Introduction to Digital Security

- **What is Digital Security?**
  - It refers to protecting computers, networks, data, and information from threats like hackers, viruses, and unauthorized access.
  - Four main areas:
    1. **Computer Security**
    2. **Information Security**
    3. **Cybersecurity**
    4. **Network Security**

1. Computer Security

- **Definition:**
  - Protects computers, laptops, and servers from theft, damage, or unauthorized access.
- **Focus Areas:**
  - **Hardware Security:** Protects physical devices (e.g., locking your laptop).
  - **Software Security:** Keeps programs and operating systems safe from bugs and viruses.
  - **Data Security:** Protects files and information stored on the computer.
- **Examples:**
  - Using antivirus software.
  - Installing firewalls to block hackers.
  - Encrypting sensitive files.

---

2. Information Security

- **Definition:**
  - Protects information (both digital and physical) from unauthorized access, changes, or destruction.
- **Examples:**
  - Encrypting emails.
  - Using access controls like biometrics.
  - Regularly backing up data.

<u>CIA Triad:</u>

- **Confidentiality:** Only authorized people can access the data (e.g., using passwords).
- **Integrity:** Ensures data is accurate and not tampered with (e.g., using checksums).
- **Availability:** Ensures data is accessible when needed (e.g., backups).

Real-Life Examples of the CIA Triad

1. **Confidentiality:**
   - A hospital encrypts patient records so only doctors and nurses can access them.
2. **Integrity:**
   - A student's exam grades are protected to ensure they aren't changed by anyone.
3. **Availability:**
   - An online store ensures its website is always up so customers can shop anytime.

Summary of the CIA Triad

Principle	What it Means	How it's Achieved
Confidentiality	Only authorized users can access data.	Encryption, passwords, access controls.
Integrity	Data is accurate and untampered.	Checksums, digital signatures, version control.
Availability	Data and systems are accessible when needed.	Backups, redundancy, maintenance.

---

3. Cybersecurity

- **Definition:**
  - Protects systems, networks, and programs from digital attacks.
- **Focus Areas:**
  - Prevents cyberattacks like malware, phishing, and ransomware.
  - Protects sensitive data from being stolen.
  - Ensures businesses and individuals can operate safely online.
- **Examples:**
  - Using antivirus software.
  - Training employees to avoid phishing scams.
  - Monitoring networks for suspicious activity.

---

4. Network Security

- **Definition:**
  - Protects the infrastructure that allows data to flow between devices (e.g., the internet, Wi-Fi, or office networks).

- **Focus Areas:**
  - Secures devices like routers, switches, and firewalls.
  - Prevents unauthorized access to networks.
  - Monitors and controls network traffic.
- **Examples:**
  - Using firewalls to block harmful traffic.
  - Setting up VPNs to encrypt internet connections.
  - Segmenting networks to isolate sensitive data.

---

5. Common Threats

- **Types of Threats:**
  - **Malware:** Viruses, worms, and ransomware that harm devices.
  - **Phishing:** Fake emails or websites that steal personal information.
  - **Denial-of-Service (DoS) Attacks:** Overloading a system to make it crash.
  - **Data Breaches:** Unauthorized access to sensitive data.
- **How to Stay Safe:**
  - Use strong passwords and enable multi-factor authentication (MFA).
  - Keep software and systems updated.
  - Avoid clicking on suspicious links or downloading unknown files.

Useful links:

https://www.youtube.com/watch?v=kPPFNrlN3zo