Cybersecurity Basics & Attack Surface: Comprehensive Guide

1. The Foundation: The CIA Triad

The **CIA Triad** is the gold standard for information security. Every security control or attack can be mapped back to these three principles.

- **Confidentiality:** Ensuring that sensitive information is accessed only by authorized parties.
    - *Real-World Example (Banking):* Your bank uses encryption so that only you and the bank can see your account balance. If a hacker intercepts the data but cannot read it, confidentiality is maintained.
- **Integrity:** Ensuring that data is accurate, complete, and has not been tampered with.
    - *Real-World Example (social media):* When you post a message, integrity ensures that the message received by your friends is exactly what you typed, not modified by a third party.
- **Availability:** Ensuring that systems and data are accessible when needed by authorized users.
    - *Real-World Example:* A DDoS (Distributed Denial of Service) attack on a banking app prevents you from paying bills. This is a failure of availability.

2. Identifying the Attackers (Threat Actors)

Understanding *who* is attacking helps in predicting *how* they will attack.

Attacker Type	Motivation	Skill Level
Script Kiddies	Thrill, bragging rights	Low (uses pre-made tools)
Insiders	Revenge, financial gain	High (has authorized access)
Hacktivists	Political or social change	Varied (targets specific orgs)
Nation-State Actors	Espionage, warfare	Very High (highly funded/stealthy)
Cybercriminals	Financial profit	Moderate to High

3. **Understanding the Attack Surface**

An **Attack Surface** is the sum of all points (the "vectors") where an unauthorized user can try to enter or extract data from an environment.

- **Web Applications:** Vulnerabilities in code (like login forms or search bars).
- **Mobile Apps:** Insecure data storage on the phone or weak communication with the server.
- **APIs:** The "bridges" between software. If unsecured, they allow direct access to databases.
- **Networks:** Open Wi-Fi, unpatched routers, or exposed ports (like SSH or RDP).
- **Cloud Infrastructure:** Misconfigured S3 buckets or weak Identity and Access Management (IAM) roles.

4. **Data Flow & Vulnerability Mapping**

To secure a system, you must understand how data moves.

The Flow: User $\rightarrow$ Application $\rightarrow$ Server $\rightarrow$ Database

Where Attacks Happen:

1. **At the User/Browser:** Phishing, Session Hijacking.
2. **During Transit (User to App):** Man-in-the-Middle (MitM) attacks if HTTPS isn't used.
3. **At the Application:** Injection attacks (SQLi, XSS) where the app "trusts" malicious user input.
4. **At the Database:** Unauthorized access or data exfiltration.

5. **OWASP Top 10 Highlights**

The Open Web Application Security Project (OWASP) lists the most critical risks. Key examples include:

- **Broken Access Control:** Users can access data outside of their permissions (e.g., viewing another user's private profile).

- **Cryptographic Failures:** Using weak encryption or plain text for sensitive data like passwords.
- **Injection:** Sending malicious code to an interpreter (e.g., SQL Injection to bypass login).