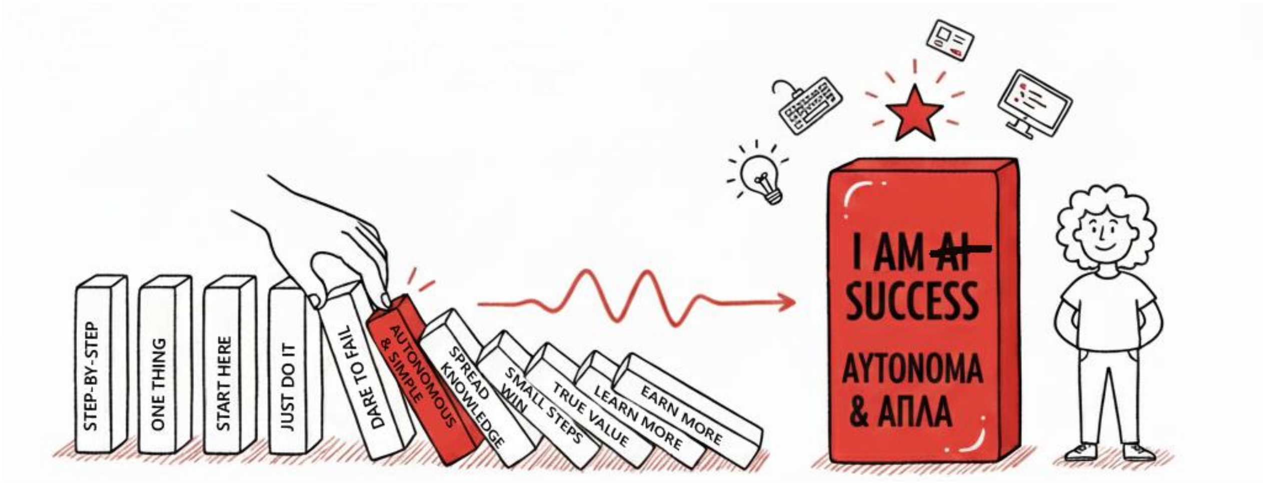
Cybersecurity & Digital Collaboration Quiz



Quiz Statistics:

Total Questions: 55

Section A (Questions 1-15): Cybersecurity Fundamentals - definitions, frameworks, professional roles
Section B (Questions 16-30): Common Cyber Threats - malware types, attack methods
Section C (Questions 31-42): Security Tools & Countermeasures - protective technologies
Section D (Questions 43-50): Security Best Practices - passwords, authentication, updates
Section E (Questions 51-55): Digital Collaboration - Teams, Slack, project management tools

Recommended Time: 60-75 minutes

Section A: Cybersecurity Fundamentals (Questions 1-15)

1. What is the primary definition of cybersecurity?

A) Installing antivirus software on computers
B) The practice of protecting systems, networks, and data from digital attacks, theft, and damage
C) Creating complex passwords for user accounts
D) Monitoring employee internet usage

2. Which of the following is NOT a scope of cybersecurity?

A) Information security
B) Network security
C) Application security
D) Marketing security

3. What is cybercrime?

A) Any crime involving a computer network

B) Any criminal action perpetrated primarily using a computer
C) Only hacking activities
D) Internet fraud exclusively

