Computer chapter # 06 Security

Why is computer security important?
Answer: Computer security is crucial to protect sensitive data, maintain privacy, prevent unauthorized access, and ensure the integrity and reliability of computer systems.

Define cybercrime.
Answer: Cybercrime refers to criminal activities conducted over the internet, including hacking, identity theft, and various forms of online fraud.

Hackers and Crackers:
What is the difference between a hacker and a cracker?
Answer: A hacker is someone who uses their skills to gain knowledge and solve problems, while a cracker is someone who breaks into computer systems with malicious intent.

Define malware.
Answer: Malware, short for malicious software, is any software specifically designed to harm or exploit computers, networks, or users.

List different types of malware.
Answer: Types of malware include viruses, worms, spyware, adware, trojan horses, ransomware, and more.

Explain what a computer virus is.
Answer: A computer virus is a type of malware that attaches itself to legitimate programs and spreads when those programs are executed.

Differentiate between viruses and worms.
Answer: Viruses require a host file to spread, while worms are standalone programs that can replicate and spread independently.

What is spyware?
Answer: Spyware is software that secretly gathers information about a user's activities without their knowledge and sends it to third parties.

Define adware.
Answer: Adware is software that displays unwanted advertisements on a user's device, often in the form of pop-ups or banners.

What are common symptoms of a malware attack?
Answer: Common symptoms include slow computer performance, unexpected crashes, pop-up ads, unauthorized access, and changes to system settings.
How can you protect your computer from malware?
Answer: Use antivirus software, keep operating systems and software updated, be cautious of email attachments and links, and avoid downloading from untrusted sources.

What is antivirus software used for?
Answer: Antivirus software is used to detect, prevent, and remove malware from a computer system.

Explain the purpose of anti-spyware.
Answer: Anti-spyware tools are designed to detect and remove spyware from a computer, protecting users' privacy and preventing unauthorized data collection.

What is authentication?
Answer: Authentication is the process of verifying the identity of a user, system, or device to ensure that it is legitimate and authorized to access certain resources.

Explain the concept of authorization.
Answer: Authorization is the process of granting or denying access to specific resources or services based on the authenticated identity of a user.

Define authorized access.
Answer: Authorized access refers to the legitimate and permitted use of resources or services by a user who has been properly authenticated and granted permission.

What is unauthorized access?
Answer: Unauthorized access occurs when a user gains entry to a system, application, or data without proper authentication or permission, violating security protocols.

List common authentication methodologies.
Answer: Common authentication methodologies include something you know (e.g., passwords), something you have (e.g., access cards), and something you are (e.g., biometrics).

Explain the use of a username and password for authentication.
Answer: A username is a unique identifier for a user, and a password is a secret code known only to the user, providing a combination for authentication.

What are the challenges associated with using usernames and passwords?
Answer: Challenges include the risk of password theft, users choosing weak passwords, and the need to remember multiple username-password combinations.

Define Personal Identification Number (PIN) and its use.
Answer: A PIN is a numeric code used for authentication. It is typically associated with access to devices, accounts, or services and is often used with a card or token.

How do access cards contribute to authentication?
Answer: Access cards, often used in combination with PINs, serve as physical tokens granting access to a secure area or system when presented to a card reader.

Explain the concept of biometrics in authentication.
Answer: Biometrics involves using unique physical or behavioral characteristics, such as fingerprints, iris scans, or facial recognition, for identity verification.

What are the advantages of using biometrics for authentication?
Answer: Advantages include increased security, reduced reliance on passwords, and the difficulty of replicating or forging biometric traits.

What is multimodal authentication?
Answer: Multimodal authentication involves using multiple forms of identification, such as fingerprints, facial recognition, and voice recognition, to verify a user's identity.

Define computer ethics.
Answer: Computer ethics is the study of ethical issues related to the use of computers and technology, addressing moral dilemmas and responsible behavior in the digital realm.

Why is the ethical use of computers important?
Answer: The ethical use of computers is crucial to promote responsible behavior, protect privacy, prevent cybercrimes, and ensure fair access to technology.

List some areas of computer ethics.
Answer: Areas of computer ethics include privacy, security, intellectual property, digital rights, accessibility, and responsible use of technology.

Why is information accuracy important in computer ethics?
Answer: Information accuracy is essential to prevent the spread of misinformation, maintain trust, and ensure that users make informed decisions based on reliable information.

Explain information ownership or intellectual rights.
Answer: Intellectual rights involve the legal protection of creations of the mind, such as inventions, literary and artistic works, and symbols, names, and images used in commerce.

What is intellectual property?
Answer: Intellectual property refers to creations of the mind, such as inventions, literary and artistic works, designs, symbols, names, and images used in commerce, for which there are legal protections.

Why is respecting intellectual property important in computer ethics?
Answer: Respecting intellectual property ensures that creators are rewarded for their efforts, encourages innovation, and protects the rights of individuals and organizations.

Define software privacy.

Answer: Software privacy involves protecting users' personal information and ensuring that software applications do not compromise their privacy.

What is information privacy in the context of computer ethics?
Answer: Information privacy is the protection of individuals' personal information and the right to control how their data is collected, stored, and used.

Why is internet privacy a concern in computer ethics?
Answer: Internet privacy is a concern as it involves safeguarding users' personal information, preventing unauthorized access, and ensuring that individuals have control over their online data.

How can individuals protect their privacy on the internet?
Answer: Individuals can protect their privacy by using strong passwords, being cautious about sharing personal information, using privacy settings, and being aware of online security pra