#1. What does “Phishing” refer to in the context of cybersecurity?

- ☐ Unauthorized access to a computer system
- ☐ Sending deceptive emails or messages to trick recipients into revealing sensitive information
- ☐ Installing malicious software on a computer
- ☐ Encrypting files to prevent unauthorized access
- ☐ None of the above

#2. What is a firewall in the context of network security?

- ☐ A physical barrier that prevents unauthorized access to a network
- ☐ A software program that monitors and filters incoming and outgoing network traffic
- ☐ A tool used for hacking into computer systems
- ☐ A device used for wireless network connections
- ☐ None of the above

#3. What does VPN stand for in the context of network security?

- ☐ Virtual Private Network
- ☐ Very Private Network
- ☐

Virtual Personal Network

☐

Visual Private Network

☐

None of the above

#4. What is the purpose of encryption in cybersecurity?

☐

To protect sensitive data by converting it into a code that can only be deciphered with the right key

☐

To detect and prevent network intrusions

☐

To filter spam emails

☐

To physically secure computer hardware

☐

None of the above

#5. What is a common method to enhance password security?

☐

Using easily guessable passwords

☐

Sharing passwords with trusted colleagues

☐

Changing passwords regularly and using a combination of letters, numbers, and symbols

☐

Writing down passwords and keeping them near the computer

☐

None of the above

#6. What is a common type of malware that encrypts files and demands a ransom for their release?

☐
Ransomware
☐
Spyware
☐
Adware
☐
Worm
☐
Trojan Horse

#7. What is the term for a software vulnerability that allows attackers to gain unauthorized access to a system?

☐
Exploit
☐
Firewall
☐
Patch
☐
Intrusion
☐
Antivirus

#8. Which of the following is an example of a strong, secure password?

☐
P@ssw0rd
☐
Password123

☐
123456
☐
MyDog123
☐
CorrectHorseBatteryStaple

#9. What does a biometric authentication method rely on for identity verification?

☐
Unique physical or behavioral characteristics of an individual
☐
Knowledge of a shared secret
☐
Possession of a physical token
☐
Knowledge of a password or PIN
☐
None of the above

#10. What is the term for a fake website designed to mimic a legitimate one and trick users into entering their login credentials?

☐
Phishing site
☐
Spoofed site
☐
Clone site
☐
Imposter site
☐
None of the above

#11. Which of the following is NOT a recommended security practice for protecting personal information online?

☐
Sharing passwords with friends
☐
Using two-factor authentication
☐
Regularly updating software and applications
☐
Avoiding public Wi-Fi for sensitive transactions
☐
Using a virtual private network (VPN)

#12. What is a DDoS attack?

☐
Distributed Denial of Service attack
☐
Direct Denial of Service attack
☐
Determined Denial of Service attack
☐
Digital Denial of Service attack
☐
None of the above

#13. What is a keylogger?

☐
Malware that records keystrokes entered by a user
☐
A physical device used to open locked doors
☐
A software tool used for encryption

☐
A device for secure authentication
☐
None of the above

#14. Which protocol is used to secure email communication?

☐
SMTP
☐
SSL/TLS
☐
HTTP
☐
FTP
☐
None of the above

#15. What is the purpose of a security patch?

☐
To fix vulnerabilities in software and improve security
☐
To enhance the appearance of user interfaces
☐
To increase processing speed
☐
To optimize network performance
☐
None of the above

#16. What is the first line of defense against malware for a computer system?

☐
Antivirus software

☐
Firewall
☐
User awareness and cautious behavior
☐
Encryption
☐
None of the above

#17. What does the acronym CIA stand for in cybersecurity?

☐
Confidentiality, Integrity, Availability
☐
Cybersecurity, Information Security, Analysis
☐
Central Intelligence Agency
☐
Computer Intrusion Alert
☐
None of the above

#18. What is a vulnerability assessment?

☐
Process of identifying and evaluating security weaknesses in a system
☐
Process of encrypting sensitive data
☐
Process of blocking unauthorized access
☐
Process of monitoring network traffic
☐
None of the above

#19. Which type of attack involves intercepting communication between two parties without their knowledge?

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

#20. What is the purpose of a security token?

☐
To provide an additional layer of authentication
☐
To encrypt sensitive information
☐
To filter network traffic
☐
To block malicious websites
☐
None of the above

Next

Results