CYBER – SECURITY

SESSION ONE

What is Cyber - Security

- Cyber Security is a set of processes, technologies, and methods to protect servers, computers, networks, electronic systems, data, and mobile devices from unauthorized access through malicious attacks.
- Securing the **availability**, **confidentiality**, and **integrity** of an organization's digital assets and software against internal or external threats is the primary objective of cyber security.
- Cyber security sometimes has been referred to as **information technology security** or **information security (infosec for short)**.

What is Cyber - Security

Let us see some differences between **cybersecurity and information security.**

- Information security (commonly known as InfoSec) refers to the procedures and practices used by corporations to protect their data.
- This contains policy settings that prevent unauthorized people from accessing company or personal data.
- Information security is a broader category that protects all information assets, whether in hard copy or digital form.
- Information security is a fast-evolving and dynamic discipline that includes everything, from network and security design to testing and auditing.

Types/Categories of security

Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect.

Information security protects the integrity and privacy of data, both in storage and in transit.

Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

Types/Categories of security

Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

Threats and Types of Cyber Threats

Cyber threats also refer to the possibility of a successful cyber attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property or any other form of sensitive data.

A threat can be anywhere between a **minor bug** in a code to a complex cloud hijacking liability.

Threats and Types of Cyber Threats

Malware simply put, malicious software,malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer.

Virus A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

Trojans A type of malware that is disguised as legitimate software.

Threats and types of cyber threats

Spyware A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

Ransomware Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.

Adware Advertising software which can be used to spread malware.

Botnets Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

Tasks

Question 1:
What do you understand by cybersecurity?

Question 2
Explain cyber security in your own terms.

Question 3
Differentiate between cyber sec. and info sec.

Question 4
Differentiate between a malware and a virus.

Tasks ctd..

Question 5

Using a Facebook app, explain how Trojan can affect a cyber space

Question 6

Which of the cyber threats has the primary function of blackmailing users?

Question 7

The malicious pop ups we get during our internet sessions are known as?