Cyber Security Quiz: 40 Questions and Answers

Free from Cyber Snowden · cybersnowden.com/cyber-security-quiz-questions-and-answers-pdf/

Name: _____ Score: _____ / 40

Use this free cyber security quiz to test yourself or your team. It has 40 multiple-choice and true/false questions grouped by topic, and every question comes with the correct answer and a short explanation. Run it as a self-check, a team training warm-up, or print the PDF version for a workshop.

How to use this quiz

- **Self-assessment:** cover the answers, note your choices, then score yourself at the end.
- **Team training:** pick one section per meeting and discuss the explanations together.
- **Onboarding:** give new starters the phishing and password sections in their first week.

Phishing and social engineering questions

1. You receive an email from "IT Support" asking you to confirm your password through a link. What should you do?

- A) Click the link and confirm it quickly
- B) Reply with your password so IT can check it
- C) Report the email using your organisation's phishing process and do not click
- D) Forward it to colleagues to warn them

2. TRUE or FALSE: Attachments should be treated with caution even when you know the sender.

3. Which of these URLs is the legitimate PayPal site?

- A) https://www.payapl.com
- B) http://www.paypay.com.home/
- C) https://www.pay.pal.com
- D) https://www.paypal.com/us/home

4. What is "spear phishing"?

- A) Phishing sent to millions of random addresses
- B) A targeted phishing attack tailored to a specific person or organisation
- C) Phishing by phone call
- D) A type of firewall

5. A caller says they are from your bank and asks for the one-time code just sent to your phone. What is this most likely to be?

- A) A routine security check
- B) A vishing attempt to bypass your multi-factor authentication
- C) A software update
- D) A data backup request

6. What does the "L" in the SLAM method stand for?

- A) Login
- B) Links
- C) Location
- D) Language

7. A pop-up says "You won a free phone! Click to claim." What should you do?

- A) Click and claim the prize
- B) Share it with friends

- C) Close the pop-up without clicking inside it

8. Which is a common sign of business email compromise (BEC)?

- A) An urgent request from a senior manager to change supplier bank details
- B) A newsletter you subscribed to
- C) A calendar invite from a colleague
- D) An automatic out-of-office reply

Password and authentication questions

9. Which of these would be the hardest password to crack?

- A) Summ3r2017
- B) t3chnologyRulz
- C) 12345678
- D) correct-river-lantern-gravel-42

10. TRUE or FALSE: Reusing the same strong password on several sites is safe.

11. What is the best way to manage many unique passwords?

- A) Write them on a sticky note
- B) Use a reputable password manager
- C) Use the same base word with different numbers
- D) Save them in an unprotected spreadsheet

12. What does multi-factor authentication (MFA) require?

- A) Two passwords
- B) Two or more different types of proof, such as something you know and something you have
- C) A longer username
- D) Logging in from two devices

13. Which MFA method is the most resistant to phishing?

- A) SMS codes
- B) Email codes
- C) Passkeys or FIDO2 hardware security keys
- D) Security questions

14. You get repeated MFA push notifications you did not request. What should you do?

- A) Approve one to make them stop
- B) Deny them and report it, then change your password
- C) Ignore them
- D) Turn off MFA

Malware and ransomware questions

15. What is ransomware?

- A) Software that speeds up your computer
- B) Malware that encrypts or steals data and demands payment
- C) A type of antivirus
- D) A backup tool

16. What is the best protection against data loss from a ransomware attack?

- A) Antivirus software alone
- B) Restricting internet access
- C) Regular, tested backups kept offline or immutable

17. What does the 3-2-1 backup rule recommend?

- A) 3 copies of data, on 2 different types of media, with 1 copy offsite
- B) 3 passwords, 2 devices, 1 account
- C) Backing up 3 times a day
- D) 3 antivirus tools on 2 computers

18. What is a Trojan?

- A) Malware disguised as legitimate software
- B) A hardware firewall
- C) A secure messaging app
- D) A password rule

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

- A) There is no difference
- B) A worm spreads by itself across networks; a virus needs a host file or user action
- C) Viruses only affect phones
- D) Worms only affect email

