CHAPTER 6
COMPUTER SECURITY AND ETHICS

SHORT AND LONG QUESTIONS

Q.1 Define cybercrime.

Ans: Cybercrime:

Cybercrime refers to any crime that is committed by means of computer and Internet technology by having unlawful access to others' computers.

Many governments have passed cybercrime bill that carry fines and prison sentences for cybercriminals.

Q.2 Describe some commonly committed cybercrimes.

Ans: Commonly committed cybercrimes:

The following are the commonly committed cybercrimes.

i. Computers have been involved in crimes such as fraud, kidnapping, murder and crimes related with stealing money from bank and credit card company.

ii. Criminals use Internet to steal personal information of other users and commit various types of cybercrimes. Personal information includes username, password, credit card number, bank account number, etc.

iii. Downloading illegal software, music files and videos are also cybercrimes.

iv. Internet harassment or cyber bullying is also a serious crime committed by cybercriminals. Internet harassment includes sending threatening e-mail, spreading rumors or virus, making defamatory comments, sending pornography or other bad material.

v. Making negative comments about an individual on Internet can damage reputation or cause physical or mental harm to the victim.

Q.3 What are computer viruses?

Ans: Computer Viruses:

Some computer experts create malware such as virus, spyware, worm etc. and spread through Internet. It is very importance to understand how malware spreads and how to protect computer from them.

It is very difficult to list all the symptoms of infected computers. The reason for this is that there are hundreds and thousands of malicious programs and new ones are created every day. Sometime, some infected computers do not show any symptom and the user thinks that his computer is not infected.

For Your Information

Firewall is a software or piece of hardware used to prevent unauthorized Internet users from accessing computer systems that are connected to Internet.

Tip

To create a strong password, you should combine upper-case and lower-case letters, numbers and special symbols.

Q.4 Describe the term multimodal authentication.

Ans: Multimodal Authentication:

Multimodal authentication means combination of two or more types of authentication methods. Normally, authentication methods use a single source of information for authentication such as features of face, fingerprint, hand geometry, access cards, etc. Multimodal authentication uses multiple sources of information for identification.

For example, fingerprint and face recognition can be combined for a multimodal biometric authentication system. As another example, a multimodal authentication can combine access card and PIN to open security gate.

Q.5 Describe computer ethics in information accuracy, information ownership, intellectual property rights, software piracy and information privacy.

Ans: Areas of Computer Ethics:

The following are main areas of computer ethics.

- Information accuracy
- Information ownership/Intellectual rights
- Intellectual Property
- Software piracy
- Information privacy
- Internet and Privacy

Information Accuracy:

Information stored on computers must be accurate, up-to-date and complete. If wrong information is entered in computer, it can be very harmful. People may suffer because of inaccurate information stored on computer. For example, a credit card holder may be wrongly blacklisted if wrong information is entered into the computer.

Information Ownership/Intellectual Rights:

Information ownership or intellectual rights mean persons who create ideas in any form are the actual owners. Ideas may be in the form of poems, plays, novels, films, drawings, paintings, software, etc. Intellectual rights protect creative work from unauthorized use by other people and allow creators to benefit financially from their work.

Intellectual Property:

Intellectual property means the legal rights of an individual or a corporation that result from intellectual activity in literary, artistic, scientific and industrial fields. Countries have law to protect intellectual property to foster innovation and promote creativity.

Software Piracy:

Software piracy means making illegal copies of software for use or sale for financial benefit. When computer users buy licensed software, they have the right to use it on a single computer. Software Copyright Law does not allow to make illegal copies of software and install it on other computers or sell it. It allows software developers to benefit financially from their work.

Information Privacy:

Information privacy refers to an individual's right to the privacy of personal information. In modern information age, people are concerned that computers may be taking away their privacy. The Data Protection Act (Law) protects the rights of the individuals against misuse of personal information by organizations. Organizations that hold the information should not allow unauthorized people to have access to information or disclose it to anyone outside the organization.

