Cybersecurity Foundations

Cybersecurity · Answer Key · 25 Questions

1. What does the term 'multi-factor authentication' (MFA) require for a user to gain access?

A) Only a password
B) Two or more independent methods of verification
C) A secret security question only
D) A hardware key connected to a local server

2. Which of these describes a 'phishing' attack?

A) A physical theft of a computer
B) Fraudulent emails designed to trick users into revealing sensitive data
C) An attempt to overload a server with traffic
D) A program that encrypts files and demands payment

3. What is the primary purpose of a firewall?

A) To speed up internet connection
B) To monitor and control incoming and outgoing network traffic
C) To prevent physical damage to hardware
D) To remove viruses from a smartphone

4. What does 'encryption' do to data?

A) Deletes data to save space
B) Converts data into a coded format to prevent unauthorized access
C) Compresses data to make it transfer faster
D) Identifies the sender of an email

5. What is a 'strong' password policy according to NIST guidelines?

A) Using a child's nickname
B) Using a mix of upper and lowercase letters, numbers, and symbols
C) Using the same password for every account
D) Keeping the password under eight characters

6. Which of the following is considered a 'biometric' factor for authentication?

A) A security token
B) A fingerprint scan
C) A password manager
D) A hidden answer to a recovery question

7. What is a 'VPN' used for in network security?

A) Creating a private, encrypted tunnel for internet traffic
B) Increasing the physical speed of a network
C) Automatically blocking all pop-up advertisements
D) Removing malware from an operating system

8. What is the primary danger of connecting to an 'unsecured public Wi-Fi' network?

A) The signal strength is always weak
B) Hackers can potentially intercept data transmitted over the network
C) The network will automatically download viruses
D) It is illegal to use public Wi-Fi without a permit

9. What does 'malware' stand for?

A) Malicious hardware
B) Malicious software
C) Maladjustedware
D) Mainframeware

10. Which of these is a common characteristic of a 'ransomware' attack?

A) The user is forced to change their username
B) The computer files are encrypted and a fee is demanded for the key
C) The browser history is automatically deleted
D) The webcam is used to record the user without consent

11. What is the 'principle of least privilege' in cybersecurity?

A) Giving users the highest level of access possible
B) Granting users only the minimum access necessary to perform their job
C) Allowing everyone on a network to see all files
D) Restricting access based on the time of day

12. Which of the following is a symptom of a device being infected by a 'keylogger'?

A) The keyboard stops working entirely
B) Sensitive keystrokes are recorded and sent to an attacker
C) The screen resolution automatically changes
D) The battery drains faster than usual

13. What is 'social engineering' in the context of cyber threats?

A) Writing computer code for social media apps
B) Manipulating individuals into divulging confidential information
C) Creating profiles on social media sites
D) Analyzing user behavior for marketing purposes

14. What is the main purpose of an 'antivirus' program?

A) To back up data to the cloud
B) To detect, prevent, and remove malicious software
C) To increase the RAM of the computer
D) To manage email passwords

15. What does 'HTTPS' indicate when visiting a website?

A) The website is highly popular
B) The data sent between the browser and server is encrypted
C) The website is free of all advertisements
D) The website is hosted in a secure physical location

16. What is 'two-factor authentication' (2FA) most commonly used for?

A) Improving search engine rankings
B) Adding an extra layer of security to an account login
C) Increasing the speed of account recovery
D) Reducing the need for a password

17. Which of the following is an example of 'spyware'?

A) Software that monitors user activity without their knowledge
B) A game that tracks high scores
C) A browser extension that blocks ads
D) A tool that organizes files in folders

18. What is the function of a 'patch' in software security?

A) To add new features to the software
B) To fix security vulnerabilities or bugs in existing software
C) To delete old software from the system
D) To change the background color of an application

19. What is 'cloud security' primarily concerned with?

A) Protecting data stored in remote, internet-accessible servers
B) Monitoring the weather for data centers
C) Cleaning physical computer hardware
D) Fixing broken internet cables

20. What is a 'botnet'?

A) A network of robots in a factory
B) A collection of internet-connected devices infected with malware and controlled by a hacker
C) A secure messaging app for teenagers
D) A tool used to monitor network speed

21. What does 'DDoS' stand for?

A) Distributed Denial of Service
B) Data Destruction of System
C) Digital Delivery of Software
D) Dynamic Device Operating System

22. What is the main goal of 'pharming' attacks?

A) To steal computer hardware
B) To redirect users to a fake website that looks legitimate
C) To increase website traffic artificially
D) To update outdated software versions

23. Why should you keep your software updated?

A) To get new wallpapers
B) To patch security vulnerabilities that hackers could exploit
C) To clear hard drive space
D) To reduce the amount of electricity used

24. What is a 'worm' in terms of cybersecurity?

A) A type of hardware cable
B) A standalone malware program that replicates itself to spread to other computers
C) A software tool that sorts files
D) A programming language for security scripts

25. What is 'data breach'?

A) The accidental deletion of a folder
B) The unauthorized access and retrieval of sensitive data from a secure system
C) The act of upgrading a network speed
D) The legal distribution of public documents