TASK 1 CS

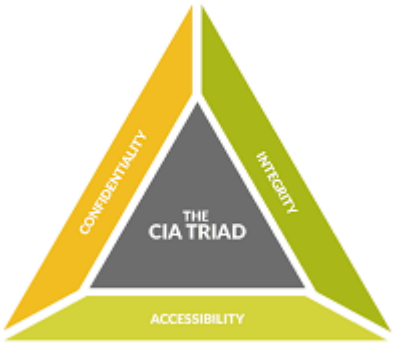
This guide serves as a comprehensive overview of the fundamental pillars of cybersecurity, moving from core principles to the practical identification of vulnerabilities.

---

1. The Core Principles: The CIA Triad

The **CIA Triad** is a model designed to guide policies for information security within an organization.

Pillar	Definition	Real-World Example
Confidentiality	Ensuring that sensitive information is accessed only by authorized parties.	**Banking:** Using multi-factor authentication (MFA) to ensure only you can see your account balance.
Integrity	Maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.	**Social Media:** Ensuring that when you post a status, it cannot be altered by another user or a malicious actor.
Availability	Ensuring that information and resources are available to users when they need them.	**E-commerce:** Ensuring a website stays online and functional during high-traffic events like Black Friday.



2. The Threat Landscape: Types of Attackers

Understanding *who* is attacking helps professionals build better defenses.

- **Script Kiddies:** Unskilled individuals who use pre-existing scripts or programs to launch attacks, usually for thrill or basic disruption.
- **Insiders:** Current or former employees who have authorized access to a network and misuse it to steal data or cause damage.

- **Hacktivists:** Individuals or groups who hack for political or social motives (e.g., Anonymous).
- **Nation-State Actors:** Highly sophisticated, government-funded groups targeting critical infrastructure or engaging in espionage.

---

3. Common Attack Surfaces

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

- **Web Applications:** Forms, login pages, and scripts that can be exploited (e.g., SQL Injection).
- **Mobile Apps:** Insecure data storage on the device or weak communication with the backend.
- **APIs:** The "bridges" between software; if unauthenticated, they can leak massive amounts of data.
- **Cloud Infrastructure:** Misconfigured storage buckets (like AWS S3) that leave data public to the internet.

---

4. The OWASP Top 10 (Critical Vulnerabilities)

The Open Web Application Security Project (OWASP) maintains a list of the most critical web security risks. Key examples include:

1. **Broken Access Control:** Users can access data outside of their intended permissions.
2. **Cryptographic Failures:** Sensitive data (passwords, CC numbers) is transmitted or stored in plain text.
3. **Injection:** An attacker sends disguised code to a system to make it execute unintended commands.

---

5. Data Flow and Attack Points

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

Typical Flow:

User (Browser/App) → Internet (Network) → Web Server → Database

Where attacks happen in this flow:

- **At the User:** Phishing or session hijacking.
- **In Transit:** "Man-in-the-Middle" attacks where data is intercepted on public Wi-Fi.
- **At the Server:** Exploiting unpatched software or weak configurations.
- **At the Database:** Stealing the entire "crown jewels" of data through injection attacks.

---

6. Summary for Clarity

Cybersecurity is not just about "hacking"; it is the continuous process of protecting the **CIA** of data. By identifying the **Attackers** (Who), mapping the **Attack Surface** (Where), and monitoring the **Data Flow** (How), we can apply frameworks like the **OWASP Top 10** to mitigate risks and keep systems resilient.

Would you like me to create a mock "Security Audit" for a specific app, like WhatsApp or a banking app, based on these hints?