**Assignment - 1**

**Ans 1.**

Distributed information systems represent an increasingly important trend to computer users. Distributed processing is a technique for implementing a single logical set of processing functions across a number of physical devices, so that each performs some part of the total processing required.

As mentioned above, there are many current issues concerning Information Systems security. Some of these issues include spamming, hacking, jamming, malicious software, sniffing, spoofing, and identity theft; each one of these problems fit under one of two heading, computer abuse or computer crime

**Ans 2.**

The fundamental principles (tenets) of information security are confidentiality, integrity, and availability. Every element of an information security program (and every security control put in place by an entity) should be designed to achieve one or more of these principles. Together, they are called the CIA Triad.

**Ans 3.**

**Threat –** Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

**Vulnerability –** Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.

**Risk –** The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

**Ans 4. Didn’t understood the question..**

**Ans 5.** Having a strong encryption mechanism on wireless access points prevents unwanted users from joining your network just by being nearby. A weak encryption mechanism can allow an attacker to brute-force his way into a network and begin man-in-the-middle attacking.

**Ans 6.**

Mobile Security Threats (and What You Can do to Fight Back)

1. Public WiFi.
2. Lack of end-to-end encryption.
3. Inactive apps.
4. IoT mobile security threats.
5. Botnets.
6. No password protection.
7. Phishing attacks.

To secure mobile threats, follow these rules :

1. Use strong passwords/biometrics. Strong passwords coupled with biometric features, such as fingerprint authenticators, make unauthorized access nearly impossible.
2. Ensure public or free Wi-Fi is protected.
3. Utilize VPN.
4. Encrypt your device.
5. Install an Antivirus application.
6. Update to the latest software.

**Ans 7.**

E-Commerce site security is critical for a number of reasons, specifically when it comes to protecting the privacy and sensitive data of customers on a website, safeguarding the finances of an online business, preventing fraud and financial scams and defending the reputation of an online store as a safe place to conduct.

The stability of an e-commerce website can be disrupted by the following:

1. Power failure.
2. Fire, floods, and other natural disasters.
3. Computer viruses and hacker attacks.
4. Software glitches.
5. User error and system mismanagement.

**Ans 8.**

A simplified way to view this is looking at invaders versus saboteurs. External threats, or invaders, act from outside the company and must overcome your exterior defenses in order to reach your database. Internal threats, or saboteurs, work within the company and can thus bypass exterior defenses.