Chapter- 3
Computer Security
Questions with its Solutions

Question Pattern:
Full Forms: 1 Mark Type
Technical Term: 1 Mark Type
Very Short : 1 Mark Type
Short Q/A : 2 Marks Type

❖Write the full form of the following. *[1 Mark Type]*

a. **AC:** Air Conditioning
b. **ACL:** Access Control List
c. **AMC:** Annual Maintenance Contract
d. **AMD:** Advanced Micro Devices
e. **CCTV:** Closed – Circuit Television
f. **CIA:** Confidentiality Integrity Availability
g. **DDoS:** Distributed Denial of Service
h. **DRP:** Disaster Recovery Planning
i. **INFOSEC:** Information Security
j. **MAC OS:** Macintosh operating system
k. **NAT:** Network Address Translation
l. **NAV:** Norton Antivirus
m.**PIN:** Personal Identification Number
n. **PKC:** Public key cryptography
o. **SKC:** Symmetric Key Cryptography
p. **UPS :** Uninterruptible Power Supply
q. **VIRUS:** Vital Information Resources Under Siege

❖**Write appropriate technical term of the following.** *[1 Mark Type]*

a. The fake attempt to obtain sensitive information.

⇨ **Phishing**

b. The hardware or software for recording the keys pressed on a keyboard.

⇨ **Keylogger**

c. Law that governs the legal issues of cyberspace.

⇨ **Cyber Law**

d. The skilled computer expert who uses technical knowledge to overcome a problem.

⇨ **Computer hacker**

e. The kind of harmful computer code or web script designed to create system vulnerabilities.

⇨ **Malicious code**

f. The process of identifying an individual usually based on a username and password.

⇨ **Authentication System**

g. A memorized secret code used to confirm the identity of a user.

⇨ **Password**

h. A process of performing variety of tech-enabled activities via virtual communities and network.

⇨ **Social Media**

i. The uniquely identified by evaluating one or more distinguishing biological traits.

⇨ **Biometric verification**

j. The network security systems that monitors and controls the traffic flow.

⇨ **Firewall**

k. The technology to encode file or message.

⇨ **Encryption**

l. A small destructive program whose intention is harms computer software and data.

⇨ **Computer Virus**

m. Secret word needed to unlock a computer.

⇨ **Password**

n. Making duplicate copy of the file for security purpose.

⇨ **Backup**

o. A software installed on your PC that collects your information without your knowledge.

⇨ **Spyware**

p. A type of malicious software that bombards you with incessant pop-ups.

⇨ **Adware**

q. A program downloaded and installed on a computer that appears harmless, but is , in fact malicious.

⇨ **Trojans**

r. A malware computer program that replicates itself in order to spread to other computers.

⇨ **Worms**

s. A program that can disinfect a file from virus.

⇨ **Antivirus**

t. A system of copying data and information residing in computer into another location,

⇨ **Backup System**

u. Secret group of characters which helps to protect file from unauthorized person.

⇨ **Password**

❖**Answer the following questions in one sentence.** ***[1 Mark Type]***

1. What is social media?

Ans: social media is a process of performing a variety of tech-enabled activities via virtual communities and network. Example: facebook, twitter, Instagram etc.

2. Define computer virus.

Ans: Virus is a program or piece of code designed to damage our computer by corrupting system files, wasting resources and destroying data.

3. What are Trojans?

Ans: A program downloaded and installed on a computer that appears harmless, but is, in fact malicious.

4. Define malware / malicious code.

Ans: Malware is short form of malicious software, and is a general term used to describe all of the viruses, spyware, worms, adware, trojan.

5. What are computer worms?

Ans: A computer worm is a type of malicious software program which is self-replicating malware that duplicates itself to spread to uninfected computers.

6. What is keylogger?

Ans: Keylogger is a malicious type of monitoring software or hardware that records the keys pressed on a keyboard secretly so that person using the keyboard does not know that their actions are being monitored.

7. What is spyware?

Ans: Spyware is a software installed on the PC that collects your information without your knowledge which sends that information back to the creator so they can use personal information in some immoral way.

8. What is firewall?

Ans: A firewall is the network security systems that monitors and controls the traffic flow between the internet and private network or private computer on the basis of a set of user-defined rules.

9. Define rootkit.

Ans: A rootkit is a collection of multiple malware programs that can implant itself on various authorization levels of a computer.

10.Define phishing.

Ans: Phishing is a fake attempt to obtain sensitive information such as usernames, passwords, credit cards detail etc.

11.What is antivirus?

Ans: Antivirus software is a type of program designed to detect and remove viruses from computer system.

12.What is social engineering?

Ans: Social engineering is a hacker term for tricking people into revealing their passwords or some forms of security information.

❖Answer the following questions *[Most Imp Question] [2 Mark Type]*

1. What is computer security? Write its importance.

Ans: Computer security is the branch of information technology which deals with the protection of data on a network. It denotes both hardware and software security of a computer.

Some of the importance of computer security are listed below in points: a. To protect confidential and potential data in computer.

b. Protection Against Malware and Viruses.

2. What is information security? Write its importance.

Ans: Information security is the protection of information and information system from unauthorized access, use, disclosure, disruption, modification or destruction.

Some importance of the information security are:

a. It enables the safe operations of applications implemented on the organizations.

b. It protects the data that organization collects and uses.

