CYBER SECURITY BASICS & ATTACK SURFACE **NROUPSINH GOHIL**

Elevate Labs – Cyber Security Internship (Task 1)

---

1. What is Cyber Security?

Cyber Security is the practice of protecting computers, mobile phones, networks, applications, and data from unauthorized access, attacks, or damage.
It ensures that sensitive information remains safe from hackers and cyber criminals.

In today's digital world, cyber security is important because people use online banking, social media, email, and cloud services daily. Any weakness in security can lead to data theft, financial loss, or service disruption.

---

2. CIA Triad (Core Principles of Cyber Security)

Cyber Security is based on three fundamental principles known as the **CIA Triad**:

a) Confidentiality

Confidentiality ensures that information is accessible only to authorized users.

Real-world examples:

- Banking app passwords and ATM PINs should only be known to the account holder.
- Personal chats and photos on social media should not be visible to strangers.

---

b) Integrity

Integrity ensures that data remains accurate and is not modified without permission.

Real-world examples:

- A bank balance should not be changed by an attacker.
- Social media posts should not be edited by someone else without permission.

---

c) Availability

Availability ensures that systems and data are accessible when needed.

Real-world examples:

- Banking apps should work during online payments.
- Social media apps should be available to send messages anytime.

---

3. Types of Cyber Attackers

Different attackers have different skills and motives:

a) Script Kiddies

They have little technical knowledge and use ready-made tools available online to perform attacks for fun or curiosity.

b) Insiders

They are employees or ex-employees who misuse their authorized access to steal or leak sensitive data.

c) Hacktivists

They attack systems to promote political, social, or ideological causes.

d) Nation-State Attackers

They are highly skilled hackers backed by governments and target critical infrastructure, financial systems, or national data.

---

4. Attack Surface

An **attack surface** refers to all possible entry points where an attacker can try to exploit a system.

Common attack surfaces include:

- Web applications (login forms, search boxes)
- Mobile applications
- APIs
- Networks (Wi-Fi, internet connections)
- Servers and cloud infrastructure
- Databases

The larger the attack surface, the higher the risk of attack.

---

5. Mapping Daily-Used Applications to Attack Surfaces

Example: Banking Application

- Login page → Password and OTP attacks
- Mobile app → Application vulnerabilities
- Network → Data interception
- Server → Unauthorized access
- Database → Data leakage

Example: Social Media Application

- Mobile app → Insecure storage
- Network → Man-in-the-middle attacks
- Server → Account takeover
- Database → Personal data exposure

---

6. Data Flow in Applications

In most applications, data flows as follows:

User → Application → Server → Database

For example:

- In a banking app, the user enters payment details, which are sent to the server and stored or updated in the database.
- In social media, posts and messages travel from the user's app to servers and are stored in databases.

---

7. Where Attacks Can Happen

Cyber attacks can occur at any stage of the data flow:

- **User level:** Phishing attacks, weak passwords
- **Application level:** Bugs and insecure coding
- **Network level:** Public Wi-Fi interception
- **Server level:** Misconfiguration or weak authentication
- **Database level:** Unauthorized access or data leaks

---

8. Importance of OWASP Top 10

OWASP Top 10 is a list of the most critical security risks found in web applications.
It helps developers and security professionals understand common vulnerabilities and prevent real-world cyber attacks.
Many organizations and interview processes rely on OWASP Top 10 for security awareness.

---

9. Conclusion

This task helped build a strong foundation in cyber security concepts such as the CIA Triad, types of attackers, attack surfaces, data flow, and common attack points.
Understanding these basics is essential for identifying risks and protecting systems against cyber threats.