Descriptive

1. **a.** Define cybercrime and discuss its origins. How does understanding the definition and origins help in addressing cybercrime?

b. Who are cybercriminals, and what motivates them to engage in cybercrime? Analyze the different motivations and types of cybercriminals.

2. **a.** Describe the different categories of cybercrime. How do these categories influence the planning and execution of cyberattacks?

b. Explain the process of reconnaissance and passive attacks in the context of cybercrime. How do these techniques contribute to the success of subsequent cyberattacks?

3. Discuss the different types of credit card frauds that occur in the mobile and wireless computing era. What preventive measures can organizations implement to combat these frauds?

* * * * *

1. **a.** Describe and classify different types of cybercrimes such as email spoofing, spamming, and identity theft. How do these classifications help in developing preventive measures?

b. Analyze the impact of online frauds and computer sabotage on organizations. What strategies can be employed to mitigate these issues?

2. **a.** Discuss the different types of social engineering and their effectiveness in cyberattacks. How can individuals and organizations protect themselves from social engineering tactics?

b. Analyze the impact of botnets on cybercrime. What are the primary attack vectors used by botnets, and how can organizations defend against them?

3. Explain the concept of social engineering and its various classifications. How can organizations design security measures to mitigate the risks associated with social engineering attacks?

* * * * *

1. **a.** Explain the concept of internet time theft and salami attacks. How do these types of cybercrimes affect individuals and organizations?

b. What is the significance of password sniffing and credit card frauds in the context of cybercrime? Discuss the methods used in these attacks and preventive measures.

2. **a.** Explain the concept of cyberstalking and its different types. Provide a real-life example of a cyberstalking incident and discuss the impact it had on the victim.

b. How does cloud computing contribute to or mitigate cybercrime? Discuss the relationship between cloud computing services and cybercrime.

3. Analyze how unconventional or stealth storage devices can pose security risks. What best practices can organizations follow to mitigate risks associated with these devices?

* * * * *

Open Book

1. Discuss the concept of computer network intrusions and explain the various techniques used by cybercriminals to execute such attacks. How can organizations protect themselves from these intrusions?
2. Analyze the process of gaining and maintaining system access during a cyberattack. What techniques do cybercriminals use, and how can organizations detect and prevent these techniques?
3. Assess the security implications of using cloud computing in the context of mobile and wireless devices. What are the potential risks, and how can they be mitigated?

* * * * *

1. Evaluate the impact of identity theft and software piracy on both individuals and businesses. What legal and technical measures can be taken to prevent and address these issues?
2. Discuss the impact of botnets on the security of network systems. How do botnets operate, and what strategies can be implemented to mitigate their effects?
3. Examine the different types of mobile device attacks, such as mishing, vishing, and smishing. How can users and organizations effectively defend against these attacks?

* * * * *