4. What is a white-hat hacker?

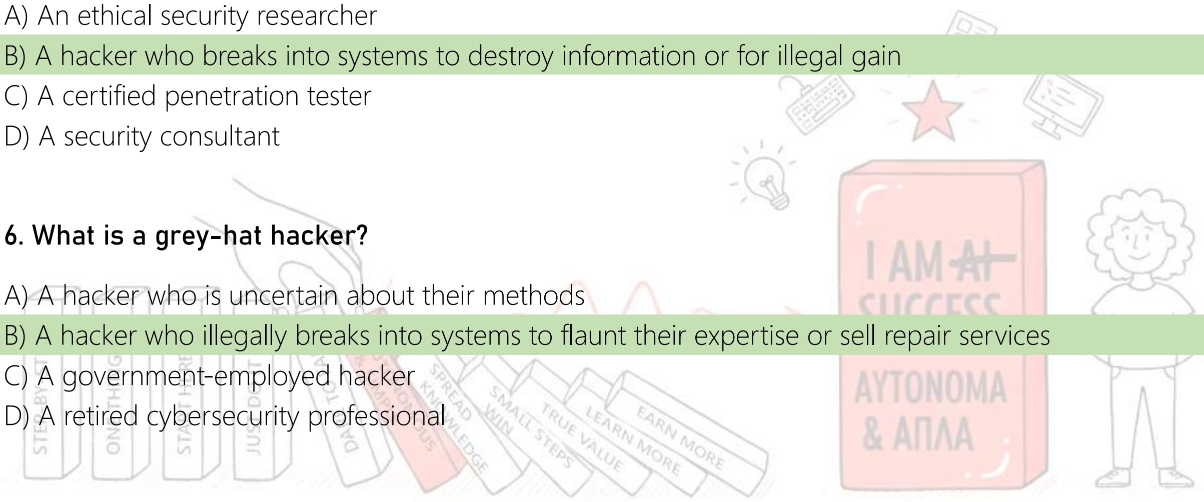
A) A hacker who wears white protective gear
B) An ethical hacker who breaks into systems for non-malicious reasons, such as testing security vulnerabilities
C) A beginner-level hacker
D) A hacker who only attacks government systems

5. What is a black-hat hacker?

A) An ethical security researcher
B) A hacker who breaks into systems to destroy information or for illegal gain
C) A certified penetration tester
D) A security consultant

6. What is a grey-hat hacker?

A) A hacker who is uncertain about their methods
B) A hacker who illegally breaks into systems to flaunt their expertise or sell repair services
C) A government-employed hacker
D) A retired cybersecurity professional



7. What is a packet analyzer (sniffer)?

A) A hardware device that filters network cables
B) A program that looks at each packet as it travels on the Internet
C) An antivirus scanning tool
D) A type of firewall

8. What is a keylogger?

A) A password management application
B) A program that captures all keystrokes made on a computer
C) A keyboard maintenance tool
D) A typing speed measurement software

9. According to Forbes Advisor statistics on cybersecurity, what trend is evident?

A) Cyber threats are decreasing globally

B) Cyber threats and attacks are increasing
C) Only small businesses are targeted
D) Cybersecurity is no longer a concern

10. Which framework is commonly used to guide cybersecurity best practices?

A) NIST
B) SWIFT
C) IBAN
D) GAAP

11. What does ISO/IEC 27001 provide?

A) Internet speed standards
B) Cybersecurity frameworks and standards
C) Hardware specifications
D) Software development guidelines

12. What role do cybersecurity professionals play?

A) Only installing antivirus software
B) Protecting information systems and responding to incidents
C) Managing social media accounts
D) Designing websites

13. Which emerging technology is increasingly important in cybersecurity?

A) Floppy disks
B) Artificial Intelligence and Machine Learning
C) Morse code
D) Telegraph systems

14. What is the growing importance of cybersecurity related to?

A) Entertainment industry only
B) Policy and regulation
C) Fashion trends
D) Sports management

15. What does OWASP stand for?

A) Online Web Application Security Platform
B) Open-Source Foundation for Application Security

C) Operational Web Access Security Protocol
D) Organized Worldwide Application Safety Program

Section B: Common Cyber Threats (Questions 16-30)

16. What is malware?

A) Faulty hardware components
B) Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems
C) A type of computer game
D) Legitimate software with minor bugs

17. Which of the following is a type of malware?

A) HTTPS
B) Ransomware
C) Firewall
D) VPN

18. What is a computer virus?

A) A standalone program that runs independently
B) A program that attaches itself to another program and spreads to other computers
C) A hardware malfunction
D) An operating system error

19. How do viruses typically spread?

A) Through air ventilation systems
B) By sharing disks, opening email attachments, or downloading infected files
C) Through power cables
D) Via telephone lines only

20. What is the main difference between a virus and a worm?

A) There is no difference
B) Worms are standalone malware that replicate themselves; viruses attach to legitimate programs
C) Viruses are always more dangerous
D) Worms only affect smartphones

