Objective: Understand the core principles of cybersecurity, common threats, and their real-world applications.

This session is dedicated to building the theoretical foundation upon which all your practical skills will be built. A deep grasp of these initial concepts will make every subsequent topic easier to understand and apply.

1. Reading: Introduction to Cybersecurity

- **Action:** Begin by reading the introductory chapters of **"Cyber Security Basics - Protect your organization by applying the fundamentals.pdf"**.
- **Focus:** Pay close attention to the initial concepts. Don't worry about mastering everything at once; the goal is to familiarize yourself with the language and core ideas of the field. Take notes on terms or ideas that are new to you.

2. The CIA Triad: The Bedrock of Information Security

The CIA Triad is the most fundamental concept in cybersecurity, forming a security model for protecting information. Every security control, vulnerability, and attack can be analyzed in terms of its impact on these three pillars. It's important to understand that these three principles often exist in a state of tension; for example, implementing extremely strict confidentiality measures might make data less available to authorized users, so a balance must be struck based on the data's purpose and sensitivity.

- **Confidentiality:** This principle is about **secrecy and privacy**. It's focused on preventing the unauthorized disclosure of sensitive information. The core goal is to ensure that data is accessed only by individuals who are explicitly authorized to see it.
    - **Analogy:** Think of a sealed, registered letter or a private diary. Only the intended recipient has the authority to open and read the contents. Similarly, medical records should only be accessible to the patient and their authorized healthcare providers.
    - **Real-World Examples:** Your online banking password and personal identification information (PII) should be kept confidential. A breach of confidentiality occurs when a company's customer database is leaked online, exposing names, addresses, and credit card numbers. This can lead to identity theft and financial fraud.
    - **Key Tools & Methods: Encryption** is a primary tool. It scrambles data into an unreadable format that can only be deciphered with a specific key. Beyond encryption, confidentiality is enforced through **access controls** (like usernames, passwords, and multi-factor authentication), **data classification** (labeling data based on sensitivity), and physical security measures.
- **Integrity:** This principle is about maintaining the **trustworthiness, accuracy, and consistency of data** over its entire lifecycle. It ensures that data cannot be modified, altered, or deleted in an unauthorized or undetected manner.
    - **Analogy:** Imagine your academic transcript or your bank account balance. You must have absolute confidence that the information is correct and hasn't been tampered with. If someone could secretly change a 'B' to an 'A' on your transcript, its integrity

    would be lost.
    - **Real-World Examples:** A breach of integrity happens if a malicious actor intercepts a financial transaction and changes the destination account number or the amount. Another example is an attacker altering system logs to hide their malicious activity, thus compromising the integrity of the security records themselves.
    - **Key Tools & Methods: Hashing** is a fundamental technique. A hash function generates a unique, fixed-length digital fingerprint for a piece of data. If even a single character in the data changes, the hash will change completely, instantly revealing that the data has been tampered with. **Digital signatures** and **version control systems** are also used to ensure data integrity.
- **Availability:** This principle ensures that systems, networks, and data are **accessible and operational** for authorized users whenever they are needed. Information is useless if it cannot be accessed when required.
    - **Analogy:** A library is only useful if its doors are open during its stated hours and you can access the books. If the doors are inexplicably locked or the books are inaccessible, the library's service is not available.
    - **Real-World Examples:** A **Distributed Denial-of-Service (DDoS)** attack is a classic assault on availability. It floods a website's server with overwhelming traffic, causing it to crash and become unavailable to legitimate users. However, availability can also be compromised by non-malicious events like hardware failures, power outages, or natural disasters. Ransomware is another direct attack on availability, as it encrypts critical files and makes them inaccessible until a ransom is paid.
    - **Key Tools & Methods:** To ensure availability, organizations use **redundancy** (e.g., having multiple web servers), **hardware fault tolerance** (RAID arrays for disks), comprehensive **disaster recovery plans**, and reliable data backups.

3. Understanding Threats and Attack Vectors

Now, let's look at *how* the CIA Triad gets compromised. A **threat** is a potential for harm, while an **attack vector** is the path or means by which an attacker can gain access to a system to deliver a malicious outcome.

- **Phishing:**
    - **What it is:** A deceptive attempt to trick a person into revealing sensitive information or deploying malware. It is a primary vector for many major security breaches.
    - **How it works:** An attacker sends a fraudulent email, text message (smishing), or social media message that appears to be from a legitimate source (e.g., your bank, HR department, or a popular online service). The message often creates a sense of urgency, fear, or curiosity, prompting the victim to click a malicious link or open an infected attachment. This link leads to a fake website that is designed to steal credentials.
    - **It's a form of: Social Engineering**. There are several types, including **spear phishing** (highly targeted at a specific individual or organization) and **whaling** (spear phishing aimed at senior executives).

- **Malware (Malicious Software):**
  - **What it is:** A broad term for any software intentionally designed to cause disruption, damage, or gain unauthorized access to a computer system.
  - **Common Types:**
    - **Viruses:** Attach themselves to legitimate programs or files. They require a host to spread and are often triggered when a user runs the infected program.
    - **Worms:** Self-replicating malware that can spread across networks without any human interaction, exploiting security vulnerabilities to infect other systems.
    - **Trojans:** Disguise themselves as legitimate or useful software to trick users into installing them. Once installed, they create a backdoor for attackers to access the system, steal data, or install other malware.
    - **Ransomware:** A particularly nasty form of malware that encrypts a victim's files, making them inaccessible. The attacker then demands a ransom payment, usually in cryptocurrency, in exchange for the decryption key.
    - **Spyware:** Secretly gathers information about a person or organization without their knowledge and sends it to another entity.
- **Social Engineering:**
  - **What it is:** The art of psychological manipulation to trick people into divulging confidential information or performing actions they shouldn't. It exploits human psychology—trust, fear, helpfulness, and curiosity—rather than technical vulnerabilities.
  - **How it works:** Phishing is the most common example. Other techniques include **pretexting** (where an attacker invents a scenario to gain trust, like pretending to be from IT support needing your password to "fix" an issue), **baiting** (leaving a malware-infected USB drive in a public place for a curious victim to find and use), and **tailgating** (following an authorized employee into a secure area). It underscores that humans are often the weakest link in the security chain.