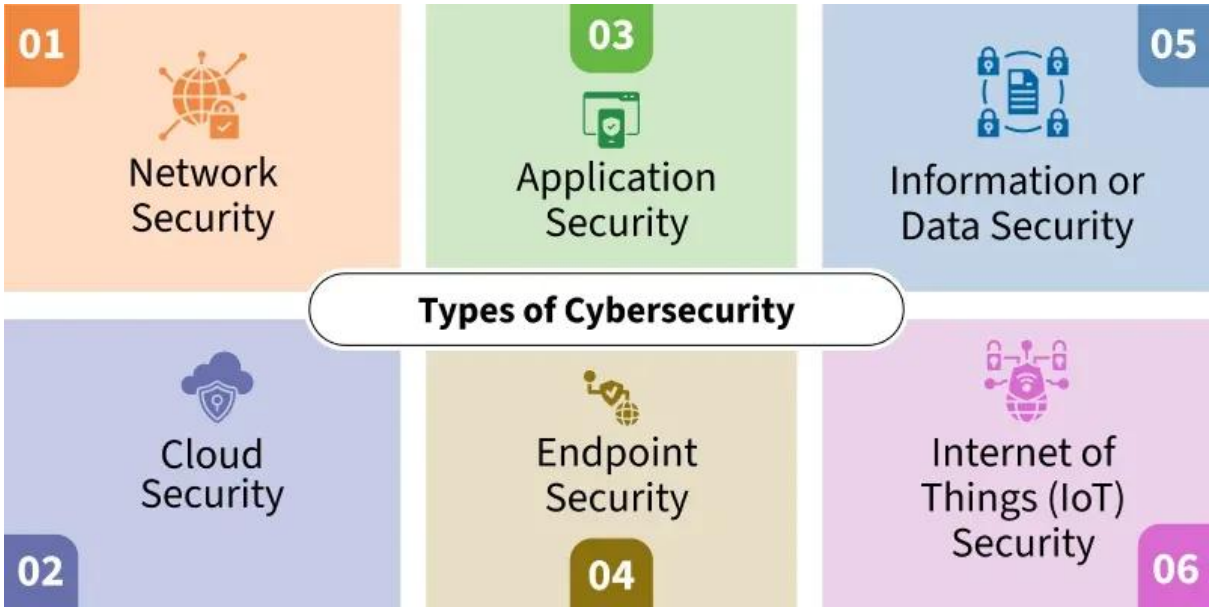
CYBER SECURITY INTERNSHIP

TASKE 1:- Understanding Cyber Security Basics & Attack Surface

- Cybersecurity is the practice of protecting digital devices, networks, and sensitive data from threats like hacking, malware, and phishing. Also known as Information Security (INFOSEC), Information Assurance (IA), or System Security.
- Protects systems, networks, and personal information
- Uses security tools, policies, and safe online practices
- Prevents data theft, system damage, and unauthorized access



➢ **Cybersecurity follows the CIA triad:**

Confidentiality ensures only authorized users access data through encryption and access controls; Integrity prevents unauthorized changes using checksums and digital signatures; Availability keeps systems operational via redundancies and defenses against denial-of-service attacks

The CIA triad is a foundational model in cyber security that ensures information security.

- **Confidentiality**: Ensures that sensitive information is accessed only by authorized individuals. For example, online banking systems use encryption and authentication to protect user data from unauthorized access.

- **Integrity:** Ensures that data is accurate and unaltered. For instance, when transferring money online, the amount must remain unchanged during transmission.

- **Availability:** Ensures that systems and data are accessible when needed. For example, social media platforms like Instagram must be available to users at all times without downtime

➢ Types of Attackers-

Script Kiddies: Inexperienced individuals who use existing tools to launch attacks without understanding how they work.

Insiders: Employees or contractors who misuse their access to harm the organization

Hacktivists: Individuals or groups who hack systems for political or social causes.

Nation-State Actors: Government-sponsored hackers targeting other nations for espionage or disruption

➢ Common Attack Surfaces

- **Web Applications:** Vulnerable to SQL injection, XSS, etc.
- **Mobile Apps:** Can be reverse-engineered or exploited via insecure APIs.
- **APIs:** Often exposed and can be abused if not properly secured.
- **Networks:** Susceptible to sniffing, spoofing, and DDoS attacks.
- **Cloud Infrastructure:** Misconfigurations can expose sensitive data.

➢ The most critical web application security risks:

1. Broken Access Control
2. Cryptographic Failures
3. Injection

4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-Side Request Forgery (SSRF

➢ Daily Applications to Attack Surfaces-

-Email: Phishing, malware attachments.
- WhatsApp: Social engineering, account hijacking.
- Banking Apps: Credential theft, man-in-the-middle attack.

➢ Data Flow and Attack Points:

- **Data typically flows from:**

User -> Application -> Server -> Database Attack points:-

-User: Phishing, malware.
-Application: Exploits like XSS CSRF.
-Server: Unauthorized access, DDoS.
-Database: SQL injection, data breaches.

➢ Conclusion:

Through this task, I gained a clear understanding of basic cyber security concepts such as the CIA Triad, attack surfaces, types of attackers, and OWASP Top 10 vulnerabilities.
Cyber security is essential in today's digital environment to protect user data, privacy, and online services.