#1. What is a common method for protecting sensitive information on a mobile device?

☐
Using a strong passcode or biometric authentication
☐
Disabling all security features
☐
Sharing passwords with friends
☐
Keeping the device unlocked
☐
None of the above

#2. What does the acronym IDS stand for in the context of cybersecurity?

☐
Intrusion Detection System
☐
Internet Data Security
☐
Internal Data System
☐
Integrated Defense System
☐
None of the above

#3. What is the term for a program that appears to be useful or legitimate, but actually carries out malicious activities in the background?

☐
Trojan Horse
☐

Spyware
☐
Adware
☐
Ransomware
☐
None of the above

#4. Which of the following is NOT a recommended method for securing a Wi-Fi network?

☐
Changing the default SSID and password
☐
Enabling WPA2 or WPA3 encryption
☐
Disabling remote management
☐
Broadcasting the network name (SSID)
☐
None of the above

#5. What is the purpose of a security audit?

☐
To assess and evaluate the security measures and controls in place
☐
To hack into a system to identify vulnerabilities
☐
To delete sensitive information
☐
To optimize network performance
☐
None of the above

#6. What is the term for a technique used to verify the authenticity of a message or document?

☐
Digital signature
☐
Encryption
☐
Authentication
☐
Authorization
☐
None of the above

#7. Which of the following is a common social engineering technique that involves impersonating a trusted entity in order to trick individuals into revealing sensitive information?

☐
Phishing
☐
Denial of Service
☐
Firewall
☐
Penetration testing
☐
None of the above

#8. What is the primary goal of a security incident response plan?

☐
To outline the steps to take in the event of a security breach
☐
To prevent security incidents from occurring

☐
To analyze network traffic
☐
To install antivirus software
☐
None of the above

#9. Which type of attack involves flooding a network or server with excessive traffic to make it unavailable to legitimate users?

☐
DDoS (Distributed Denial of Service) attack
☐
Man-in-the-Middle (MitM) attack
☐
Phishing attack
☐
Trojan attack
☐
None of the above

#10. What is the term for the practice of gaining unauthorized access to a system by exploiting software vulnerabilities?

☐
Exploiting
☐
Hacking
☐
Cracking
☐
Phreaking
☐
None of the above

#11. Which encryption algorithm is commonly used for securing web traffic (e.g., HTTPS)?

☐
TLS/SSL
☐
DES
☐
AES
☐
MD5
☐
None of the above

#12. What is the term for the process of masking sensitive information to protect it from unauthorized access?

☐
Redaction
☐
Encryption
☐
Obfuscation
☐
Deletion
☐
None of the above

#13. Which of the following is a type of physical security control used to restrict access to a secure area based on biometric data?

☐
Biometric access control system
☐
Firewall

☐
Intrusion Detection System
☐
Virtual Private Network
☐
None of the above

#14. What is the purpose of network segmentation in cybersecurity?

☐
To isolate different parts of a network for added security
☐
To increase network speed
☐
To block all incoming traffic
☐
To monitor network traffic
☐
None of the above

#15. What is the term for a process that verifies the integrity of data by comparing it to a known value or checksum?

☐
Data validation
☐
Data encryption
☐
Data integrity check
☐
Data authentication
☐
None of the above

#16. Which of the following is a common method for protecting against SQL injection attacks?

☐
Input validation and parameterized queries
☐
Ignoring security best practices
☐
Using weak passwords
☐
Disabling firewalls
☐
None of the above

#17. What is the purpose of a security awareness training program for employees?

☐
To educate employees about cybersecurity best practices
☐
To encourage employees to share their passwords
☐
To block all external email communication
☐
To increase network bandwidth
☐
None of the above

#18. What is the term for a program that replicates itself and spreads to other computers or devices through removable media?

☐
Worm
☐
Virus

☐
Spyware
☐
Ransomware
☐
None of the above

#19. Which of the following is a recommended practice for securely disposing of paper documents containing sensitive information?

☐
Shredding or using a cross-cut shredder
☐
Throwing them in the regular trash
☐
Leaving them in a public place
☐
Storing them in a public area
☐
None of the above

#20. What is the term for a software program that monitors and filters incoming and outgoing network traffic based on an applied rule set?

☐
Firewall
☐
Antivirus
☐
Intrusion Detection System
☐
Encryption software
☐
None of the above

Next

Results