Do You Respect Online Security Rules?

Test your digital street smarts!

---

1. A surprise email says you've won a prize and asks you to click a link. What's your move?

A. Click the link — who says no to free stuff?
B. Hover over the link to check the URL before deciding.
C. Delete the email — sounds like a phishing scam.
D. Forward it to friends to see what they think.

---

2. True or False:

It's safe to reuse the same strong password across multiple accounts.

---

3. Which password is the most secure option?

A. password123
B. John2024
C. il0vePizza!
D. q$T7g!z9Lw#

---

4. When should you update your antivirus software?

A. Once a year
B. Only when your device starts acting weird
C. As soon as a new update is available
D. Antivirus? That's old-school.

---

5. True or False:

It's safe to access your bank account while connected to public Wi-Fi.

---

6. What does two-factor authentication (2FA) do?

A. Lets you log in from two devices at once
B. Provides a backup password in case you forget
C. Adds a second step (like a code or fingerprint) to verify your identity
D. Upgrades your firewall settings

---

7. You get a friend request from someone you don't recognize, but you share mutual contacts. What do you do?

A. Accept it — they probably know you somehow.
B. Send them a message asking who they are.
C. Investigate their profile for anything suspicious.
D. B or C

---

8. How should you handle security questions (like "What's your first pet's name")?

A. Answer truthfully for easy recall
B. Use the same answers everywhere for consistency
C. Treat them like passwords — use fake but trackable answers
D. Skip them if possible

---

9. True or False:

If software is free and seems helpful, it's okay to download it from any site.

---

10. You suspect someone has hacked your account. What's the best first step?

A. Wait and see if anything suspicious happens
B. Change your password right away and enable 2FA
C. Delete the account just to be safe
D. Post about it on social media asking for advice

🛑 Scenario 1: The Mystery Message

Emma gets a message on Instagram from someone claiming to be a popular brand ambassador. They offer her a chance to win free clothes if she fills out a form with her name, email, and password.

Question:
What should Emma do, and how can she protect herself from potential scams like this?

📶 Scenario 2: The Risky Wi-Fi

James is at a coffee shop and decides to use the free public Wi-Fi to check his bank account and do some online shopping.

Question:
Why is this risky, and what could James do to stay secure when using public Wi-Fi?

🔐 Scenario 3: The Shared Password

Lily shares her Netflix password with a few of her classmates. A few weeks later, she notices someone has changed her password and she can't access her account anymore.

Question:
What did Lily do wrong, and how could she better manage her accounts and passwords?

📲 Scenario 4: The Fake App

Carlos downloads a free photo editing app from a website he found on a random forum. Later, his phone starts acting weird, and he notices unauthorized charges on his account.

Question:
What might have gone wrong, and what should Carlos do now? How can he avoid this in the future?

💬 Scenario 5: The Overshare

Sophie posts a TikTok video showing her new student ID card, which includes her full name and student number. She also tags her school.

Question:
What are the potential risks of posting personal information like this online? What should Sophie be more careful about?