Chapter 6: Cyber Safety

Assignment Solutions

Multiple-Choice Questions (MCQs)

1. Which of the following is/are the stages in the life cycle of a virus?
   a. Creation b. Assimilation
   c. Eradication d. All of these

Ans. d

2. Which of the following terms describes the condition in which your computer stops working temporarily?
   a. Hang b. Virus attack
   c. Hacking d. None of these

Ans. a

3. Which of the following is a form of malware threat?
   a. Worm b. Trojan
   c. Virus d. All of these

Ans. d

4. Which of the following types of malware send advertisements to your computer?
   a. File infectors b. Boot sector viruses
   c. Macro viruses d. Adware

Ans. d

5. Which of the following types of malware locks your resources and releases them once payment gets made?
   a. Virus b. Worm
   c. Adware d. Ransomware

Ans. d

Very Short Answer Questions

6. What do you understand by hacking?

Ans. Hacking refers to the act of gaining an unauthorized access to another person's computer to steal or destroy crucial data or information.

7. What is data backup?

Ans. The copy of data that can be used to restore and recover data is called data backup.

8. Give examples of some popular antivirus software.

Ans. Some popular antivirus software are Norton Antivirus, McAfee, Quick Heal Antivirus, Kaspersky Antivirus, etc.

9. Name different resources used for data backups.

Ans. The different resources used for data backups are CD, Digital Versatile Disc (DVD), External hard disk, USB drive, Online backup and storage services, etc.

10. What is cyberbullying?

Ans. Cyberbullying mainly occurs to harass or embarrass someone else by using the Internet, mobile phones, emails, chatting or social networking.

Short Answer Questions

11. List some ways in which viruses can enter your computer.

Ans. E-mail attachments, games and animations are examples of programs that generally carry viruses from one computer to another. When the use of the Internet was not so widespread, viruses used to spread from one computer to another by means of a removable media, such as CD, DVD, flash drive, or floppy disk.

12. What are the damages that a virus attack can cause to a computer?

Ans. The damages that a virus attack can cause to a computer are:
- Destroying your computer File Allocation Table (FAT), which may eventually corrupt the entire file system. As a result, you may have to reinstall the file system.
- Deleting or removing files and programs from your hard disk.
- Creating duplicate files, thereby reducing the available space on your hard disk

13. What precautions can you take to prevent a virus attack on your computer?

Ans. You can follow these precautions to prevent a virus attack on your computer:
- Avoiding the temptation to open e-mail attachments and downloads from unreliable sources.
- Resist the urge to double-click everything in your mailbox. If you get an unexpected file attachment, send an enquiry e-mail to its sender. Ask him about the nature and function of the file attachment.
- Installing a reliable antivirus scanning software and downloading its updates regularly.
- Keeping regular backups of your data.

14. What is firewall? Why is it used in a network?

Ans. A firewall is software and hardware that protects networks, servers and computers from virus and hacker attacks. It is used to provide protection against unauthorized and unwanted communication between computers over a network. It enforces strong authentication for a user who wants to access information

and resources over the network. It protects a computer against security vulnerabilities and malicious activities on the Internet.

15. What is spoofing? What are its different types?

Ans. Spoofing is the technique used by unethical hackers to certify fake data over the Internet for stealing confidential information. Spoofing can be done in two ways:

1. **IP spoofing:** In this method, unethical hackers create IP (Internet Protocol) packets with a fake IP address to hide the true IP of the sender or pose as another computer's IP. An IP address is a unique address allocated to a computer on the network.

   E-mail spoofing: In this method, unethical hackers create e-mail messages with fake or forged sender addresses.

Long Answer Questions

16. Discuss the concept of phishing with a suitable example.

Ans. Phishing refers to a technique of obtaining personal information, such as login name, password and credit card details. Phishing normally takes place through e-mail or instant messaging. In phishing, an imposter sends you an e-mail or uses a website, that looks genuine, to trick people into giving important information about themselves. For example, the imposter may send an e-mail (which appears genuine to you), pretending to be a representative of your company. In the e-mail, he/she may ask you to update your information online by clicking a specified link. As you click the link, you may be redirected to a fraudulent website where you are asked to enter important information about yourself, which can later be used for cybercrime and fraud.

17. What is computer security? What should be done to keep the information secure in your computer?

Ans. Computer security is the process of ensuring the integrity, availability, and confidentiality of computer data and resources against threats, viruses and vulnerability. On the other hand, information security refers to the protection of information. Security is implemented mainly through two processes, authentication and authorization. Authentication refers to the process of recognizing the identity of a user, while authorization is the process of providing access to various resources, such as databases and printers, to the authenticated users. Integrity, confidentiality, and availability of information should be maintained for securing information. You must follow these guidelines in order to secure your information:

- Avoiding the temptation to open e-mail attachments and downloads from unreliable sources.
- Resisting the urge to double-click everything in your mailbox. If you get an unexpected file attachment, send an enquiry e-mail to its sender. Ask him about the nature and function of the file attachment.
- Installing a reliable antivirus-scanning software and downloading its updates regularly.
- Updating the system and antivirus software on a regular basis.