21. What is a Trojan horse in cybersecurity?

A) A secure communication protocol

B) Malware that disguises itself as legitimate software but performs malicious activities when activated

C) A type of antivirus program

D) A network monitoring tool

22. What is phishing?

A) A legitimate email marketing technique

B) A cyber attack where attackers masquerade as trustworthy entities to steal sensitive information

C) A type of firewall configuration

D) A network scanning tool

23. What are common techniques used in phishing?

A) Sending birthday cards

B) Deceptive emails, fake websites, and phone calls

C) Television advertisements

D) Radio broadcasts

24. What is ransomware?

A) Software that speeds up computer performance

B) A type of malware that encrypts a victim's files and demands payment for the decryption key

C) A legitimate backup solution

D) A free data recovery tool

25. What is a Denial-of-Service (DoS) attack?

A) Refusing to provide customer service

B) Overwhelming systems with traffic to disrupt services

C) Shutting down a computer properly

D) Denying user access to legitimate websites

26. What is a Distributed Denial-of-Service (DDoS) attack?

A) A DoS attack from a single source

B) A DoS attack using multiple compromised systems to overwhelm the target

C) A legitimate stress test

D) A network optimization technique

27. What is a Man-in-the-Middle (MitM) attack?

A) An attack on the middle server in a network

B) An attack where attackers intercept and alter communication between two parties without their knowledge

C) A physical security breach

D) A social media hacking technique

28. What is SQL injection?

A) A database backup method

B) An exploit that uses malicious SQL statements to execute unauthorized database operations

C) A legitimate database query technique

D) A data encryption method

29. What is a zero-day exploit?

A) An attack that happens on day zero of a project

B) An attack that targets software vulnerabilities unknown to the software provider and not yet patched

C) An attack that takes zero days to execute

D) A failed attack attempt

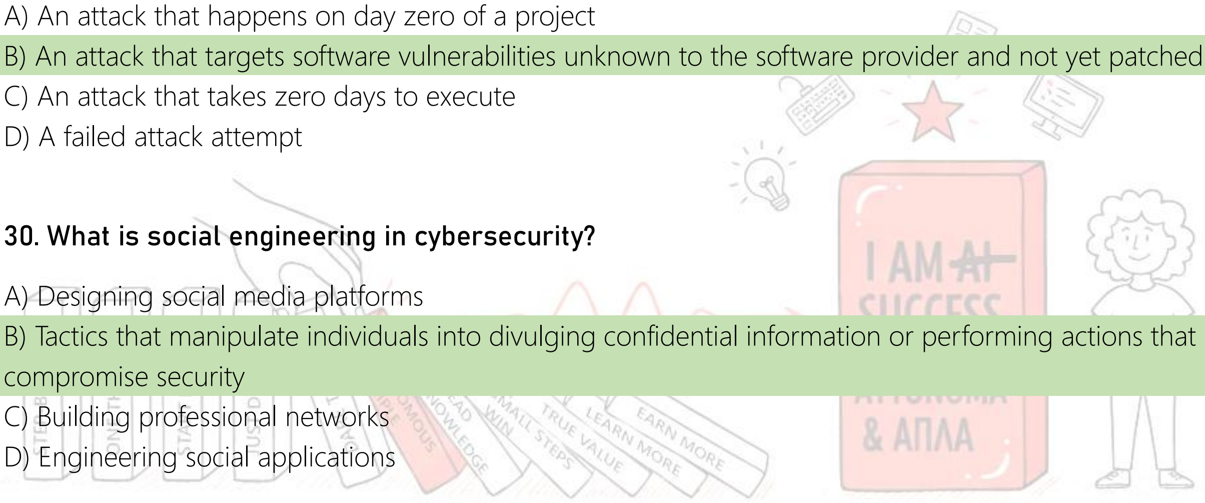
30. What is social engineering in cybersecurity?

