The CIA Triad

Shaun Dennis | 9.13.23

Old Dominion Student

Cybersecurity

What is the CIA Triad?

The CIA Triad is a 3-step protocol that businesses and companies use within their systems to keep information secure. It is used to ensure that the information they are receiving and giving out is always safe, secure and trustworthy. The CIA Triad has 3 key components to it, being **C**onfidentiality, **I**ntegrity, and **A**vailability. These 3 principles work together for cybersecurity experts, preventing confidential information from being stolen, and/or holding secret information, for example, during a ransom during an attack.

Confidentiality

The first term in the CIA Triad is confidentiality. Confidentiality is a big aspect of this protocol because it ensures that the information you provide through any online vendor like online ordering, appointments, medical information, etc is kept safe, protected, and private.

Integrity

The second term in the CIA Triad is Integrity. Integrity is the principle that any data shared is trustworthy, complete, and hasn't been messed up or tampered with. Integrity is involved with hashing, encrypting, online certificates and online signatures in the cybersecurity world.

Availability

The last term in the CIA Triad is Availability. Availability ensures that networks and systems are properly functioning, and they are working when they need to be. An example for availability can be DDoS for if an attacker crashes a server or makes the system or network not function properly.

Authentication vs. Authorization

Referring to the cyber world, the term authentication is verifying a user or action to approve it or deny it. An example of authentication is when ODU students and staff sign in they have to complete a multi-factor authentication to be granted access to the system. Authorization is the amount of access they are limited to and granted. An example of Authorization is when ODU students and staff sign in, students have limited access compared to the faculty.