**1. Compare and contrast phishing and social engineering. How might an attacker use these techniques in combination to compromise an organization's security? Provide a specific example scenario.**

**Additional details:**

This question tests the understanding of two key concepts in cybersecurity: phishing and social engineering. Both involve manipulation and deception, but phishing often refers to specific email-based attacks, while social engineering is broader, covering any manipulation of people to bypass security. The scenario element challenges students to think critically about how these techniques can work together to breach an organization’s defenses.

**Expected elements of a strong answer:**

* **Definitions**: Clear and accurate definitions of phishing (typically email-based attacks using deception to trick users into revealing sensitive information) and social engineering (the broader manipulation of individuals into compromising security, often through psychological tactics).
* **Similarities and Differences**:
  + Similarities: Both rely on manipulating human behavior and exploiting trust.
  + Differences: Phishing is a specific tactic (often email-based), while social engineering includes various methods (such as phone calls, impersonation, or in-person interaction).
* **Example Scenario**: A strong scenario might involve a phishing email that tricks an employee into revealing login credentials, followed by a phone call (social engineering) to gather more details (e.g., security questions or two-factor authentication codes) to fully compromise an account.

**2. Discuss the potential security vulnerabilities in wireless communications. What measures can individuals and organizations take to mitigate these risks?**

**Additional details:**

This question explores the vulnerabilities of wireless networks, a common topic given how many individuals and businesses rely on wireless communication. Responses need to demonstrate knowledge of specific risks associated with wireless communication and think critically about mitigation strategies from both personal and organizational perspectives.

**Expected elements of a strong answer:**

* **Vulnerabilities**:
  + Eavesdropping, where unauthorized individuals intercept data.
  + Man-in-the-middle (MitM) attacks, where attackers insert themselves between two communicating parties.
  + Rogue access points, where attackers set up fake Wi-Fi networks to lure users.
* **Mitigation for Individuals**:
  + Using virtual private networks (VPNs) when on public Wi-Fi.
  + Avoiding sensitive transactions (like banking) over unsecured networks.
  + Enabling two-factor authentication (2FA).
* **Mitigation for Organizations**:
  + Implementing WPA3 for better encryption.
  + Regular security audits of wireless networks.
  + Using network segmentation to isolate sensitive data.

**3. Define malware and describe its potential effects on a computer system. What are some common ways malware is spread, and how can individuals protect their devices from infection?**

**Additional details:**

This question encourages responses which explain what malware is, describe its impact, and offer preventive solutions. It asks them to connect general cybersecurity knowledge with practical advice that they can apply in their daily lives.

**Expected elements of a strong answer:**

* **Definition of Malware**: Malicious software designed to harm, exploit, or take unauthorized control of a computer system.
* **Potential Effects**:
  + Slowing down system performance.
  + Stealing or destroying sensitive data.
  + Locking users out of their systems (e.g., ransomware).
* **Spread Methods**:
  + Email attachments with malware.
  + Infected websites (drive-by downloads).
  + Malicious downloads from seemingly legitimate sources.
* **Protection Strategies**:
  + Installing and regularly updating antivirus software.
  + Avoiding suspicious links, email attachments, and downloads.
  + Regularly scanning devices for threats.
  + Keeping operating systems and applications up to date.