cybersecurity 111 days

Day 1 - INTRO TO CYBERSECURITY

- Definition
- CIA
- Types of threats
- Levels of Protection

Cybersecurity

practice of protecting systems, networks, and data from digital attacks. It includes ensuring CIA is maintained of data.

Core Security Principles (CIA)

1. **Confidentiality** – Only the right people access data
2. **Integrity** – Data remains accurate and unaltered
3. **Availability** – Systems and data are accessible when needed

Types of Threats

- **Malware:** viruses, worms, trojans, ransomware
- **Phishing:** fake emails/websites that look like real ones to steal data
- **Social Engineering:** manipulating people, e.g., pretending to be IT support
- **DDoS Attacks:** overloading systems to make them unavailable
- **Zero-Day Attacks:** exploiting previously unknown vulnerabilities (flaw that hasn't been patched yet)

Levels of Protection:

1. **Personal:** safeguard YOUR identity, data, and computing devices; protect from identity theft

2. **Organizational:** protect the ORGANIZATION'S reputation, data and customers; protecting financial and data assets

3. **Government:** national security, economic stability, and the safety and wellbeing of citizens