

High School Cybersecurity Fundamentals

Cybersecurity · Answer Key · 23 Questions

1. Which of the following is a common type of malware designed to encrypt a victim's files and demand payment for their decryption?

- A) Adware
- B) Spyware
- C) Ransomware**
- D) Trojan horse

2. What is the primary purpose of a firewall in a network?

- A) To speed up internet connections
- B) To block unauthorized access and control network traffic**
- C) To encrypt all outgoing data
- D) To store personal files securely

3. What does the acronym 'Phishing' refer to in cybersecurity?

- A) A type of virus that replicates itself
- B) An attempt to obtain sensitive information by masquerading as a trustworthy entity**
- C) A method of securing wireless networks
- D) A technique for hiding data within other data

4. Which of these is an example of a strong password characteristic?

- A) Using common words found in a dictionary
- B) Using personal information like birthdates
- C) Combining uppercase and lowercase letters, numbers, and symbols**
- D) Making it short and easy to remember

5. What is two-factor authentication (2FA)?

- A) Using two different email addresses for login
- B) Requiring two separate identity verification steps to access an account**
- C) A type of encryption algorithm
- D) A password manager that uses two keys

6. In the context of cybersecurity, what is a 'vulnerability'?

- A) A piece of malicious code
- B) A weakness in a system that can be exploited**
- C) A secure network connection
- D) A type of antivirus software

7. Which protocol is commonly used to encrypt communications between a web browser and a web server, indicated by 'https' in the URL?

- A) HTTP
- B) FTP
- C) SSL/TLS**
- D) SMTP

8. What is the main objective of a Distributed Denial-of-Service (DDoS) attack?

- A) To steal credit card numbers
- B) To gain unauthorized access to a server
- C) To overwhelm a system with traffic, making it unavailable to legitimate users**
- D) To install malware on user devices

9. What is 'encryption' in cybersecurity?

- A) The process of deleting files permanently
- B) The process of converting data into a code to prevent unauthorized access**
- C) The process of creating backup copies of data
- D) The process of scanning for viruses

10. Which of the following is NOT a common social engineering tactic?

- A) Impersonation
- B) Baiting
- C) Pretexting
- D) Encryption**

11. What is the purpose of an antivirus program?

- A) To increase internet speed
- B) To detect, prevent, and remove malicious software**
- C) To manage passwords securely
- D) To back up files to the cloud

12. What does the acronym 'VPN' stand for in cybersecurity?

- A) Very Private Network
- B) Virtual Private Network**
- C) Verified Personal Network
- D) Vulnerable Protocol Neutralizer

13. What is a 'cookie' in the context of web browsing and cybersecurity?

- A) A type of malware
- B) A small piece of data stored on the user's computer by a web browser, often used for tracking user activity or remembering login information**
- C) A secure connection protocol
- D) A method for encrypting emails

14. Which of these is a strong defense against SQL injection attacks?

- A) Using weak passwords
- B) Not validating user input
- C) Using parameterized queries or prepared statements**
- D) Disabling all error messages

15. What is the purpose of a 'digital certificate'?

- A) To store personal photos
- B) To verify the identity of a website or individual and to enable secure communication**
- C) To accelerate internet browsing
- D) To create new email accounts

16. What is a 'zero-day exploit'?

- A) An exploit that has been known for a long time
- B) An exploit that targets a software vulnerability unknown to the software vendor, meaning there is no patch available**
- C) An exploit that requires user interaction to activate
- D) An exploit that is only effective on older operating systems

17. Which of the following is a privacy concern associated with social media platforms?

- A) High bandwidth usage
- B) Excessive advertising
- C) Collection and potential misuse of personal data**
- D) Slow loading times

18. What is 'malware'?

- A) A system for managing network devices
- B) Software designed to cause harm to a computer system or data**
- C) A method for securely storing passwords
- D) A tool for analyzing website traffic

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

- A) Granting users the highest possible level of access to all resources
- B) Granting users only the minimum necessary permissions to perform their tasks**
- C) Restricting all user access to a system
- D) Allowing anonymous access to sensitive data

20. Which type of attack involves exploiting weaknesses in older or unpatched software?

- A) Brute-force attack
- B) Man-in-the-middle attack
- C) Exploiting software vulnerabilities**
- D) Denial-of-service attack

21. What is the main function of a 'password manager'?

- A) To automatically log you into websites
- B) To generate and store strong, unique passwords for different online accounts**
- C) To encrypt your entire hard drive
- D) To scan for viruses

22. What is 'data anonymization'?

- A) The process of deleting data permanently
- B) The process of altering or removing personally identifiable information from data so that it cannot be linked back to an individual**
- C) The process of encrypting data for storage
- D) The process of transferring data between servers

23. What is the primary risk associated with clicking on unknown links or attachments in emails?

- A) Receiving unsolicited marketing emails
- B) Experiencing a sudden increase in internet speed
- C) Potentially downloading malware or falling victim to phishing attempts**
- D) Getting a free software upgrade