

# Advanced Cybersecurity for Digital Citizens

Cybersecurity · Practice Test · 12 Questions

---

**1. Which advanced cyberattack typically involves an attacker secretly altering or compromising software during its development or distribution, impacting its users after deployment?**

- A) Phishing attack
- B) Denial-of-Service (DoS) attack
- C) Supply chain attack
- D) Brute-force attack

**2. What is the primary function of a 'honeypot' in cybersecurity, beyond simply detecting intrusion attempts?**

- A) To encrypt network traffic for secure communication
- B) To create an attractive, fake target to lure and study cyberattackers
- C) To block unauthorized access to a private network
- D) To automatically update software vulnerabilities across a system

**3. What distinguishes a 'zero-day exploit' from other software vulnerabilities?**

- A) It is a flaw that has been publicly known and patched for over a year
- B) It is a vulnerability known to the software vendor but not yet patched or publicly disclosed
- C) It is an exploit specifically designed for hardware rather than software
- D) It is a security flaw that can only be exploited by government agencies

**4. Which cryptographic principle ensures that transmitted data remains unaltered and intact during transit, protecting against accidental or malicious modification?**

- A) Confidentiality
- B) Authentication
- C) Integrity
- D) Non-repudiation

**5. What is the most significant privacy concern associated with 'data aggregation' by large tech companies?**

- A) It slows down internet speeds for individual users
- B) It prevents users from accessing their own data
- C) It allows for the creation of detailed user profiles that can predict behavior and be misused
- D) It increases the cost of internet services for consumers

**6. In the context of network security, what is the primary purpose of Network Address Translation (NAT)?**

- A) To assign unique public IP addresses to every device within a private network
- B) To translate domain names into IP addresses for web browsing
- C) To allow multiple devices on a private network to share a single public IP address
- D) To encrypt all data packets leaving a private network

**7. What kind of malware creates a 'botnet' by infecting multiple computers and allowing a remote attacker to control them as a group?**

- A) Ransomware
- B) Spyware
- C) Trojan horse
- D) Bot

**8. Which security measure is specifically designed to protect against unauthorised modification of data by verifying its origin and content through digital signatures?**

- A) Data encryption
- B) Multi-factor authentication
- C) Firewall rules
- D) Digital certificates

**9. What does 'sandboxing' refer to in cybersecurity?**

- A) Storing sensitive data on isolated physical servers
- B) Running untrusted programs in a segregated environment to prevent harm to the main system
- C) Encrypting entire hard drives to protect all stored data
- D) Using a virtual private network (VPN) to obscure online activity

**10. Why is 'public Wi-Fi' considered less secure than a private home network, even with a password?**

- A) Public Wi-Fi networks always have slower internet speeds
- B) The encryption on public Wi-Fi is usually weaker or non-existent, making traffic easier to intercept
- C) Public Wi-Fi networks do not allow access to secure websites (HTTPS)
- D) Public Wi-Fi routers do not have built-in firewalls

**11. What is the primary risk associated with 'privilege escalation' in a cyberattack?**

- A) The attacker gains faster internet access
- B) The attacker gains higher-level access than initially granted, allowing more control over the system
- C) The attacker can only view public information on the system
- D) The attacker can only disable user accounts, not modify data

**12. Which type of software is specifically designed to identify, prevent, and remove malicious software from a computer system?**

- A) Operating system
- B) Web browser
- C) Antivirus software
- D) Word processor