

#1. Which of the following is a method for securing a mobile device if it is lost or stolen?

☐

Remote wipe or lock

☐

Ignoring the loss

☐

Sharing the device location on social media

☐

Changing the device's wallpaper

☐

None of the above

#2. What is the term for a technique used to gain unauthorized access to a system by exploiting human psychology?

☐

Social Engineering

☐

Network Sniffing

☐

Port Scanning

☐

Packet Filtering

☐

None of the above

#3. Which encryption protocol is commonly used to secure email communication?

☐

S/MIME (Secure/Multipurpose Internet Mail Extensions)

☐

POP3 (Post Office Protocol version 3)

☐

IMAP (Internet Message Access Protocol)

☐

SMTP (Simple Mail Transfer Protocol)

☐

None of the above

#4. What is the purpose of a security policy in an organization?

☐

To establish guidelines and procedures for protecting information assets

☐

To increase network bandwidth

☐

To prioritize software development tasks

☐

To create marketing strategies

☐

None of the above

#5. Which of the following is an example of a strong authentication factor?

☐

Biometric data

☐

Username

☐

Email address

☐

Social security number

☐

None of the above

#6. What is the term for a program that self-replicates and spreads to other computers or devices over a network?

☐

Worm

☐

Virus

☐

Spyware

☐

Ransomware

☐

None of the above

#7. Which of the following is NOT a common method for protecting against phishing attacks?

☐

Verifying the sender's email address

☐

Clicking on suspicious links in emails

☐

Using email filtering software

☐

Being cautious of unsolicited emails

☐

None of the above

#8. What is the term for a security breach that occurs when an attacker gains unauthorized physical access to a computer or network equipment?

☐

Tailgating

☐

Shoulder surfing

☐

Social engineering

☐

Physical intrusion

☐

None of the above

#9. 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

#10. 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

#11. 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

#12. 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

#13. 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

#14. 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

#15. 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

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

☐

TLS/SSL

☐

DES

☐

AES

☐

MD5

☐

None of the above

#17. 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

#18. 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

#19. 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

#20. 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

Next



## Results

