Password Safety Quiz

Quiz · Test Your Password And MFA Knowledge.

10 questions on password creation, storage, MFA, and the 'gotchas' that make people vulnerable. Score yourself honestly — most people overestimate their password hygiene.

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. How many unique passwords should the average adult have across their accounts?

- **A.** 1 main password reused everywhere
- **B.** 5 passwords rotated across accounts
- **C.** One unique password per account (could be 80-200+ total)
- **D.** Just memorise a few; the rest can match

Q2. Which of these passwords is the LEAST secure?

- **A.** A 16-character random string from a password manager
- **B.** Four random words separated by symbols
- **C.** Your dog's name + your birth year + an exclamation point
- **D.** A 20-character passphrase you invented

Q3. Where should you store the master password for your password manager?

- **A.** In a text file on your desktop
- **B.** In your email Drafts folder
- **C.** On paper in a safe place (fire safe, locked drawer) and memorised
- **D.** Tattooed on your forearm

Q4. If a service you use is breached, you should:

- **A.** Change that password immediately, plus any others where you reused it
- **B.** Wait for the company to email you with instructions
- **C.** Only worry if the breach made news
- **D.** Cancel your account and never use the service again

Q5. Why is reusing passwords dangerous?

- **A.** It makes your password easier to memorise
- **B.** When one site is breached, attackers try the leaked credentials on hundreds of other sites
- **C.** Browsers auto-detect reuse and lock your accounts
- **D.** Reused passwords are technically illegal

Q6. MFA via SMS is:

A. The strongest form of MFA available
B. Better than no MFA, but vulnerable to SIM-swap attacks
C. Always required by banks regardless of preference
D. Faster than authenticator apps so always preferred

Q7. When a password manager flags a password as 'reused,' you should:

A. Ignore the alert — manager are paranoid
B. Change that password to a new unique one generated by the manager
C. Cancel your subscription to the manager
D. Switch to using the same password everywhere intentionally

Q8. Recovery codes for MFA should be:

A. Saved only in your phone's contacts app
B. Memorised and never written down
C. Stored in your password manager Secure Notes AND printed and kept in a safe place
D. Posted on your refrigerator for convenience

Q9. How often should you rotate strong, unique passwords on your accounts?

A. Every 30 days regardless
B. Only when there's a reason — breach, suspicion, role change
C. Every 90 days mandatory rotation
D. Once and never again

Q10. If a coworker asks you to share your password to test something, you should:

A. Share it via email — quickest
B. Share it via text — most convenient
C. Refuse — passwords should never be shared via insecure channels. Use the password manager's secure-share feature or set them up with their own access
D. Share it but ask them to delete the message after

Answer Key

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

Q1: C — Each account needs a unique password. The right number is 'one per account.' That's why you need a password manager.

Q2: C — Passwords with personal info (names, dates) are in every cracker's wordlist. Length + randomness wins.

Q3: C — Memorise it AND have a backup on paper somewhere safe. Never digital where it might be exposed.

Q4: A — Speed matters. The leaked password may be tried on other sites within hours.

Q5: B — Credential stuffing — automated attacks using leaked passwords across many sites. Unique passwords stop this.

Q6: B — SMS is better than nothing but defeated by SIM swaps. Authenticator apps and hardware keys are stronger.

Q7: B — The manager flagged it because it's a real risk. Update it to something unique and random.

Q8: C — Recovery codes are critical and rare-need. Store them encrypted (PM Secure Notes) AND on paper.

Q9: B — Modern guidance: don't rotate arbitrarily. Strong, unique passwords with MFA don't need scheduled rotation.

Q10: C — Sharing passwords via insecure channels is a top breach vector. Use proper sharing tools.

Scoring

Score	Level	What it means
0–4	Beginner	Your password habits are creating risk. Set up a password manager TODAY and read the Beginner's Guid
5–7	Intermediate	Solid foundation. Run the Password Security Checklist to lock down the remaining gaps.
8–10	Advanced	Excellent password hygiene. Help your family run this same quiz to bring them up.