Multiple Choice Questions 1 Mark

Q 1. In which of the following, a person is constantly followed/chased by another person or group of several peoples?

(a) Phishing (b) Bulling

[✓ (c) Stalking] (d) Identity theft

Sol. (*c*) Stalking

Q 2. Which of the following is considered as the unsolicited commercial email?

(a) Virus (b) Malware

(c) Spam (d) All of these

Sol. (*c*) Spam

Q 3. Which of the following usually observe each activity on the internet of the victim, gather all information in the background, and send it to someone else?

(a) Malware (b) Spyware

(c) Adware (d) All of these

Sol. (*b*) Spyware

Q 4. ______ is a type of software designed to help the user's computer detect viruses and avoid them.

(a) Malware (b) Adware

(c) Antivirus (d) Both (b) and (c)

Sol. (*c*) Antivirus

Q 5. It can be a software program or a hardware device that filters all data packets coming through the internet, a network, etc. it is known as the______

(a) Antivirus [✓ (b) Firewall]

(c) Cookies (d) Malware

Sol. (*b*) Firewall

Q 6. Which of the following refers to stealing one's idea or invention of others and use it for their own benefits?

(a) Piracy

(b) Plagiarism

(c) Intellectual property rights

(d) All of the above

Sol. (*d*) All of the above

Q 7. Which of the following refers to exploring the appropriate, ethical behaviors related to the online environment and digital media platform?

(a) Cyber law (b) Cyberethics

(c) Cybersecurity (d) Cybersafety

Sol. (*b*) Cyberethics

Q 8. Which of the following refers to the violation of the principle if a computer is no more accessible?

(a) Access control (b) Confidentiality

(c) Availability (d) All of these

Sol. (c) Availability

Q 9. Which one option is not a type of cybercrime?

(a) Data theft

(b) Forgery

(c) Damage to data and systems

(d) Installing antivirus for protection

Sol. (*d*) Installing antivirus for protection

Q 10. McAfee is an example of

(a) Photo Editing Software

(b) Quick Heal

(c) Virus

(d) Antivirus

Sol. (*d*) Antivirus

Q 11. Cyber-crime can be categorised into ______ types.

(a) 4 (b) 3

(c) 2 (d) 6

Sol. (c) 2

Q 12. What is the name of the IT law that India is having in the Indian legislature?

(a) India's Technology (IT) Act, 2000

(b) India's Digital Information Technology (DIT) Act, 2000

(c) India's Information Technology (IT) Act, 2000

(d) The Technology Act, 2008

Sol. (a) India's Technology (IT) Act, 2000

Q 13. In which year India's IT Act came into existence?

(a) 2000 (b) 2001

(c) 2002 (d) 2003

Sol. (a) 2000

Q 14. McAfee is an example of

(a) Photo Editing Software

(b) Quick Heal

(c) Virus

(d) Antivirus

Sol. (*d*) Antivirus

Very Short Answer Type Questions

1 Mark

Q 1. What are the different cyber crime classifications?

Sol. Cyber crimes can generally be divided into three major categories

- Cyber crimes against individuals
- Property cyber crimes, and
- Anti-government cyber crimes.

Q 2. What is fraud by mail?

Sol. Mail fraud is an offence under U.S. federal law that involves any scheme that seeks to obtain money or valuables unlawfully under which the postal system is used in the commission of a criminal act at any point.

Q 3. What's ID Spoofing?

Sol. It is the practice of using the telephone network to display a number that is not that of the actual originating station on the receiver's caller ID display.

Q 4. What is the difference between hashing and encryption?

Sol. Both hashing and encryption are used to convert readable data into an unreadable format. The significant difference is that encrypted data can be transformed into original data by decryption, whereas hashed data cannot be processed back to the original data.

Q 5. How will you keep yourself updated with the latest cybersecurity news?

Sol. The following ways will help you to keep up with the latest cybersecurity updates:

- Follow news websites and blogs from security experts.
- Browse security-related social media topics.
- Check vulnerability alert feeds and advisory sites.
- Attend cybersecurity live events.

Short Answer Type I Questions

2 Marks

Q 1. What does cybercrime mean?

Sol. Cybercrime extends to all the actions carried out in cyberspace with criminal intent. Due to the internet's anonymous nature, miscreants participate in a number of criminal activities. The cybercrime field is just emerging and with each passing day, new types of criminal activities in cyberspace are coming to the fore.

Q 2. What is cybercrime against Government?

Sol. One distinct example of cybercrime against the government is cyber terrorism. The development of the internet has shown that individuals and groups are using the medium of cyberspace to threaten governments as well as terrorize a country's people. When a person hacks into a website run by the government or military, this crime manifests itself into terrorism.

Q 3. What is Hacking?

Sol. Hacking is the activity of identifying weaknesses in a computer system or a network to exploit the security to gain access to personal data or business data. An example of computer hacking can be: using a password cracking algorithm to gain access to a computer system.

Q 4. What is phishing in cyber crime? What are its types?

Sol. Phishing happens when an unsuspecting victim responds to fraudulent requests that demand action. This action can include downloading an attachment, clicking a link, filling out a form, updating a password, calling a phone number, or using a new Wi-Fi hotspot.

The 5 Most Common Types of Phishing Attack

- Email phishing. Most phishing attacks are sent by email.

- Spear phishing. There are two other, more sophisticated types of phishing involving email.
- Whaling. Whaling attacks are even more targeted, taking aim at senior executives.
- Smishing and vishing.
- Angler phishing.

