Cybersecurity Basics Quiz

Quiz · Test Your Foundational Cybersecurity Knowledge.

10 questions covering passwords, MFA, phishing, encryption, and common attack patterns. Find out where your knowledge is solid — and where the gaps are.

Instructions

10 multiple-choice questions. Pick the BEST answer for each. Don't peek at the answer key on the next page. Score yourself at the end. There's no time limit, but most people finish in 5-7 minutes.

Questions

Q1. What does MFA (Multi-Factor Authentication) require?

- **A.** Just a strong password
- **B.** A password plus a second factor like a code or hardware key
- **C.** Three different passwords
- **D.** A fingerprint instead of a password

Q2. What's the SAFEST way to store passwords for many accounts?

- **A.** A spreadsheet on your desktop
- **B.** Sticky notes on your monitor
- **C.** A reputable password manager
- **D.** Browser autofill alone with no master password

Q3. Which of these is the strongest password?

- **A.** P@ssw0rd!
- **B.** Summer2024
- **C.** qD7%kRm9!vZpL2eN (16 random characters)
- **D.** MyDog'sName1990

Q4. The 'lock' icon in your browser tells you that:

- **A.** The website is legitimate and safe
- **B.** Your traffic to the site is encrypted (HTTPS)
- **C.** The site has been verified by Google
- **D.** Nobody can see your activity on the site

Q5. Which of these emails is most likely a phishing attempt?

- **A.** Your bank, addressed to you by name, asking you to call the number on your card
- **B.** A 'final notice' from 'IRS-Tax-Refund@gmail.com' with a link to claim your refund
- **C.** Your password manager telling you a password was found in a breach
- **D.** A receipt from a store you bought from yesterday

Q6. What's the best second factor for high-value accounts?

- **A.** SMS / text message codes
- **B.** Authenticator app or hardware security key
- **C.** Security questions like your mother's maiden name
- **D.** An email-based code

Q7. What does it mean to 'freeze your credit'?

- **A.** Cancelling all your credit cards
- **B.** Blocking new credit accounts from being opened in your name
- **C.** Stopping your credit score from changing
- **D.** Locking your bank account

Q8. Why is updating your operating system important?

- **A.** To get cool new features
- **B.** Updates often patch security vulnerabilities that attackers can exploit
- **C.** Updates are required by your ISP
- **D.** Older OS versions cost more in electricity

Q9. If a stranger calls claiming to be from 'Microsoft Tech Support' about a virus on your computer, you should:

- **A.** Give them remote access so they can fix it
- **B.** Pay them to remove the virus
- **C.** Hang up — Microsoft does not call users about viruses
- **D.** Email them your account credentials

Q10. The MOST common cause of account compromise is:

- **A.** Brilliant hackers using cutting-edge zero-days
- **B.** Reused passwords leaked from past data breaches
- **C.** Government surveillance
- **D.** Public Wi-Fi sniffing

Answer Key

Don't peek before completing the quiz. Read explanations even for answers you got right — they reinforce the why.

Q1: B — MFA combines something you know (password) with something you have (phone, key) or are (biometric).

Q2: C — Password managers generate, store, and auto-fill strong unique passwords. Encrypted with your master password.

Q3: C — Length and randomness matter most. 'P@ssw0rd!' and 'MyDog'sName1990' are in every cracker's wordlist.

Q4: B — HTTPS encrypts traffic between you and the site. It does NOT mean the site is legitimate — phishing sites use HTTPS too.

Q5: B — Real IRS / banks don't email from gmail.com. Generic 'final notice' urgency + suspicious sender domain = phishing.

Q6: B — SMS is vulnerable to SIM swap. Authenticator apps (Authy, 2FAS) and hardware keys (YubiKey) are far stronger.

Q7: B — A credit freeze blocks new credit lines. Existing accounts work normally. Free at all 3 bureaus.

Q8: B — Most successful attacks exploit known, patched vulnerabilities. Updating closes those holes.

Q9: C — Microsoft never proactively calls users. Tech-support scams generate billions of dollars yearly. Hang up.

Q10: B — Credential stuffing attacks reuse leaked passwords across sites. Unique passwords + MFA stop this entirely.

Scoring

Score	Level	What it means
0–4	Beginner	You're at the start of your cybersecurity journey — perfect place to be. Start with the Beginner's Guide to C
5–7	Intermediate	You know the basics. Run the 30-Day Cybersecurity Sprint to fill the gaps and build the habits.
8–10	Advanced	You've got strong foundational knowledge. Move on to topic-specific guides (privacy, scams, family) for adv