INTRODUCTION TO CYBERSECURITY

Video Link: https://youtu.be/z5nc9MDbvkw

What is Cyber Security?

Cyber security is the process and design used to protect networks, devices, and data from unauthorized access, damage, or attacks. Its main goals are to protect businesses, increase productivity, and inspire customer confidence.

The Three Pillars (CIA Triad)

The foundation of cyber security rests on three main principles:

- **Confidentiality:** Ensuring only authorized people can access specific information.
- **Integrity:** Making sure data is trustworthy and has not been changed by unauthorized users.
- **Availability:** Ensuring that data and systems are available to authorized users whenever they need them.

Types of Hackers

The video categorizes hackers based on their intent:

- **White Hat:** "Ethical hackers" who use their skills for defense and have permission from organizations.
- **Black Hat:** Criminals who hack with malicious intent for personal gain or to cause damage.
- **Grey Hat:** Hackers who fall in between, sometimes acting defensively and other times offensively.
- **Others:** Includes **Suicide Hackers** (motivated by a cause, ignore legal consequences), **Script Kiddies** (unskilled, using pre-made tools), and **StateSponsored Hackers** (employed by governments for spying).

Common Cyber Attacks

- **Denial of Service (DoS):** Overwhelming a server so legitimate users cannot access it.
- **Malware:** Malicious software like viruses, worms, and Trojans.
- **Phishing:** Sending fake emails or messages to trick people into giving up sensitive info.

- **Man-in-the-Middle:** A hacker intercepts communication between two parties to steal data.
- **SQL Injection:** Sending malicious queries to a database to compromise its data.

How to Protect Systems

Key defense mechanisms include:

- **Authentication:** Using strong passwords and Two-Factor Authentication (2FA).
- **Regular Updates:** Installing "patches" to fix security holes in software.
- **Firewalls & Antivirus:** Software that blocks unwanted traffic and scans for threats.
- **Cryptography:** Encrypting data so it cannot be read even if stolen.

Becoming an Expert

A cyber security expert identifies weaknesses, monitors systems, and repairs flaws. Important certifications mentioned include:

- **CEH (Certified Ethical Hacker):** For technical testing and penetration.
- **CISSP:** A high-level management certification for designing security policies.
- **CISA/CISM:** Focused on auditing and managing security operations.
- **CCSP:** Focused on Cloud Security.