A) Designing social media platforms

B) Tactics that manipulate individuals into divulging confidential information or performing actions that compromise security

C) Building professional networks

D) Engineering social applications



Section C: Security Tools & Countermeasures (Questions 31-42)

31. What is SPAM?

A) A type of malware

B) Unwanted or junk email

C) A legitimate marketing term

D) A network protocol

32. What is a spam filter?

A) A hardware device

B) An option in email that places known or suspected spam messages into a separate folder

C) A type of antivirus

D) A network firewall

33. What is SPIM?

A) Spam via instant messaging
B) Unsolicited instant messages
C) A type of virus
D) Both A and B are correct

34. What are cookies in the context of web browsing?

A) Viruses that infect computers
B) Small text files that websites store on your computer's hard drive
C) Antivirus programs
D) Network protocols

35. What is the primary purpose of cookies?

A) To delete user data
B) To assign an ID number to your computer and track browsing habits
C) To encrypt passwords
D) To scan for viruses

36. What is scareware?

A) Legitimate security software
B) Malware that attempts to convince you that something is wrong and to pay money to fix it
C) A type of firewall
D) An educational tool

37. What is a hoax in cybersecurity?

A) A legitimate security alert
B) An attempt to make someone believe something that is untrue
C) A type of encryption
D) A network configuration

38. What is a firewall?

A) A physical barrier around servers
B) Software or hardware designed to monitor and control network traffic to close logical ports to invaders
C) An antivirus program
D) A backup system

39. Where can software firewalls be found?

A) Only in third-party applications
B) Built into the operating system or available from vendors
C) Only in smartphones
D) Only in external hardware

40. What is biometric authentication?

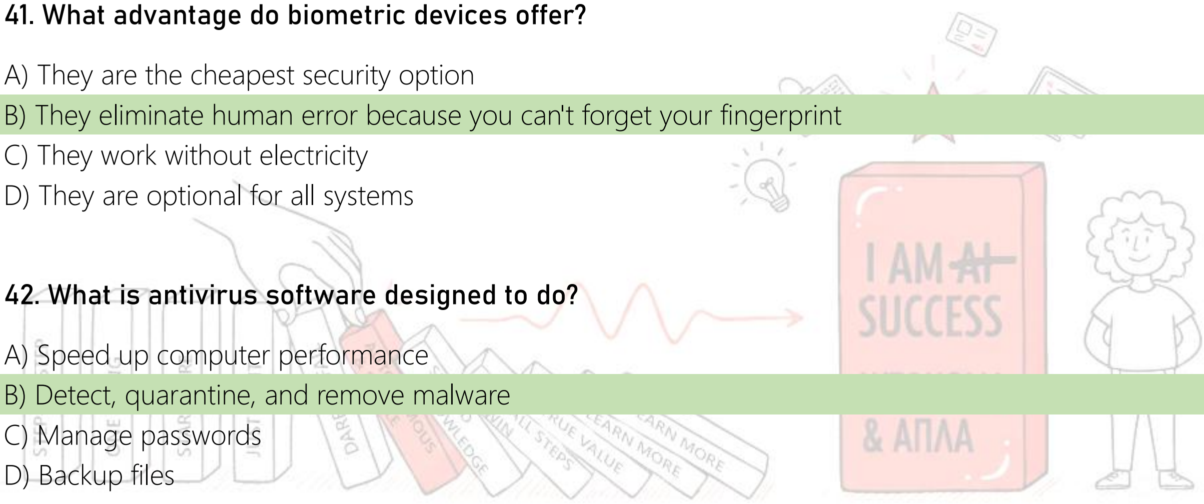
A) Using passwords and PINs
B) Devices that read unique personal characteristics like fingerprints or iris patterns
C) Two-factor authentication via SMS
D) Security questions

41. What advantage do biometric devices offer?

A) They are the cheapest security option
B) They eliminate human error because you can't forget your fingerprint
C) They work without electricity
D) They are optional for all systems

42. What is antivirus software designed to do?

A) Speed up computer performance
B) Detect, quarantine, and remove malware
C) Manage passwords
D) Backup files



Section D: Security Best Practices (Questions 43-50)

