Vedansi Parsana

* **Consider these seven information security concepts confidentiality, integrity, availability, non-repudiation, authentication, authorization, and encryption. For each term, provide a definition and one good and one bad example of these concepts in action. You may use real example from your own or other’s lives or make up fake examples.**

1. Confidentiality

* **Definition:** the state of keeping or being kept secret or private. Confidentiality refers to protecting information from being accessed by unauthorized parties.
* **Good example:** John kept accountant/client confidentiality with Roger by not giving any information about Roger to an unknown guy.
* **Bad example:** Mia talks loudly in public about her bank details.

1. Integrity

* **Definition:** Assuring that information and programs are changed only in a specified and authorized manner
* **Good example:** When John mailed Roger, he got the exact same data what John mailed him.
* **Bad example:** When John mailed Roger, he got the mail, but the mail was slight changed then the original one when he received the mail.

1. Availability

* **Definition:** assuring that authorized users have continued access to information and resources
* **Good example:** My advisor made sure that he told me about every-thing I can have access to before I joined the campus.
* **Bad example:** John gave and showed every information about the access information to the office except one which could cause problems for Rony.

1. Non-Repudiation

* **Definition:** Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data.
* **Good example:** Maya did notary before submitting her papers.
* **Bad example:** Maya forgot to sign on paper after she got her mail delivery.

1. Authentication

* **Definition:** Verifying the identity of a user, process or device often as a prerequisite to allowing access to resources in an information system
* **Good example:** All the college student’s login to icollege with their login id and password.
* **Bad example:** Gary works in a company where everyone has to use only one account for their work, which may have case sensitive data.

1. Authorization

* **Definition:** Authorization is a security mechanism to determine access levels or user/client privileges related to system resources including files, services, computer programs, data and application features.
* **Good example:** Any person can create an account in the bank, but the bank has to provide the commitment that the information would not to delivered to anyone else except the authorized user.
* **Bad example:** Accountant shared the personal information of a person without the permission of the person who is the authorized user.

1. Encryption

* **Definition:** Data encryption is a security method where information is encoded and can only be accessed or decrypted by a user with the correct encryption key.
* **Good example:** During video calls before sharing personal information with each other Mia and Gia made sure that the call was end to end encrypted.
* **Bad example:** During a video call, two people shares revealing pictures before noticing that the call was not end to end encrypted.