TRAINING DAY 1 REPORT :

- ## Understanding Information, Data, and Information Security

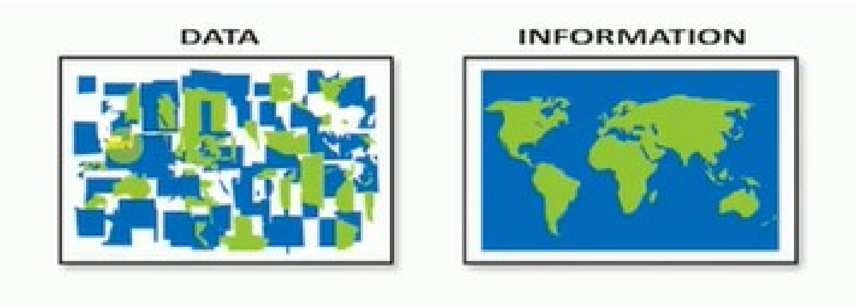
Today, I learned some important concepts:

Data :

Data is a collection of **raw facts and figures**. These can be numbers, characters, images, or any other outputs that, by themselves, may not carry meaning.
Example: *Marks of students, temperature readings, or names.*

Information :

Information is **processed or organized data** that is meaningful and useful. When data is analyzed and interpreted, it becomes information.
Example: *Average marks of a class* give information about the class performance.



Information Security :

Information security means **protecting information** from unauthorized access, use, disclosure, disruption, modification, or destruction.
The goal is to ensure *Confidentiality*, *Integrity*, and *Availability* of information.

- ## Information Security Threats :

Information Security Threats are **potential dangers or attacks** that can harm the *Confidentiality*, *Integrity*, or *Availability* of information. These threats try to access, damage, or steal sensitive data.

Types of Information Security Threats

1. *Inadvertent Threats* (human failure) – Mistakes made accidentally by people, like deleting important files or misconfiguring systems.
2. *Physical Disasters* (natural disasters) – Events like earthquakes, floods, or fires that damage systems and data physically.
3. *Technical Failures* (hardware or software) – Malfunctions in equipment or software bugs causing data loss or system downtime.
4. *Deliberate Acts* (hacking, espionage) – Intentional attacks by individuals or groups aiming to steal, damage, or misuse information.

- ## Introduction to Cyber Security

Cyber Security is the practice of **protecting computers, networks, programs, and data** from digital attacks, damage, or unauthorized access.

The main goal of cyber security is to ensure *Confidentiality*, *Integrity*, and *Availability* of information, also called the **CIA Triad**.

Why is Cyber Security important?

To protect **personal data** like passwords and bank details.

To keep **business information** safe from hackers.

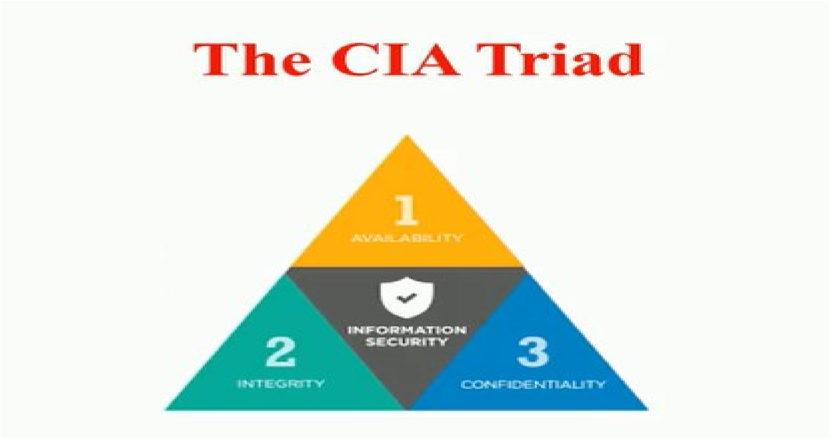
To prevent **financial loss** and **identity theft**.

To ensure **safe and reliable communication** over the internet.

- ## The CIA Triad

CIA Triad, which is the **foundation of information security**.

The **CIA Triad** stands for:



- *Confidentiality* – Ensuring that information is **accessible only to authorized people**. It protects data from unauthorized access or disclosure.
  Example: Encrypting sensitive files so only those with a password can read them.
- *Integrity* – Making sure information is **accurate and unaltered**. It prevents unauthorized changes to data.
  Example: Using checksums or digital signatures to detect tampering.
- *Availability* – Ensuring information and systems are **accessible when needed** by authorized users.
  Example: Backups and disaster recovery plans keep systems running even if something goes wrong.

The **CIA Triad** helps organizations build a **strong security strategy** by focusing on these three essential principles.

Ethical Hacking & Essential Skills

Today, I learned about **Ethical Hacking** and the skills required to become an ethical hacker.

What is Ethical Hacking?

Ethical Hacking is the practice of **legally testing and evaluating computer systems, networks, or software for security vulnerabilities**, so they can be fixed before criminals exploit them. Ethical hackers, also called **white hat hackers**, help organizations stay secure.

Skills Required for Ethical Hacking:

1. *Computer Networking Skills*
   Understanding how networks work, including protocols like TCP/IP, routers, switches, and firewalls.
2. *Computer Skills*
   Strong knowledge of computer systems, operating systems, file systems, and commands.

3. *Linux Skills*
   Since many hacking tools and servers run on Linux, it’s important to know commands, file permissions, and system administration.
4. *Programming Skills*
   Ability to read and write code in languages like Python, C/C++, Java, or scripting languages like Bash.
5. *Basic Hardware Knowledge*
   Understanding computer hardware components and how they interact with software.
6. *Database Skills*
   Knowing how databases like MySQL, Oracle, or MongoDB work, and how to test them for vulnerabilities like SQL injection.
7. *Problem Solving Skills*
   Thinking creatively and analytically to find weaknesses and solutions.

Developing these skills helps ethical hackers identify and fix security issues, making digital systems **more secure and reliable**.

- **Terms Used in Hacking**

Today, I learned about some important **terms used in hacking**:

1. *Vulnerability*
   A **weakness in a system** that can be exploited by attackers to gain unauthorized access.
2. *Exploit*
   A **piece of code or method** that takes advantage of a vulnerability to cause unintended behavior or gain control.
3. *Botnet*
   A **network of infected computers (bots)** controlled by a hacker, often used to launch large-scale attacks like DDoS.
4. *Spam*
   Unwanted or **unsolicited messages**, usually sent in bulk, often containing ads or malicious links.

5. *Malware*
   Short for **Malicious Software**, it includes viruses, worms, trojans, ransomware, spyware — all designed to harm systems or steal data.

6. *Rootkit*
   A type of malware that **hides its presence and gives attackers root or admin-level access** to a computer.

7. *Hack Value*
   A term hackers use to describe **how interesting or worthwhile a target is to hack**.

8. *Zero-Day*
   A **vulnerability unknown to the software vendor**, with no fix available. Attackers exploit it before it’s patched — called a **zero-day attack**.

9. *Phishing*
   A technique where attackers **send fake emails or messages** pretending to be trustworthy to steal sensitive information like passwords.

10. *Pharming*
    A type of attack that **redirects users from legitimate websites to fake ones**, even if they type the correct URL, to steal information.