FUNDAMENTAL CONCEPTS

CYBER SECURITY

Fundamental Concepts

- **Threats, Vulnerabilities, and Risks:**
  - **Threats:** Refers to potential events or actions that can exploit vulnerabilities in systems or networks, leading to harm or damage.

Fundamental Concepts

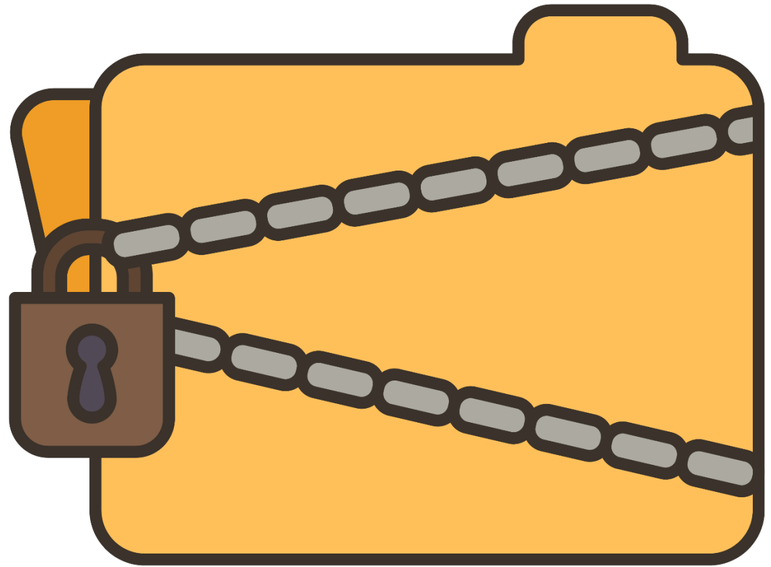
- **Threats, Vulnerabilities, and Risks:**
  - **Vulnerabilities:** Weaknesses or flaws in systems, networks, or processes that could be exploited by threats to compromise security.
  - To take advantage of vulnerabilities, attackers need a path to launch an exploit (a piece of software). **An attack vector** is the pathway Hackers use to breach a network (Unpatched software).

Fundamental Concepts

- **Threats, Vulnerabilities, and Risks:**
  - **Risks:** The likelihood of a threat exploiting a vulnerability, leading to a negative impact on an organization's assets or operations.
  - **Risk Management**: Identifying, assessing and mitigating potential security risks

Fundamental Concepts

- **Confidentiality, Integrity, and Availability (CIA):**
  - **Confidentiality**: Ensuring that sensitive information is accessible only to authorized individuals or entities.



Fundamental Concepts

- **Confidentiality, Integrity, and Availability (CIA):**
  - **Integrity**: Maintaining the accuracy, consistency, and trustworthiness of data and systems, ensuring that they are protected against unauthorized modification or tampering.

Fundamental Concepts

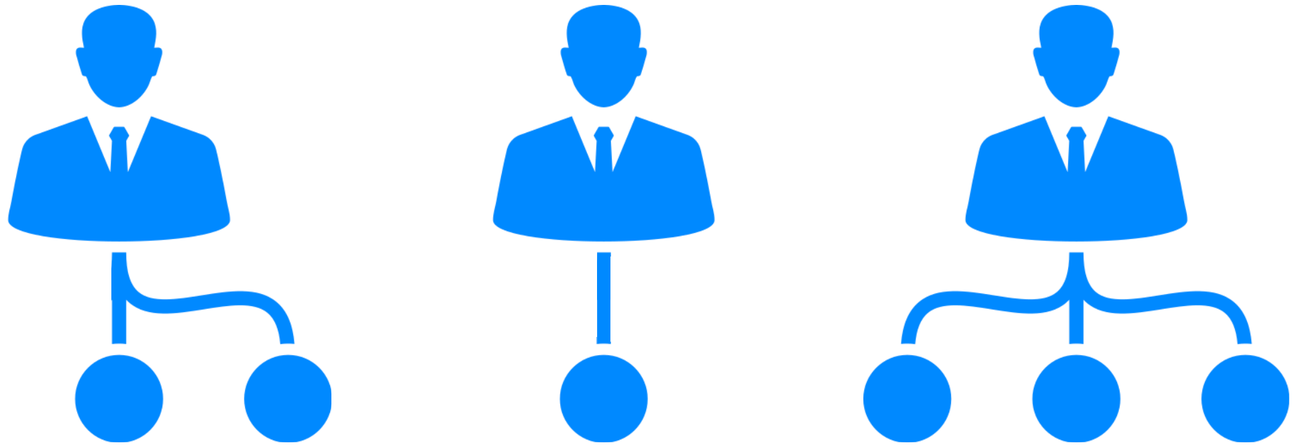
- **Confidentiality, Integrity, and Availability (CIA):**
  - **Availability**: Ensuring that systems, networks, and data are accessible and usable when needed by authorized users, preventing disruptions or downtime.