18. Explain the importance of maintaining privacy in Internet.

Ans. Maintaining privacy refers to preserving the confidentiality of information related to an individual or an organization. The regulations that support privacy consider that every individual has the right not to publicize everything related to him. The issue of privacy includes the following:

- **Access to Personal Information:** Refers to the access to such information related to an individual, which he/she may or may not want to share. For example, the personal contact number, address, and relationship status are some of the personal information of an individual, which should not be made public without the individual's consent.
- **Ethical Responsibility of Business:** Involves fair disclosure of terms of employment, policy and procedures to be followed, and equal treatment for all the employees. Hurting the sentiments of any employee intentionally is an unethical practice by the employer.
- **Adequate Disclosure:** Involves maintaining a balance between the right to information and privacy of an individual. The data that is not required to be disclosed should not be disclosed. In case it becomes necessary to disclose any such information, prior consent must be taken from the individual to whom this information belongs.
- **Personal Communication:** Involves unauthorized access to personal communication between two parties without their consent. Every individual has the right to express his or her feelings to the extent that it does not hurt the sentiments of anybody else. Accessing the personal email inbox and reading personal mails of an individual is unethical.

19. Discuss cookies along with their type.

Ans. A cookie is a file that contains small textual information about the activity of a user. For example, it may contain your log-in details of a particular website, so that, when you visit the same website again, it retrieves the information about you from the cookie and automatically fills your log-in details. Different types of cookies store different types of information about a user. For example, session cookies are used to track a person when he/she is currently navigating a website. When the person leaves the website for some time, the session cookie disappears. The tracking cookies are used for creating and storing user's long-term records during his/her multiple visits to a particular website. Another kind of cookies is known as authentication cookies which are used for determining whether a particular user is logged-in or not. If the user is logged-in, then what's the name of the user? Cookies are very useful for activity tracking, but there are some threats attached to them. Some virus or malware can be transferred to your computer in the form of cookies. Moreover, hackers can also steal your private or personal information stored in cookies.

20. Describe confidentiality of information along with the practices for maintaining confidentiality.

Ans. Confidentiality ensures that only an authorized person can access the network resources to get the valuable information provided on the network. A good example where confidentiality of information plays an important role is the credit card transaction. When we use a credit card to pay our dues through a computer system, the credit card number is transmitted over the network in an encrypted format, so that the other persons cannot read the information. The confidentiality of information can be ensured by the following practices:

- **Use Firewall:** Firewalls are software and hardware that protect networks, servers and computers from virus and hacker attacks. They are used to provide protection against unauthorized and unwanted communication between computers over a network. A firewall enforces strong

authentication for a user who wants to access information and resources over the network. Firewalls protect a computer against security vulnerabilities and malicious activities on the Internet.

- **Use your browser settings to prevent your tracking:** When you are online, a website tracks your information by using IP address. Your information may include your location, identity of your computer, system names, etc. You can prevent websites from tracking you by using the Inprivate browsing settings and disabling cookies in your browser.
- **Avoid posting personal information on the Internet:** Whatever you post on the Internet using social networking sites or chat platforms is available to unknown people on the Internet. Your post can be used later for any illicit purposes. Therefore, it is recommended that you must be careful while posting your personal information.

Application Oriented Questions

1. What are the different ways of finding IP address of a computer using some popular operating system?

Ans. The different ways of finding IP address of a computer using some popular operating system are:

Windows operating system:

- Open Command Prompt. The command prompt window opens.
- Type ipconfig in the command prompt window.
- Press Enter.
- The IP address gets displayed.

Linux operating system:

- Open terminal. The terminal window opens.
- Type ipconfig or ip in the terminal window.
- Press Enter.
- The IP address gets displayed.

2. Match the following:

TERMS	DESCRIPTION
A. Cookie	1. It refers to the technique used by unethical hackers to certify fake data over the Internet for stealing confidential information.
B. Spoofing	2. It refers to the technique of obtaining personal information, such as login name, password and credit card details.
C. Phishing	3. It refers to the act of gaining an unauthorized access to another person's computer to steal or destroy crucial data or information.
D. Hacking	4. It refers to a program that appears or pretends to be a genuine application but actually causes damage to the executable files on the computer.
E. Trojan horse	5. It is a file that contains small textual information about the activity of a user.

Ans.

A 5
B 1
C 2
D 3
E 4