**Unit-3**

1. What are common mobile phone attacks and why are they significant for organizations?

2. Explain the security implications mobile devices pose for organizations and how they can manage them.

3. Discuss the role of policies and Mobile Device Management (MDM) in enhancing mobile security for organizations.

**Unit-4**

1. What is the primary objective of using proxy servers and anonymizers in cybercrimes? Provide examples of scenarios where these tools are employed and discuss their impact on anonymity and security.

2. Explain the concept of phishing and its common methods. Discuss the potential risks and consequences of falling victim to phishing attacks, both for individuals and organizations.

3. How do virus and worm malware differ in their modes of operation and potential impact on computer systems and networks? Provide real-world examples of virus and worm attacks and discuss the key distinctions between these two types of malware.

**Unit-5**

1. Explain the concept of insider threats in the context of cybercrimes. Provide examples of insider threat scenarios and discuss the potential impact on organizations.

2. Discuss the importance of privacy in cyber security and its implications for organizations. Explain how organizations can balance privacy concerns with the need for effective cyber security measures.

3. Outline the key challenges that organizations face in the realm of cyber security. Discuss the impact of these challenges on organizational security and strategies organizations can adopt to address them.