20. You find a USB stick in the car park labelled "Salaries". What should you do?

- A) Plug it in to find the owner
- B) Hand it to IT or security without plugging it in
- C) Take it home
- D) Plug it into a colleague's computer

Network and Wi-Fi security questions

21. What does a firewall do?

- A) Cools down servers
- B) Controls network traffic based on security rules
- C) Stores backups
- D) Encrypts all email

22. What does HTTPS (the padlock in the address bar) tell you?

- A) The website is definitely safe and trustworthy
- B) The connection between your browser and the site is encrypted
- C) The site has no malware
- D) The company is verified by your government

23. Which Wi-Fi security standard should a home or office router use today?

- A) WEP
- B) WPA
- C) WPA2 or, preferably, WPA3
- D) No password

24. TRUE or FALSE: Public Wi-Fi is risky because others on the network may be able to intercept or redirect your traffic.

25. What does a VPN mainly do?

- A) Makes you completely anonymous
- B) Encrypts traffic between your device and the VPN server
- C) Removes malware
- D) Blocks all phishing

26. What is a DDoS attack?

- A) Stealing passwords from a database

- B) Flooding a service with traffic from many sources so real users cannot reach it
- C) Encrypting files for ransom
- D) Guessing a Wi-Fi password

Data protection and privacy questions

27. What does the CIA triad stand for in cyber security?

- A) Central Intelligence Agency
- B) Confidentiality, Integrity, Availability
- C) Control, Identity, Access
- D) Cloud, Internet, Applications

28. What is the "principle of least privilege"?

- A) Give everyone admin rights to save time
- B) Give users only the access they need to do their job
- C) Only managers can use computers
- D) Remove all passwords

29. Which is the safest way to share a sensitive file with a colleague?

- A) A personal email account
- B) Your organisation's approved, access-controlled file-sharing tool
- C) A public link anyone can open
- D) A USB stick left on their desk

30. TRUE or FALSE: Deleting a file and emptying the recycle bin always makes the data unrecoverable.

31. What is encryption?

- A) Compressing a file
- B) Converting data into a form that only someone with the right key can read
- C) Deleting data
- D) Copying data to the cloud

Safe device and workplace habits

32. Why should you install software updates promptly?

- A) They only add new features
- B) Many updates fix security vulnerabilities attackers already exploit
- C) Updates slow your device down on purpose
- D) It is not important

33. You leave your desk for a coffee. What should you do with your computer?

- A) Leave it unlocked
- B) Lock the screen (for example Windows key + L)
- C) Turn off the monitor only
- D) Ask a colleague to watch it

34. What is "shoulder surfing"?

- A) Looking over someone's shoulder to steal information such as a PIN or password
- B) A type of malware
- C) Browsing on a phone
- D) A secure login method

35. Someone without a badge follows you through a secure door. What is this called?

- A) Tailgating

- B) Phishing
- C) Spoofing
- D) Patching

36. TRUE or FALSE: It is fine to install any browser extension that looks useful on a work device.

Incident response questions

37. You clicked a link in a suspicious email and entered your password. What should you do first?

- A) Do nothing and hope for the best
- B) Report it to IT or security immediately and change the password
- C) Delete the email so nobody knows
- D) Wait to see if anything happens

38. Your screen shows a message that your files are encrypted and demands payment. What should you do?

- A) Pay immediately
- B) Disconnect from the network and report it to IT or security at once
- C) Restart repeatedly
- D) Email the attackers

39. What is a "zero-day" vulnerability?

- A) A bug fixed on the first day of release
- B) A flaw attackers can exploit before the vendor has released a fix
- C) A virus that deletes itself
- D) A password that expires today

40. Why do organisations run regular security awareness quizzes and phishing simulations?

- A) To punish staff
- B) To measure knowledge, find gaps and build safe habits over time
- C) Because the law requires daily quizzes
- D) To replace technical security controls

Answer key

1. C. Legitimate IT teams never ask for your password by email. Reporting it lets the security team block the message for everyone; forwarding spreads the malicious link.

2. TRUE. A known sender's account can be compromised or spoofed, so unexpected attachments deserve the same caution as unknown ones.

