Understanding Cyber Security Basics & Attack Surfaces

This document provides a foundational understanding of cyber security concepts, common attacker types, attack surfaces, and real-world application risks.

1. What is Cyber Security?

Cyber security is the practice of protecting systems, networks, and data from digital attacks. Its main goal is to ensure the Confidentiality, Integrity, and Availability (CIA) of information.

CIA Triad Explained:

1 **Confidentiality:** Ensuring information is accessible only to authorized users. Example: Online banking passwords.

2 **Integrity:** Ensuring data is accurate and not altered unlawfully. Example: Transaction amounts not being modified.

3 **Availability:** Ensuring systems and data are accessible when needed. Example: Banking apps working 24/7.

2. Types of Attackers

1 **Script Kiddies:** Beginners using pre-made tools without deep knowledge.

2 **Insiders:** Employees or trusted users misusing access.

3 **Hacktivists:** Attackers motivated by political or social causes.

4 **Nation-State Actors:** Highly skilled groups sponsored by governments.

3. Common Attack Surfaces

1 Web Applications (login pages, forms)

2 Mobile Applications (Android/iOS apps)

3 APIs (data exchange points)

4 Networks (Wi-Fi, routers, firewalls)

5 Cloud Infrastructure (storage, virtual machines)

4. OWASP Top 10 Overview

OWASP Top 10 lists the most critical web application security risks. These include injection attacks, broken authentication, sensitive data exposure, security misconfiguration, and insufficient logging and monitoring. They are dangerous because they can lead to data theft, system takeover, and service disruption.

5. Mapping Daily Applications to Attack Surfaces

1 Email: Phishing, malware attachments

2 WhatsApp: Account takeover, malicious links

3 Banking Apps: Credential theft, man-in-the-middle attacks

6. Data Flow in Applications

Typical data flow: User → Application Interface → Server → Database. Data travels through networks and APIs before being stored or retrieved.

7. Where Attacks Can Occur

1. User side: Phishing, weak passwords
2. Application: Input validation flaws, authentication issues
3. Network: Packet sniffing, man-in-the-middle attacks
4. Server/Database: SQL injection, privilege escalation

8. Summary (In Simple Words)

Cyber security protects digital information from misuse and attacks. Understanding who attackers are, where systems are exposed, and how data flows helps identify risks early. A strong security foundation reduces chances of data loss, financial damage, and privacy violations.