Cybersecurity Foundations for Teens

Cybersecurity · Answer Key · 10 Questions

1. What is the primary function of a firewall in a computer network?

A) To increase internet speed
B) To block unauthorized access while allowing authorized communications
C) To remove viruses from files
D) To encrypt all outgoing emails

2. Which of the following is an example of multi-factor authentication (MFA)?

A) Using a complex password only
B) Logging in with a username and a fingerprint scan
C) Sharing your password with a trusted friend
D) Saving your password in a web browser

3. What does HTTPS stand for in a website URL?

A) Hypertext Transfer Protocol Secure
B) Hyperlink Transmission Technology Standard
C) High-speed Transfer Protocol System
D) Hypertext Terminal Processing Service

4. Which type of malicious software is designed to encrypt a user's files and demand payment for the decryption key?

A) Spyware
B) Adware
C) Ransomware
D) Trojan Horse

5. What is the purpose of 'salting' in the context of password storage?

A) To make the password easier to remember
B) To add random data to passwords before hashing to prevent rainbow table attacks
C) To shorten the length of the password
D) To encrypt the internet connection

6. What is 'phishing' in the context of cybersecurity?

A) A technique to optimize website search rankings
B) Sending fraudulent communications that appear to come from a reputable source
C) The physical theft of a computer device
D) A method for backing up data to the cloud

7. Which encryption method uses two different keys: a public key for encryption and a private key for decryption?

A) Symmetric encryption
B) Asymmetric encryption
C) Block encryption
D) Stream encryption

8. What is the primary goal of a 'Denial-of-Service' (DoS) attack?

A) To steal user banking information
B) To corrupt the data on a personal hard drive
C) To make a network or server resource unavailable to its intended users
D) To gain administrative control over a private network

9. What is a 'zero-day' vulnerability?

A) A vulnerability that has been patched for zero days
B) A flaw that is known to software vendors but has no available patch yet
C) A vulnerability that only affects computers that are zero days old
D) A security flaw in open-source software

10. Which of the following is considered a best practice for password management?

A) Using the same password for all websites
B) Writing passwords on a sticky note near the monitor
C) Using a unique, complex password for every account managed by a password manager
D) Using your birth date as your password