1. Meaning of Cyber Security (CIA Triad)

Cyber Security is the practice of protecting systems, networks, applications, and data from cyber attacks, unauthorized access, and damage.

It is built on the **CIA Triad**:

a) Confidentiality

Ensures that information is accessible **only to authorized users**.

Real-world examples:

- **Banking apps** use passwords, OTPs, and encryption to protect account details.
- **Social media platforms** like WhatsApp use end-to-end encryption to protect chats.

Failure example:
If a hacker steals login credentials → confidentiality is compromised.

---

b) Integrity

Ensures that data is **accurate, complete, and unaltered**.

Real-world examples:

- Bank transaction amounts should not be modified.
- Exam results stored online must remain unchanged.

Failure example:
If transaction data is modified during transfer → integrity is compromised.

---

c) Availability

Ensures that systems and services are **available when required**.

Real-world examples:

- Online banking services must be available 24/7.
- Email services should not go offline.

Failure example:
DDoS attacks that crash a website → availability is compromised.

---

2. Types of Attackers (From Security Blogs)

1. Script Kiddies

- Beginners using ready-made hacking tools
- Little technical knowledge

Example:
Website defacement using downloaded tools.

---

2. Insiders

- Authorized users who misuse access

Example:
An employee leaking customer data.

---

3. Hacktivists

- Attack systems for political or social causes

Example:
Defacing government websites to protest policies.

---

4. Nation-State Actors

- Government-sponsored attackers
- Highly skilled and well-funded

Example:
Cyber-espionage or cyber warfare between countries.

---

3. Common Attack Surfaces

An **attack surface** is any point where an attacker can attempt to gain access.

Major Attack Surfaces:

- **Web applications** (login pages, forms)
- **Mobile applications** (banking, payment apps)
- **APIs** (communication between services)
- **Networks** (Wi-Fi, routers)
- **Cloud infrastructure** (AWS, Azure, Google Cloud)

---

4. OWASP Top 10 Vulnerabilities (Why They Are Dangerous)

OWASP Top 10 lists the **most critical web application security risks**.

Key examples:

- **Broken Access Control** – Unauthorized access to restricted areas

- **Injection (SQL Injection)** – Malicious database queries
- **Authentication Failures** – Weak passwords, no MFA
- **Security Misconfiguration** – Default credentials, open ports
- **Cross-Site Scripting (XSS)** – Execution of malicious scripts

Why dangerous?

- Lead to data breaches
- Allow account takeover
- Can result in full system compromise

---

5. Mapping Daily-Used Applications to Attack Surfaces

Application	Possible Attack Surface
Email	Phishing emails, weak passwords
WhatsApp	Malware links, account hijacking
Banking Apps	Insecure APIs, fake applications
Social Media	XSS, session hijacking

---

6. Data Flow: User → Application → Server → Database

Example: Online Banking Login

1. User enters credentials
2. Application receives the request
3. Request is sent to the server
4. Server checks data in the database
5. Response is sent back to the user

---

7. Possible Attack Points in the Data Flow

Stage	Possible Attacks
User	Phishing, malware
Application	XSS, fake apps
Network	Man-in-the-Middle attack

Stage	Possible Attacks
Server	SQL Injection, privilege escalation
Database	Data theft, data tampering

---

8. Final Summary (In My Own Words)

Cyber security protects digital systems by ensuring confidentiality, integrity, and availability of data. Different attackers—from beginners to nation-state actors—exploit various attack surfaces such as web apps, mobile apps, APIs, and cloud systems. The OWASP Top 10 highlights common vulnerabilities that can cause serious security breaches. Understanding how data flows from the user to the database helps identify attack points and apply proper security controls to prevent cyber attacks.