Internet and Privacy:

People who use Internet are worried that it may be eroding their privacy. Internet users post their personal information such as full name, date of birth, place of residence, phone numbers, pictures, videos etc. on the Web and it stays there. Internet users enter personal information in websites to sign up or register for services without realizing that this may lead to invasions of privacy. This information can be accessed by hackers and used for harmful purpose. This poses a serious threat to privacy as unauthorized people can access personal information of individuals. Therefore, people are concerned about invasion of computer and Internet technology into people's privacy.

KEY POINTS

- Computer security refers to protecting computer hardware, software and information stored on computer from threats.
- A crime that is committed by means of computer and Internet technology is known is cybercrime.
- A person who illegally breaks into others' computer systems is known as hacker.
- A person who uses special tools for breaking into computer systems is known as cracker.
- Malware means malicious software. It comprises of barmful software such as virus, worm, spyware etc. that are threats to all computer users.
- Malware spreads through infected flash drives, CDs, pirated software, Internet, e-mail attachments and devices that are plugged into computer's USB ports.
- Authentication means identifying a person based on a method such as Username and Password, Personal Identification Number, Access Card or Biometrics.
- Authorization verifies that an authenticated person has permission to access computer system and use it.

- Personal Identification Number (PIN) is a confidential numeric password used to authenticate a user to get access to computer system.
- Access cards are very similar in appearance to credit cards. They are used to open security gates, parking barrier and doors of hotel rooms.
- Biometrics is a method based on measurement of features of face, fingerprint, hand geometry, signature and voice for authentication of individuals.
- Multimodal authentication combines two or more types of authentication methods such as face and fingerprint for identification of individuals.
- Computer ethics is concerned with the moral guidelines for the ethical use of computer technology. It specifies what is right and what is wrong when using computers.
- Information ownership or intellectual rights mean a person who creates an idea in any form is the actual owner. Intellectual rights protect creative work from unauthorized users and allows creator to benefit financially.
- Software piracy means making illegal copies of computer software for use or sale for financial benefit.

EXERCISE

Q1. Select the best answer for the following MCQs.

i. What is a person who illegally breaks into others' computer systems called?
A. Computer engineer B. System programmer
C. Hacker D. Cracker

ii. What is a person who uses special tools for breaking into computer systems called?
A. Computer engineer B. System programmer
C. Hacker D. Cracker

iii. Which malware spreads automatically in computer networks and replicates itself?
A. Virus B. Worm
C. Adware D. Spyware

iv. Which of the following malware displays advertisements on the screen?
A. Virus B. Worm
C. Adware D. Trojan

v. Which of the following authentication method is used for opening security gates?
A. Username and password B. Personal Identification Number
C. Access card D. Biometrics

vi. Which of the following authentication method is most reliable?
A. Username and password B. Personal Identification Number
C. Access card D. Biometrics

- Personal Identification Number (PIN) is a combinational numeric password.
- Passwords are the most common form of authentication.
- Hackers uses are very similar to password to crack code. They are used to gain access to computer systems, networks and data files.
- Biometrics is a method based on measurement of features of the individual, such as fingerprints, signature and voice, eye and face recognition.
- Biometrics is used to authenticate a user to access your computer networks and sensitive data and business information.

Q1. Select the best answer for the following MCQs.

What is the full form of PIN which is used for authentication purpose when?
a. Personal Identification Number b. Personal Identification Number
c. Personal Identification Number d. Personal Identification Number

Which of the following is not a good way to create a strong into computer systems when?
a. Use a mixture of letters, numbers and symbols b. Use a mixture of letters, numbers and symbols
c. Use a mixture of letters, numbers and symbols d. Use a mixture of letters, numbers and symbols

Which of the following authentication method is based on features of individuals such as face, fingerprint and voice?
a. Biometrics b. Personal Identification Number
c. Biometrics d. Personal Identification Number

What is known as the process of authentication for use on other computers in case called?
a. Single sign on b. Intellectual rights
c. Single sign on d. Intellectual rights

Which of the following authentication method is based on your activities on computer?
a. Voice b. Voice
c. Voice d. Voice

Which of the following authentication technology is used in drive cash from ATM?
a. Personal Identification Number b. Personal Identification Number
c. Personal Identification Number d. Personal Identification Number

Q1	Q2	Q3	Q4	Q5
a	a	a	a	a

Write descriptive answers.