Q 5. What are the laws concerning Cybercrimes in India?

Sol. Cyber crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the Information Technology Act, 2000. The Act does not define 'cyber crime'. However, any activities which basically offend human sensibilities would come within its ambit.

Short Answer Type II Questions

4 Marks

Q 1. Is Cyber harassment also a Cybercrime?

Sol. Yes, it is a distinct Cybercrime. Various kinds of harassment can and does occur in cyberspace, or through the use of cyberspace. Harassment can be sexual, racial, religious, or other. Persons perpetuating such harassment are also guilty of Cybercrime.

Q 2. Is hacking a Cybercrime?

Sol. Hacking is amongst the gravest Cybercrimes known till date. In simple terms it means an illegal intrusion into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. The offence is punishable under Section 66 of the IT Act,2000.

Q 3. What are the main types of cyber security?

Sol. Types of cyber security are as follows

- Network Security
- Cloud Security
- Endpoint Security
- Mobile Security
- IoT Security
- Application Security
- Zero Trust

Q 4. What is a CIA triad?

Sol. CIA (confidentiality, integrity, and availability) triad is a model designed to handle policies for information security within an organization.

- **Confidentiality** A collection of rules that limits access to information.
- **Integrity** It assures the information is trustworthy and reliable.
- **Availability** It provides reliable access to data for authorized people.

Q 5. List the common types of cybersecurity attacks.

Sol. The following are the most common types of cybersecurity attacks:

- Malware
- SQL Injection Attack
- Cross-Site Scripting (XSS)
- Denial-of-Service (DoS)
- Man-in-the-Middle Attacks
- Credential Reuse
- Phishing
- Session Hijacking

Long Answer Type Questions

8 Marks

Q 1. What is cyber crime? What are its types?

Sol. Cybercrime is the activity of using computers and networks to perform illegal activities like spreading computer viruses, online bullying, performing unauthorized electronic fund transfers, etc. Most cybercrime hacks are committed through the internet, and some cybercrimes are performed using Mobile phones via SMS and online chatting applications.

Types of Cybercrime

- **Privacy violation** Exposing personal information such as email addresses, phone number, account details, etc. on social media, hacking a websites, etc.
- **Identity theft** Stealing personal information from somebody and impersonating that person.
- **Sharing copyrighted files/information** This involves distributing copyright protected files such as eBooks and computer programs etc.
- **Electronic funds transfer** This involves gaining an un-authorized access to bank computer networks and making illegal fund transfers.
- **Electronic money laundering** This involves the use of the computer to launder money.
- **ATM fraud** This involves intercepting ATM card details such as account number and PIN numbers. These details are then used to withdraw funds from the intercepted accounts.
- **Denial of service attacks** This involves the use of computers in multiple locations to attack servers with a view of shutting them down.
- **Spam** Sending unauthorized emails. These emails usually contain advertisements.

Q 2. What is the main goal of Cyber Security?

Sol. The main objective of cyber security is to protect data from cyber-attacks. It follows a principle called CIA trio. It is a security sector that provides a triangle of three connected principles. The CIA model is used to help organizations to develop policies for their information security architecture. There are three main components Confidentiality, Integrity, and Availability of this CIA model. One or more of these principles is broken when it finds a security breach. This model provides a security paradigm to guide individuals through many aspects of IT security.

Confidentiality Confidentiality is used to provide privacy to prevent unauthorized access to data. It ensures that the data is only accessible to those who are authorized to use it and restricts access to others. It restricts vital information to be exposed to the wrong hands. A good example of Confidentiality is Data encryption which is used to keep information private.

Integrity The Integrity principle is used to assure that the data is genuine, correct, and safe from unwanted threat actors or unintentional user alteration. It also specifies that the source of information must be genuine. If any changes are made, precautions should be taken to protect sensitive data from corruption or loss and recover from such an incident quickly.

Availability The Availability principle ensures that the information is constantly available and accessible to those who have access to it. It also ensures that any types of system failures or cyber-attacks do not obstruct these accesses.

Q 3. What do you understand by Black Hat Hackers, White Hat Hackers and Grey Hat Hackers?

Sol.

- **Black hat hackers** Black Hat Hackers are the most critical types of hackers. They attempt to obtain unauthorized access to a system to disrupt its operations or steal sensitive and important data. Black Hat Hackers are also known as crackers.

  Black Hat Hacking is always illegal due to its malicious aim. The main purpose of Black Hat Hacking is to steal company data, violate privacy, cause system damage, block network connections, etc.

- **White hat hackers** White Hat Hackers are used to accessing the system for penetration testing and vulnerability assessments. They never intend to harm the system; rather, than strive to uncover holes in a computer or network system. White Hat Hackers are also referred to as Ethical Hackers.

  Hacking done by White Hat Hackers is called Ethical hacking. It is not a crime, and it is considered one of the most difficult professions in the IT business. Many businesses hire ethical hackers to do penetration tests and vulnerability assessments.

- **Grey hat hackers** Grey Hat Hackers are a combination of Black Hat Hackers and White Hat Hackers. They use elements of both black and white hat hacking techniques. They are supposed to act without malice, but for the sake of amusement, they can exploit the security flaw in a computer system or network without the permission or knowledge of the owner.

  The main goal of Grey Hat Hackers is to draw the owners' attention to the security flaw or hole in the network in the hope of receiving gratitude or a reward.