43. What is the recommended minimum character length for a strong password?

A) 6 characters
B) 8 characters
C) 10 characters
D) At least 14 characters

44. A strong password should include:

A) Only lowercase letters
B) At least 14 characters including numbers, symbols, and upper and lowercase letters
C) Your birthday
D) A single dictionary word

45. What should you avoid when creating passwords?

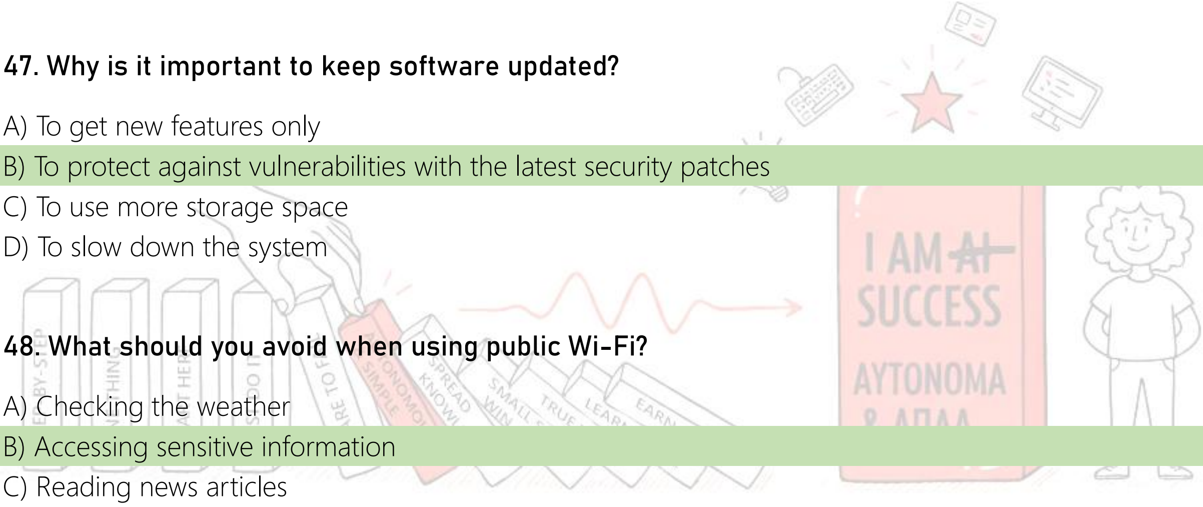
A) Using symbols
B) Using words from a dictionary or information easily associated with you
C) Using uppercase letters
D) Using numbers

46. What is Two-Factor Authentication (2FA)?

A) Using two different passwords
B) An extra layer of protection requiring a second form of verification in addition to the password
C) Two antivirus programs
D) Logging in twice

47. Why is it important to keep software updated?

A) To get new features only
B) To protect against vulnerabilities with the latest security patches
C) To use more storage space
D) To slow down the system



48. What should you avoid when using public Wi-Fi?

A) Checking the weather
B) Accessing sensitive information
C) Reading news articles
D) Watching videos

49. What is the purpose of regular data backups?

A) To use more storage space
B) To ensure data recovery in case of cyber incidents
C) To slow down the computer
D) To share files with others

50. How often should passwords be changed according to best practices?

A) Never
B) Every 5 years
C) Regularly (every month)
D) Only when compromised

Section E: Digital Collaboration Tools (Questions 51-55)

51. Microsoft Teams is best described as:

A) Only a video conferencing tool
B) A comprehensive collaboration platform that integrates chat, video conferencing, file sharing, and Office 365 applications
C) An email client
D) A standalone calendar application

52. What is the primary function of channels in Microsoft Teams?

A) To broadcast television
B) To organize workspaces into specific topics, projects, or departments
C) To encrypt messages
D) To store passwords

53. Slack is primarily known for:

A) Video editing
B) Facilitating team communication through channels, direct messages, and app integrations
C) Graphic design
D) Data analysis

54. What project management tool uses boards, lists, and cards?

A) Microsoft Word
B) Trello
C) Adobe Photoshop
D) Google Chrome

55. Jira is widely used for:

A) Email marketing
B) Agile project management and software development projects
C) Social media management
D) Video streaming