GOLIBE OKEKE NICOLE

24th July, 2023

1. What is the CIA in cyber security? Explain each component in your own words.

The full meaning of CIA is Confidential Integrity and Availability.

6. **Confidential** involves the efforts of an organization to make sure data is kept secret or private.

**Integrity** involves making sure your data is trustworthy and free from tampering during transmission.

**Availability** helps in delivering information when requested by the user. You can access it anytime.

1. Why is confidentiality important in cyber security? Can you think of a situation where confidentiality can be compromised?

Its helps in keeping information private.

It can be compromised by an attacker making an attempt to invade an application or database so they can take data from it.

1. List and explain methods used to ensure confidentiality in cyber security.

* Data encryption
* Username ID and password
* Version control

1. What does integrity mean in the context of cyber security? Why is it important?

Integrity involves making sure your data is trustworthy and free from tampering during transmission.

It is important because it makes sure data or information is maintained so that it is not modified or deleted by an unauthorized user.

1. Describe the methods used to ensure integrity in cyber security

* Backing up data
* Using access controls
* Removing duplicate data

1. What does availability mean in cyber security? Why is it crucial for data and network system?

Availability helps in delivering information when requested by the user. You can access it anytime. It is important because it safeguards all types of data against theft and losses.

1. List and explain the methods used to ensure availability in cyber security.

* Redundant networks, servers and applications.
* Enhance availability
* Backups and full disaster recovery plans

1. Imagine you are a White-Hat Hacker. What would be your responsibilities, and how would you ensure the new CIA triad in a system you are protecting?

I’ll improve the cyber security and try to find any vulnerabilities before the bad guys do.

1. What is the difference between a Black-Hat hacker and a Grey-Hat hacker?

the black-hat hackers are motivated by malicious intent while grey-hat hackers operate in the nebulous area in between- they’re not always ethical either.

1. What is a Cyber Terrorist? Can you think of any ways to protect a system from a potential cyber terrorist attack?

Cyber terrorism is referring to unlawful attacks by recognized terrorist to the computers, networks and information stored.

You can protect a system from cyberterrorism:

* Antivirus software
* Choose strong passwords
* Keep up-to-date.