Q6. Define cybercrime.
Answer:
Cybercrime refers to any crime that is committed by means of computer networks or hardware device. Cybercrime is also known as computer crime.

Q7. What is the importance of computer security?
Answer:
Computer security refers to protecting computer hardware, software, and information from unauthorized access.

Importance of Computer Security:
- Computer security is used to protect information with each other or communicate over internet. You can utilize a web browser with a strong encryption to protect your data.
- Computer security is safety is important for computer users to protect their information from hackers. Hackers can use your data for their own benefit. Hackers should attempt and business competitors.
- Computer security is important for business organizations.

Q8. Define cybercrime.
Answer:
- Hackers are highly trained into other computer systems is known as cybercrime.
- Cybercrime is also known as computer crime.
- Cybercrime is a crime that is committed by means of computer networks or hardware device.
- Cybercrime is also known as computer crime.
- Cybercrime is a crime that is committed by means of computer networks or hardware device.

Q9. What is the importance of computer security?
Answer:
Computer security refers to protecting computer hardware, software, and information from unauthorized access.

Importance of Computer Security:
- Computer security is used to protect information with each other or communicate over internet. You can utilize a web browser with a strong encryption to protect your data.
- Computer security is safety is important for computer users to protect their information from hackers. Hackers can use your data for their own benefit. Hackers should attempt and business competitors.
- Computer security is important for business organizations.

Q10. Define cybercrime.
Answer:
- Hackers are highly trained into other computer systems is known as cybercrime.
- Cybercrime is also known as computer crime.
- Cybercrime is a crime that is committed by means of computer networks or hardware device.
- Cybercrime is also known as computer crime.
- Cybercrime is a crime that is committed by means of computer networks or hardware device.

- Hackers have in-depth knowledge of network programming and can create and maintain software for others to break into networks and create viruses.

Example:
- For example, a hacker intercepts a software or email, a Dictionary file is created in the dictionary section. When the software is run it tries all the dictionary words and if one matches, the password is found. Hackers can also use a brute force attack to find a strong password that uses a mix of letters, numbers and symbols.

- Cybercrime is a computer crime that involves into computer systems without permission. Cybercrime is also known as computer crime. Cybercrime is a crime that is committed by means of computer networks or hardware device.
- Most of the hacking can be have professional computer user to be able to hack into computer systems but they have knowledge about using hacking tools.
- Hackers are highly trained into other computer systems is known as cybercrime.
- Cybercrime is also known as computer crime. Cybercrime is a crime that is committed by means of computer networks or hardware device.

Example:
- For example, a hacker can install a key logger on stealing user's computer through internet or hardware software which records every keystroke when a key is pressed. Hackers can also use a brute force attack to find a password. If a password is in the custom a computer. Hacker, he can easily hack the Facebook account.

Q11. Describe any five examples of malware.
Answer: Malware is a short for malicious software.
- A type of computer programme of malware programs is given below.
- Computer viruses are a type of malware that can be spread through the different types of an email messages spread to the network.
- Computer worms are a type of malware.
- Programs do not run on a normal way.
- Programs do not run on a normal way.
- Malware is a short for malicious software.
- Trojans are stored in computer and hard disk.
- Trojans are stored in computer and hard disk.
- Malware programs are used to destroy and program.
- Malware programs are used to destroy and program.
- Malware programs are used to destroy and program.

Q12. Differentiate between authentication and authorization.
Answer:
- Authentication is the process of ensuring that someone is who he/she claims to be.
- Authentication is the process of ensuring that someone is who he/she claims to be.
- Authentication is the process of ensuring that someone is who he/she claims to be.