Task One: Cybersecurity Fundamentals

1. What is Cybersecurity? (CIA Triad)

Cybersecurity refers to the methods, technologies, and practices used to protect computers, networks, applications, and data from unauthorized access, attacks, damage, or disruption. The foundation of cybersecurity is based on three key principles known as the **CIA Triad**: Confidentiality, Integrity, and Availability.

a) Confidentiality

Confidentiality ensures that sensitive information is only accessible to authorized users and is protected from unauthorized disclosure.

Real-world examples:

- **Banking systems:** Personal and financial data such as account numbers, balances, and transaction history are protected using passwords, PINs, encryption, and multi-factor authentication.
- **Social media and messaging apps:** Applications like WhatsApp use end-to-end encryption so that only the sender and receiver can read the messages.

If confidentiality is compromised, attackers may steal personal data, financial information, or business secrets, leading to identity theft or financial loss.

---

b) Integrity

Integrity ensures that data remains accurate, complete, and trustworthy throughout its lifecycle and is not modified without proper authorization.

Real-world examples:

- **Online banking transactions:** The amount sent by a user should remain unchanged while being processed.
- **Healthcare records:** Patient information must remain accurate to avoid medical errors.

Loss of integrity can result in incorrect data, fraud, legal issues, and loss of trust in systems.

---

c) Availability

Availability ensures that systems, services, and data are accessible to authorized users whenever needed.

Real-world examples:

- **E-commerce websites:** Customers expect platforms to be available during peak shopping times.
- **Cloud services:** Businesses rely on constant access to cloud-based applications and data.

Attacks such as Distributed Denial of Service (DDoS), hardware failures, or misconfigurations can reduce availability and cause service outages.

2. Types of Attackers

Cyber attackers differ in skills, resources, and motivations. Understanding attacker types helps organizations prepare better defenses.

- **Script Kiddies:**
  Individuals with limited technical knowledge who use pre-made tools or scripts created by others. They often target easy vulnerabilities for fun, curiosity, or recognition.
- **Insiders:**
  Employees, contractors, or partners who have legitimate access to systems. Insider threats may be intentional (data theft) or unintentional (accidental data leaks).
- **Hacktivists:**
  Attackers motivated by political, social, or ideological causes. Their actions may include website defacement, data leaks, or denial-of-service attacks to promote their beliefs.
- **Nation-State Actors:**
  Highly sophisticated groups backed by governments. They conduct cyber espionage, surveillance, and attacks on critical infrastructure such as power grids, banking systems, or defense networks.

3. Common Attack Surfaces

An attack surface includes all points where an attacker can attempt to access or compromise a system.

Common attack surfaces include:

- **Web applications:** Login pages, forms, dashboards, and admin panels
- **Mobile applications:** Insecure storage, permissions misuse, or weak APIs
- **APIs:** Poor authentication or exposed endpoints
- **Networks:** Public Wi-Fi, routers, firewalls, and open ports
- **Cloud infrastructure:** Misconfigured storage, exposed services, or weak access controls

Reducing the attack surface helps lower security risks.

---

4. OWASP Top 10 Vulnerabilities (Overview)

The **OWASP Top 10** is a widely recognized list of the most critical security risks to web applications.

Key vulnerabilities include:

- **Broken Access Control:** Users can perform actions or access data beyond their authorization level.
- **Injection Attacks:** Malicious inputs such as SQL injection manipulate backend databases.
- **Authentication Failures:** Weak passwords, poor session management, or missing multi-factor authentication.
- **Security Misconfiguration:** Default credentials, unnecessary services, or exposed error messages.
- **Sensitive Data Exposure:** Failure to encrypt sensitive data in storage or transit.

These vulnerabilities are dangerous because attackers can exploit them to gain control of systems, steal data, or disrupt services.

5. Mapping Daily-Used Applications to Attack Surfaces

Application	Possible Attack Surfaces
Email	Phishing emails, malicious attachments, fake login pages
WhatsApp	Account takeover, social engineering, SIM swapping
Banking Apps	Insecure APIs, weak authentication, malware on devices
Social Media	Credential stuffing, fake profiles, malicious links

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

A typical application data flow follows these steps:

1. **User:** Enters data such as login credentials, messages, or payment information.
2. **Application:** The web or mobile app processes the input and sends a request.
3. **Server:** Validates the request, applies business rules, and checks permissions.
4. **Database:** Stores, updates, or retrieves required data.
5. **Response:** Information is returned to the application and displayed to the user.

Understanding this flow helps identify where security controls should be applied.

---

7. Where Attacks Can Happen During the Data Flow

- **User level:** Phishing attacks, weak passwords, malware-infected devices
- **Application level:** Input validation issues, broken authentication, insecure session handling
- **Server level:** Unpatched software, misconfigurations, exposed services
- **Database level:** SQL injection, excessive privileges, data leaks
- **Data in transit:** Man-in-the-middle attacks if encryption is not used

Security measures must protect every stage of the data flow.

---

8. Summary (In My Own Words)

Cybersecurity is the practice of protecting systems and data by maintaining confidentiality, integrity, and availability.

Attackers have different motivations and skill levels, ranging from beginners to nation-state actors. Modern applications expose multiple attack surfaces, making them vulnerable if not properly secured. By understanding common vulnerabilities such as those listed in the OWASP Top 10 and analyzing how data flows through applications, organizations can identify weak points and apply effective security controls to reduce risks and protect users.