3. D. Read the domain right before the first single slash. Misspellings (payapl), extra dots (pay.pal) and odd endings (.com.home) are classic look-alike tricks.

4. B. Spear phishing uses personal details (name, role, colleagues) to look credible. Phishing by phone is called vishing.

5. B. One-time codes are for you alone. Anyone asking you to read one out is trying to log in as you.

6. B. SLAM stands for Sender, Links, Attachments and Message. Hover over links to check where they really go before clicking. Read more in our guide to the SLAM method.

7. C. Prize pop-ups are a common route to phishing pages and malware. Close the tab or window rather than clicking buttons inside the pop-up.

8. A. BEC relies on urgency and authority to push payments. Always verify bank-detail changes by calling a known number, not one in the email.

9. D. Length matters most. A long passphrase of random words is far harder to crack than short passwords with predictable substitutions like 3 for e.

10. FALSE. If one site is breached, attackers try the same email and password on other sites (credential stuffing). Use a unique password for every account.

11. B. A password manager generates and stores long unique passwords, so you only need to remember one strong master passphrase.

12. B. MFA combines factors such as a password, a phone or hardware key, or a fingerprint, so a stolen password alone is not enough.

13. C. Passkeys and FIDO2 keys are bound to the real website, so a fake login page cannot capture and reuse them. See what a passkey is.

14. B. Unexpected prompts mean someone already has your password and is trying "MFA fatigue". Deny, report and reset the password.

15. B. Modern ransomware groups often steal data before encrypting it, then threaten to leak it ("double extortion").

16. C. Backups that attackers cannot reach or change let you restore without paying. Test restores regularly; an untested backup may fail when you need it.

17. A. Multiple copies on different media, with one kept offsite or offline, protect against hardware failure, ransomware and disasters.

18. A. Like the wooden horse, a Trojan hides malicious code inside something the user wants to install.

19. B. Worms self-propagate, which is why they can spread very fast. Learn more about worms in cyber security.

20. B. Dropped USB drives are a classic baiting attack designed to make curious people run malware.

21. B. Firewalls allow or block traffic between networks according to rules, reducing what attackers can reach.

22. B. HTTPS protects data in transit, but phishing sites can use HTTPS too. Always check the domain name as well.

23. C. WEP and the original WPA are broken. Use WPA3 where your devices support it, otherwise WPA2 with a strong passphrase. See how to secure a home Wi-Fi router.

24. TRUE. On open networks, use HTTPS sites, avoid sensitive tasks, or use a trusted VPN.

25. B. A VPN protects traffic on untrusted networks, but it does not stop phishing or malware and the VPN provider can still see your traffic.

26. B. Distributed denial-of-service attacks use many machines, often a botnet, to overwhelm a target.

27. B. These three goals underpin most security decisions. Read our guide to the CIA triad.

28. B. Limiting access reduces the damage if an account is compromised.

29. B. Approved tools apply access controls, logging and encryption that personal accounts and public links do not.

30. FALSE. Data can often be recovered with forensic tools. Use secure wiping or full-disk encryption before disposing of devices.

31. B. Encryption protects data at rest and in transit. See symmetric vs asymmetric encryption.

32. B. Unpatched software is one of the most common ways attackers get in, especially for known and zero-day vulnerabilities.

33. B. An unlocked screen gives anyone nearby access to your accounts and data.

34. A. Be aware of your surroundings when typing passwords in public places.

35. A. Tailgating (or piggybacking) is a physical social-engineering technique. Politely ask unknown people to badge in or contact reception.

36. FALSE. Extensions can read the pages you visit. Only install approved extensions from trusted publishers.

37. B. Fast reporting lets the security team reset sessions and contain damage. Hiding mistakes makes incidents far worse.

38. B. Disconnecting limits spread. Leave decisions about recovery and payment to the incident response team.

39. B. Defenders have had "zero days" to patch, which is why layered defences and monitoring matter.

40. B. Training works best as a regular habit alongside technical controls, not instead of them.

Scoring: 36–40 excellent · 28–35 solid · 20–27 refresher recommended · under 20 start with the basics.