Fundamental Concepts

- **Defense in Depth:**
  - A layered approach to security that involves implementing multiple security controls and countermeasures at different layers of the IT infrastructure.
  - If one layer of defense is breached, other layers remain intact to mitigate the impact of the attack.

Fundamental Concepts

- **Least Privilege:**
  - The principle of granting users the minimum level of access or permissions necessary to perform their job functions.
  - Restricting access to sensitive data and resources helps minimize the risk of unauthorized access and data breaches.



Fundamental Concepts

- **Authentication and Authorization:**
  - **Authentication**: Verifying the identity of users or entities attempting to access a system or network**.**
  - **Authorization**: Determining the permissions or privileges granted to authenticated users or entities, specifying what actions they are allowed to perform.

Fundamental Concepts

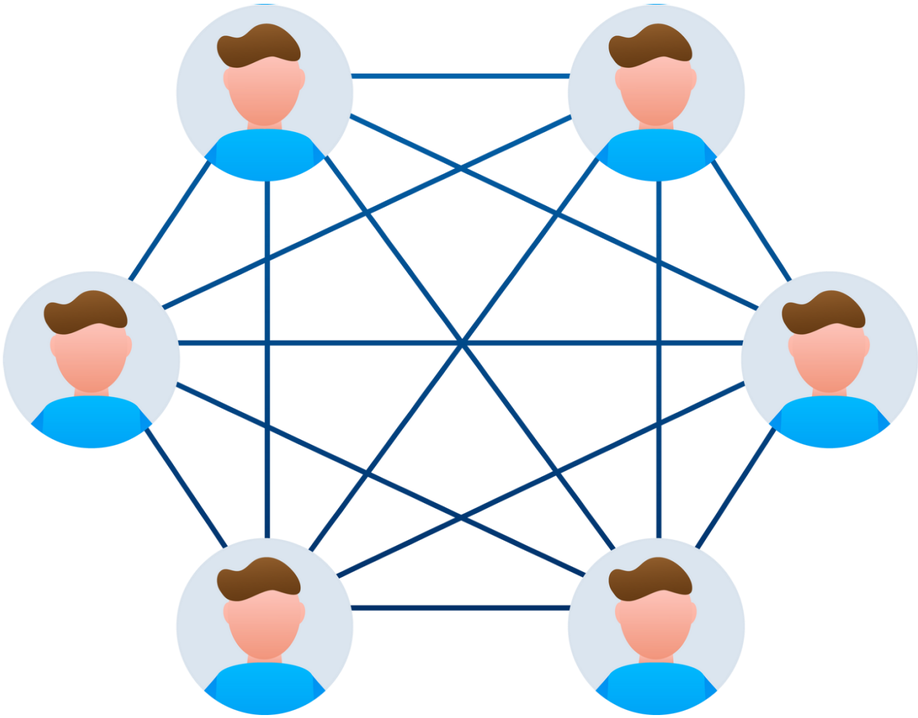
- **Non-Repudiation:**
  - Non-repudiation refers to the ability to prove that a specific action or transaction was performed by a particular entity and cannot be denied later.
  - In other words, it ensures that a sender or signer of a message cannot later deny having sent or signed it, thus providing assurance and accountability in electronic communications and transactions

Fundamental Concepts

- **Hashing:**
  - Creating a digital fingerprints to verify data integrity. Hashing is a process of converting input data (or a message) into a fixed-size string of characters, typically a hexadecimal string, using a mathematical function called a hash function. The output of a hash function is known as a hash value
  - A process of applying a mathematical algorithm against a set of data to produce a numeric value (a 'hash value') that represents the data.

