# Cyber Security Assignment-1

Q1 What is security? Why required cyber security.

⇒ Security for information technology refers to the methods, tools and personnel used to defend an organization digital assets. The goal of IT security is to protect these assets, devices and services from being disrupted, stolen or exploited by unauthorized user.

⇒ Cyber Security is important because it protects all categories of data from theft and damage. This include sensitive data, personally identifiable information, protected health information, personal information, intellectual property, data and gavermental & industry information systems.

⇒ Without a CyberSecurity program, your organization cannot defend itself against data breach campaigns, which makes it an irresistible target for cybercriminals.

Q2 What is cyber security ?

⇒ Cyber Security is the state or process of protecting and recovering computer systems, network, devices and programs from any type of cyber attack. Cyber attacks are an increasingly sophisticated and evolving danger to your sensitive data, as attackers employ new methods powered by social engineering and artificial intelligence (AI) to circumvent traditional data security controls.

Q3 What is information security ?

⇒ Information security is not only about securing information from unauthorized access. Information security is basically the practice of preventing unauthorized access, disclosure, disruption, modification inspection, recording or destruction of information.

⇒ Information can be physical or electronic one. Information can be anything like your details or we can say your profile

on social media, your data in Mobile phone, your biometric and etc. Thus information security spans so many research are like cryptography, Mobile Computing, Cyber forensics, Online social Media etc.

Q4. Difference between information security & cyber security?

| ⇒ Information Security | Cyber Security |
|---|---|
| 1. Focuses on protecting data from any type of illegal access. | 1. Focus on protecting data from unauthorize digital access. |
| 2. Applied to physical and digital information | 2. Applied to digital information. |
| 3. It's the foundation of data security which means its first step | 3. It deals with advanced persistent threat that are irrelevant. |

05) Explain any five : Cyber security objectives and policils

⇒ objectives :-

⇒ The objective of cyber security is to protect information from being stolen

⇒ Security can be measured by at least one of their goals.

⇒ Protect the confidentiality of data.

⇒ Preserve the integrity of data.

⇒ Promote the availability of data for authorised user.

* Policies :-

1) Security policy :-

Security policy its statement of responsible decision makers about the protecting mechanism of a company crucial physical & information assets.

2. Policy makers :- Security policy development as a part of collective operation of all entity of an organization that is affected by its rules.

3. Policy audience :- Security policy applies to all Senior management employees, stockholders, consultants and services providers who use company assets

4. Policy classification :- Every organization has all three policies

First that is drafted on paper, second that is in employee minar, and finally that is actually interented.

5. Policy enforcement :- Enforcement of security policies ensures compliance with the principle and protects by the company because policy procedure do not work if there are violated.

Q6. Explain any 5 :- principle of cyber security.

=> 1. Open design :- These principles states that the security of a mechanism should not depend on the secrecy of its design or implementation. It suggests that complexity does not add security. This principle is the opposite of the approach known as "security through obscurity.

2. Complete mediation :- The principle of complete mediation restricts the caching of information which often leads to simpler implementation of mechanisms.

3. Compromise recording :- The compromise Recording principles states that sometimes it is more desirable to record the details of intrusion that do adopt a more sophisticated measure to prevent it.

4. Work factor :- The principles states that the cost of circumventing ("known as work factor") can be easily calculated.

5. Separation of privilege :- This principle states that a system should grant access permission based on more than one condition being satisfied. This principle may also be restrictive because it limits access to system entities

Q7. What is cyber crime ? Types of Cyber crime.

→ Cyber crime is not an old sort of crime to the world. It is defined as any criminal activity which take place on or over the medium of computer or internet or other technology recognised by the ~~IT~~ IT act.

Types of crime :-

1. Ddos attack
2. Botnets
3. Identity theft
4. Cyberstalking
5. PUPs
6. Phishing