3. Define the principles of information security.

Ans: The basic components / principles of information security are:

a. Confidentiality
b. Integrity
c. Availability

a. <u>Confidentiality:</u> It refers to the data that is only available to authorized parties.

b. <u>Integrity:</u> It is a process that ensures the accuracy, completeness, consistency, and validity of an data.

c. **<u>Availability:</u>** It guarantees that systems, applications and data are available to users when they need them.

4. What is cryptography? Mention its role for information security and communication.

Ans: Cryptography is technique of securing information and communications through use of codes or algorithms so that only those persons for whom the information is intended can understand it and process it.

The role of cryptography in the field of information security are listed below: a. It ensures information is not altered while in storage or during transit between the sender and the recipient.
b. It supports the availability of data by guaranteeing that individuals with the right permission can use systems and retrieve data.

5. Define encryption and decryption.

Ans: Encryption is the process to encode file or message(plain text) that is being stored or transferred online so that it can only be read by the person who has the secrete code, or decryption key. Generally, encryption is done with the help of key and the key is made available to the authorized user only.

Decryption is the process to decode file or encrypted message(cipher text) back to its original form. It is generally a reverse process of encryption. Authorized user can only decrypt the data because decryption requires a secret key or password.

6. What is software security? Write any two protection measures of software security.

Ans: Software security is an idea implemented to protect software against malicious attack and other hacker risks so that the software continues to function correctly. Software security is necessary to provide integrity, authentication and availability of the data.

Any two measures of software security are:

a. Enable firewall security to monitor incoming and outgoing traffic.

b. Update programs and systems regularly from authenticated source.

7. What is hardware security? Write any two protection measures of hardware security?

Ans: It is a process of protecting hardware against vulnerabilities that are targeting these devices. It deals with the fundamental measures that we should implement to protect our computer system from any kinds of damages.

Any two protection measures of hardware security are mentioned below.

a. Regular Maintenance:

- Regular and systematic inspection, cleaning, and replacement of worn parts are required to keep the computer system is in a good state.

b. Dust Prevention:

- Dust and debris (*scattered pieces of rubbish*) can create heat, which can affect computer's motherboard. Therefore, the computer room must be free from the dust with regular cleaning practice.

8. What is antivirus software? Name any two popular antivirus softwares.

Ans: Antivirus software is a program or set of programs that are designed to prevent, search or detect, and remove software viruses and other malicious software like worms, trojans, adware etc.

Any two popular antivirus software are:

a. AVG

b. Avast

9. What is password? Write any two importance of password protection.

Ans: A password is a basic security mechanism that consists of a secret passphrase created using alphabetic, numeric, alphanumeric, and symbolic characters or a combination. A password is used to restrict access to a system, application, or service.

Any two importance of password protection are listed below:

a. It helps to protect our personal and sensitive information from unauthorized access.

b. Passwords serve as a primary means of user authentication, verifying the identity of individuals seeking access to specific systems or services.

10.What is firewall in computer? Mention any four types of firewalls used in computer system.

Ans: A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based of defined set of security rules.

Various types of firewalls used in computer are listed below:

a. Packet filtering firewalls

b. Next generation firewall (NGFW)

c. Proxy service application firewall

d. Network address translation (NAT)

11. Explain the role of power protection device in computer system.

Ans: A power protection device, often referred to as a **surge protector** or **uninterruptible power supply** (UPS), is a piece of equipment designed to safeguard electronic devices and systems from power-related issues.

The role of power protection device in computer system are listed below: a. Surge and Spike Protection.

b. UPS device provide a crucial function by offering a temporary power source during electrical outages.

c. Sudden power losses can lead to data corruption or loss so using power protection device like UPS allows the computer to run continuously for a short duration after a power outage which helps in preventing data loss.

12.What is a backup? Why is backup vital to computer security system?

Ans: Backup is the system of copying data and programs into another location or creating a duplicate copy of it's in a secured place.

Backup mechanism is vital to computer security system due to the following reasons:

a. Backup mechanism helps to retrieve the data and prevent data loss. b. Natural disasters, fires, floods, or other unforeseen events can physically damage computer systems in such cases, having offsite backups ensures that data can be recovered and systems can be rebuilt.

c. System or software updates can lead to unexpected issues or conflicts so having a backup provides a safety.

13.Write down any six possible threats to computer security.

Ans: Any six possible threats to computer security are:

a. Data Breaches
b. Malware
c. Phishing
d. Trojans
e. Ransomware
f. Keylogger

Data Breaches: It refers to an unauthorized access or use of sensitive information by individuals that were not originally intended to have access to that data.

Malware: Malware is short form of malicious software, and is a general term used to describe all of the viruses, spyware, worms, adware, trojan.

14.What is biometric verification?

Ans: Biometric verification or biometric security refers to the process of using unique physical or behavioral characteristics of an individual to verify their identity. Biometrics authentication is considered more secure than string password because physical or behavioral characteristics are distinctive to each person and difficult to forge(*copy illegally*).

Fingerprints, face detection or retina detection are being used as biometrics authentication.

15.Why is it important to protect computer system from dust?

Ans: It is important to protect computer system from dust because:

a. Dust and debris (*scattered pieces of rubbish*) can create heat, which can affect computer's motherboard.

b. It damages the electronic components by increasing the amount of heat. c. It can affect the hard disc drive.

d. Dust particles can create heat and as a result it can lead to reduced processing speed and overall system performance, affecting the user experience.