Cyber Security Basics & Attack Surface

1. What is Cyber Security?

Cyber Security means protecting computers, mobile phones, networks, and data from hackers. It helps keep our personal and important information safe.

CIA Triad (Main Goals of Cyber Security)

Confidentiality: Only the right people can see the data (example: bank password).

Integrity: Data should not be changed by hackers (example: bank amount).

Availability: Systems should work when we need them (example: banking app online).

2. Types of Attackers

Script Kiddies: Beginners who use ready-made hacking tools.

Insiders: Employees who misuse company access.

Hacktivists: Hackers who attack for political or social reasons.

Nation-State Attackers: Government-supported hackers.

3. Attack Surface (Where Attacks Happen)

Web Applications: Login pages, forms, websites.

Mobile Apps: Android and iOS applications.

APIs: Connections between app and server.

Network: Wi-Fi, internet connections.

Cloud: Online servers and storage.

Attack Surface Diagram

User
↓
Web / Mobile App
↓
API
↓
Server
↓
Database

4. OWASP Top 10 (Simple)

OWASP Top 10 is a list of the most dangerous web security problems. Examples are SQL Injection, weak passwords, and wrong server settings.

5. Daily Application Example

Example: WhatsApp or Banking App
User → Mobile App → Internet → Server → Database
Possible attacks: phishing, fake links, data stealing.

6. Data Flow Diagram

User
↓ (login, message, payment)
Application
↓
Server
↓
Database
↑
Response back to User

7. Where Attacks Can Occur

User Side: Phishing emails, fake apps.

Network: Man-in-the-middle attack.

Server: Unpatched software.

Database: Data leaks, SQL injection.

8. Summary

Cyber Security helps protect data and systems from attackers. By understanding attacker types, attack surfaces, and data flow, we can build safer applications and networks.