Fundamental Concepts

- **Separation of Duties:**
  - Dividing Responsibilities to prevent single point of failure

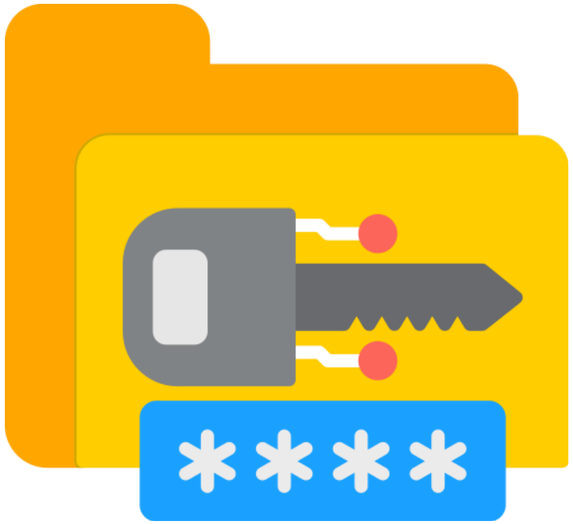


Fundamental Concepts

- **Need to Know:**
  - Limiting access to sensitive information to only those who need it.

Fundamental Concepts

- **Encryption:**
  - Encryption is the process of converting plaintext (ordinary, readable data) into ciphertext (unreadable, encoded data) using an algorithm and a key.
  - The purpose of encryption is to protect sensitive information from unauthorized access or interception by ensuring that only authorized parties can decrypt and access the original data.

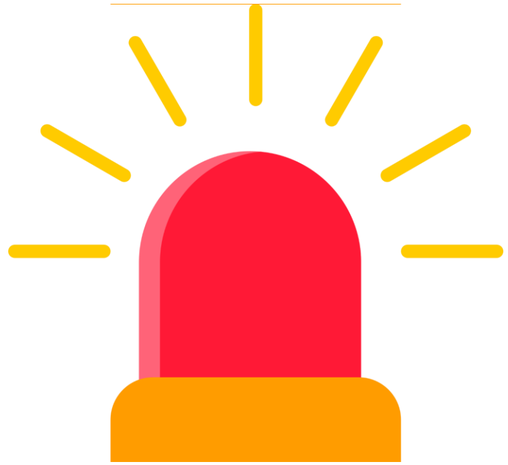


Fundamental Concepts

- **Patch Management:**
  - The process of regularly updating software, operating systems, and firmware with the latest security patches and updates.
  - Patch management helps address known vulnerabilities and reduce the risk of exploitation by cyber threats.

Fundamental Concepts

- **Incident Response:**
  - Establishing procedures and protocols for detecting, responding to, and recovering from cyber security incidents.
  - Incident response plans outline roles, responsibilities, communication channels, and escalation procedures to facilitate a coordinated and effective response to security incidents.



Fundamental Concepts

- **Security Awareness and Training:**
  - Educating about cyber security best practices, policies, and procedures.
  - Security awareness training helps raise awareness of potential threats and empowers individuals to recognize and respond to security risks effectively

Fundamental Concepts

- **Cyber Attack:**
  - An attack is a specific, intentional, and malicious action or event that aims to compromise the confidentiality, integrity, or availability of computer systems, networks, data, or assets.

Fundamental Concepts

- **Cyber Security:**
  - Cyber Security, refers to the practice of protecting computer systems, networks, devices, and data from unauthorized access, attacks, damage, disruption, or theft, and **ensuring the confidentiality, integrity, and availability of digital information** and services.

Fundamental Concepts

- **Cyber Security:**
  - It encompasses a range of technologies, processes, practices, and measures designed to safeguard against a variety of cyber threats.

Fundamental Concepts

- **Cyber Security:**
  - Cyber security aims to **mitigate risks and vulnerabilities** in digital environments by implementing security controls, policies, and procedures to detect, prevent, respond to, and recover from security incidents, thereby maintaining the trust, privacy, and integrity of information and infrastructure in an increasingly interconnected and digital world.