and payment systems
* Protecting social media accounts from hackers
* Defending computers and websites against viruses and cyberattacks

Its core principles are defined by the CIA Triad:

a) Confidentiality 🔐
Ensures that information is only accessible to authorized users.

Examples
* Banking: Online banking uses passwords, PINs, and one-time codes to protect customer accounts.

Financial data is encrypted so attackers cannot read it

* Social Media: Private messages are protected with encryption.
Privacy settings control who can see posts and personal details.

If confidentiality fails, data breaches and identity theft can occur.

b) Integrity 🛡️

Ensures that data remains accurate, complete, and unaltered without authorization.

Examples
* Banking: Transaction amounts must not be changed by attackers.
Secure logs ensure all financial records are trustworthy.

* Social Media: Posts or profiles should not be modified by hackers.
Verified accounts help confirm content authenticity.

Loss of integrity can lead to fraud and misinformation.

c) Availability 🌐

Ensures that systems and data are accessible when needed.

Examples
* Banking: Customers expect 24/7 access to ATMs and online banking.
  Backup servers prevent downtime.

* Social Media: Platforms must remain online even during heavy traffic.
  Protection against DDoS attacks keeps services available.

When availability is compromised, users cannot access critical services.

Types of Cyber Attackers

Cyber attackers are individuals or groups that attempt to gain unauthorized access to systems, networks, or data. They differ in skills, motivation, and impact. Below are the main types of cyber attackers commonly discussed in cybersecurity.

---

1. Script Kiddies

Description: Inexperienced attackers who use pre-made tools and scripts created by others.
Motivation: Curiosity, fun, or gaining attention.
Skill Level: Low.
Example: Using downloadable software to deface websites or run simple denial-of-service attacks.

2. Insiders

Description: Employees, contractors, or trusted users with legitimate access to systems.
Motivation: Revenge, financial gain, or accidental mistakes.
Skill Level: Varies.
Example: An employee leaking customer data or misusing company credentials.

3. Hacktivists

Description: Attackers driven by political, social, or ideological causes.

Motivation: Protest, activism, or spreading a message.
Skill Level: Medium.
Example: Defacing government websites or launching attacks to support a cause.

4. Cybercriminals

Description: Organized individuals or groups focused on financial gain.
Motivation: Money.
Skill Level: Medium to high.
Example: Phishing scams, ransomware attacks, and credit card theft.

5. Nation-State Actors

Description: Government-sponsored attackers
Motivation: Espionage, surveillance, sabotage, or cyber warfare.
Skill Level: Very high.
Example: Attacks on power grids, military systems, or national infrastructure.

6. Terrorist Groups

Description: Groups using cyber attacks to create fear or disrupt society.
Motivation: Ideological or religious goals.
Skill Level: Medium to high.
Example: Attacking public services or spreading propaganda online.

##Common Attack Surfaces

An attack surface is any point where an attacker can try to gain unauthorized access to a system, network, or data. The larger the attack surface, the more opportunities attackers have to exploit weaknesses.

Below are the most common attack surfaces in cybersecurity.

1. Web Applications

Web applications are one of the most frequently targeted attack surfaces.
Examples
Login pages
Search bars
Online forms

Common Threats
SQL Injection 👉 SQL Injection ka matlab hai database ko galat SQL commands dekar data chori ya change karna.
Cross-Site Scripting (XSS) 👉 XSS ka matlab hai user ko attack karna website ke zariye.
Broken authentication 👉 Broken authentication ka matlab hai login system ka properly secure na hona.
Real-world example
An attacker exploits a vulnerable login form to access a database containing user details.

2. Mobile Applications

Mobile apps often store sensitive user data and connect to backend services.
Common Threats
Insecure data storage
Weak authentication
Reverse engineering
Real-world example
A poorly secured app stores passwords in plain text on a device.

3. APIs (Application Programming Interfaces)

APIs allow different software systems to communicate.
Common Threats
Exposed endpoints
Broken access control
Data overexposure
Real-world example
An attacker abuses an unsecured API to retrieve private user data.

4. Networks

Networks include wired and wireless connections.
Common Threats
Man-in-the-Middle (MITM) attacks
Unauthorized access
Weak Wi-Fi security
Real-world example
An attacker intercepts data on an unsecured public Wi-Fi network.

5. Cloud Infrastructure

Cloud environments host applications and data remotely.
Common Threats

Misconfigured storage
Weak identity and access management (IAM)
Lack of monitoring
Real-world example
A public cloud storage bucket exposes sensitive company files.

6. Endpoints (User Devices)

Endpoints include laptops, desktops, and mobile devices.
Common Threats
Malware
Phishing
Unpatched software
Real-world example
A phishing email installs malware on an employee’s laptop.

7. Human Attack Surface

People are often the weakest link in security.
Common Threats
Social engineering
Phishing
Password reuse
Real-world example
An employee is tricked into sharing login credentials.

##OWASP Top 10 – Why These Vulnerabilities Are Dangerous

The OWASP Top 10 is a list of the most critical web application security risks.

1. Broken Access Control

Users can access data or actions they should not.
Danger: Attackers can view or modify other users’ data.

2. Cryptographic Failures

Sensitive data is not properly encrypted.
Danger: Passwords, credit card details can be stolen.

3. Injection (SQL Injection, Command Injection)

Malicious input is executed as commands.
Danger: Database data theft or deletion.

4. Insecure Design

Security not considered during app design.
Danger: Even well-coded apps can be insecure.

5. Security Misconfiguration

Default settings, open ports, unnecessary services.
Danger: Easy entry point for attackers.

6. Vulnerable and Outdated Components

Old libraries or frameworks used.
Danger: Known vulnerabilities can be exploited.

7. Identification & Authentication Failures

Weak login and session handling.
Danger: Account takeover.

8. Software and Data Integrity Failures

Untrusted updates or code execution.
Danger: Malware injection.

9. Security Logging and Monitoring Failures

Attacks go unnoticed.
Danger: Breaches stay hidden longer.

10. Server-Side Request Forgery (SSRF)

Server is tricked into making malicious requests.
Danger: Internal systems exposed.

##Mapping Daily-Used Apps to Attack Surfaces

Email Applications

Attack surfaces: Login page, attachments, links
Threats: Phishing, malware, account hijacking

WhatsApp / Messaging Apps

Attack surfaces: Messages, media files, APIs
Threats: Malicious links, account takeover, data leakage

Banking Apps

Attack surfaces: Login, APIs, databases, mobile app
Threats: SQL injection, broken authentication, malware

##Data Flow: User → Application → Server → Database

Typical data flow:

User

Enters data (login, message, transaction)
Application (Web/Mobile App)
Validates input
Sends request to server
Server
Processes logic
Communicates with database
Database
Stores or retrieves data
Response
Data goes back to user

##Final Summary

Cybersecurity is about protecting data, systems, and users from digital threats. The OWASP Top 10 highlights the most dangerous vulnerabilities that attackers commonly exploit. Everyday apps like email, WhatsApp, and banking applications have multiple attack surfaces, from login pages to APIs and databases.
Data flows from the user to the application, then to the server and database, and attacks can

occur at any point if security controls are weak. Understanding how data moves and where vulnerabilities exist helps in preventing attacks before they happen.