

# CYBERSECURITY QUIZ

Simple Questions for Everyday Online Safety

## Start here

Circle A, B, C, or D. There are no trick questions. If you are not sure, pick the safest option. This is for learning, not judging. Getting one wrong means you found something worth practicing.

## How to use this

- Circle one answer for each question: A, B, C, or D.
- Do not overthink it. If a message feels urgent or pushes you to click, slow down.
- After you finish, we will review the answers together and talk about why the safest choices are safe.

Name: \_\_\_\_\_

Date: \_\_\_\_\_

Score: \_\_\_\_\_ / 21

## Reminder

The safest answer is usually the one that slows things down, verifies information through a trusted method, and avoids giving away passwords, codes, money, or access.

## Passwords and Logins

**1. You use the same password on three websites. One website gets hacked. What is the biggest risk?**

- A. Only that one website is affected
- B. Attackers try that same email and password on your other accounts
- C. Your phone gets infected
- D. Nothing happens if the password is long

**2. Which password is the safest choice for one account?**

- A. Password123!
- B. MyDogBingo2026
- C. A long, random password you do not reuse anywhere else
- D. Your street name plus your birthday

**3. What is the best reason to use a password manager?**

- A. It makes your phone faster
- B. It lets you reuse one password everywhere
- C. It helps you use a different strong password for every account
- D. It blocks spam calls

**4. A website asks you to set up security questions, like your mother's maiden name. What is safer?**

- A. Always use real answers
- B. Use fake answers and store them in your password manager
- C. Use your Social Security number
- D. Use the same answer for every account

## Two-Factor Authentication

**5. Two-factor authentication means:**

- A. Two passwords
- B. A password plus a second step to prove it is you
- C. Strong Wi-Fi
- D. Two email addresses

**6. Which two-factor option is usually stronger for most people?**

- A. Text message code
- B. Authenticator app code
- C. Security questions
- D. A four-digit PIN

**7. You receive a two-factor code you did not request. What does that usually mean?**

- A. A friend is testing your account
- B. Nothing important
- C. Someone may be trying to log in
- D. Your phone is broken

## Email as the Master Key

**8. Why is your email account often called the master key?**

- A. It is the oldest account you have
- B. Most accounts can be reset through your email
- C. Email is private by default
- D. Email cannot be hacked

**9. What is the best first step to secure your email account?**

- A. Share your password somewhere safe
- B. Use a strong, unique password and turn on two-factor authentication
- C. Unsubscribe from newsletters
- D. Use public Wi-Fi only

## Scams and Phishing

**10. You get a text saying your bank account is locked. It includes a link. What should you do first?**

- A. Click the link quickly
- B. Reply to the text and ask if it is real
- C. Open your bank app or call the number on the back of your card
- D. Forward it to friends

**11. A caller says they are from your bank and asks for your two-factor code. What is safest?**

- A. Give it to them
- B. Hang up and call the number on the back of your card
- C. Text it instead
- D. Ask them questions until they sound real

**12. Which is the biggest red flag in a message?**

- A. It uses your name
- B. It pressures you to act immediately
- C. It arrives during business hours
- D. It has good grammar

**13. A scammer calls and says they are from tech support. They want remote access to your computer. What should you do?**

- A. Let them in because they sound professional
- B. Give them access only if they know your name
- C. Hang up and contact the company directly using an official number
- D. Ask them to call back later

**14. You see a QR code on a flyer, table, or poster. What should you remember?**

- A. Every QR code is safe
- B. QR codes can send you to fake websites
- C. QR codes only work if they are printed in color
- D. QR codes are safer than links because they look fancy

## Updates and Devices

**15. Why do updates matter?**

- A. They only add new features
- B. They can fix security holes that attackers use
- C. They delete photos
- D. They only slow down devices

**16. Which devices should get security updates?**

- A. Only phones
- B. Only computers
- C. Anything connected to the internet
- D. Only brand-new devices

## Public Wi-Fi

**17. Public Wi-Fi should be treated as:**

- A. Safe and trusted
- B. Untrusted, so use it carefully
- C. Automatically secure
- D. Safer than your phone hotspot

**18. You need to check your bank account while you are out. What is usually safer?**

- A. Public Wi-Fi
- B. Your phone's cellular data or personal hotspot
- C. A shared public computer
- D. Turning off security settings

## Backups and Home Wi-Fi

**19. What is the main reason to back up your files?**

- A. To make devices faster
- B. To avoid losing important data
- C. To stop spam
- D. To save battery

**20. What should you change first on a new router?**

- A. The color
- B. The admin password and Wi-Fi password, and then check for updates
- C. The brand name
- D. Nothing

### Final Reminder Question

**Bonus Question: You receive a message that makes you feel rushed, scared, or pressured to act now. What is the safest first move?**

- A. Act quickly
- B. Pause, verify using a trusted method, then decide
- C. Reply with personal details
- D. Click the link to see what happens