Phishing Awareness Quiz

Quiz · Can You Spot The Scam? 10 Real-World Email And Text Scenarios.

Test your phishing-detection instincts against scenarios pulled from actual scam campaigns. By the end you'll know exactly which red flags your eye is trained to catch — and which it misses.

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. An email from 'support@arnazon.com' (note the 'rn' instead of 'm') with a link to verify your account is:

- **A.** Probably legitimate — Amazon has many domains
- **B.** A phishing attempt using a typosquatted domain
- **C.** Safe if the lock icon is in the browser
- **D.** Only suspicious if it asks for your password

Q2. A text claiming 'You owe $4.50 in tolls. Pay here: bit.ly/usToll' is most likely:

- **A.** A real toll authority — they all use SMS now
- **B.** A phishing scam (smishing) — toll authorities rarely send unsolicited SMS
- **C.** Legitimate if you've driven on toll roads recently
- **D.** Safe to click since the amount is small

Q3. Which of these is a phishing red flag?

- **A.** Generic greeting like 'Dear customer' from a service that knows your name
- **B.** An email signed with the sender's full name and title
- **C.** A confirmation receipt for a purchase you actually made
- **D.** An email forwarded from a coworker to a group list

Q4. If you hover over a link and the URL displayed in the corner of your browser doesn't match the link text, you should:

- **A.** Click it anyway if the email looks professional
- **B.** Trust it if the displayed URL is short
- **C.** Treat it as suspicious — mismatched URLs are a phishing hallmark
- **D.** Right-click and copy the link to test elsewhere

Q5. Your boss emails asking you to urgently buy gift cards for a client. The email is from 'ceo@gmail.com' instead of the company domain. You should:

- **A.** Buy them immediately — the boss is urgent

B. Reply asking for clarification
C. Verify out-of-band by calling or messaging your boss directly
D. Forward the email to other employees for help

Q6. The 'lock' icon (HTTPS) in your browser means:

A. The website is verified safe and trustworthy
B. Your traffic is encrypted between you and the site (legitimacy not implied)
C. Phishing sites cannot use HTTPS
D. Your password is automatically protected on this site

Q7. Which of these is the safest way to verify a suspicious 'bank fraud alert' email or text?

A. Click the link in the message — they need fast verification
B. Reply to the email asking for more details
C. Open your bank's app or website directly, or call the number on the back of your card
D. Forward the message to friends to ask their opinion

Q8. Spear phishing differs from regular phishing in that:

A. It uses sharp images to grab attention
B. It's targeted at a specific person or organisation, often with personal details
C. It only happens via SMS
D. It's always more obvious and easier to spot

Q9. If you accidentally clicked a phishing link and entered your password, the FIRST thing you should do is:

A. Wait and see if anything bad happens
B. Change that password immediately, from a clean device, and enable MFA
C. Email the company that was impersonated
D. Reset your computer to factory settings

Q10. Which of these is NOT a typical phishing technique?

A. Manufactured urgency ('act now')
B. Fake authority impersonation
C. A friendly check-in from a known coworker about today's lunch plans
D. Threats of legal action or account closure

Answer Key

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

Q1: B — Typosquatted domains (rn looks like m) are classic phishing. Always read domain names carefully.

Q2: B — Toll-fee SMS scams are widespread. Real toll authorities send paper invoices. URL shorteners hide the actual destination.

Q3: A — Real services that know you use your name. Generic greetings + urgent action requests = phishing red flag.

Q4: C — Mismatched URLs are one of the strongest phishing signals. The displayed text and the actual destination should match.

Q5: C — Gift-card-from-boss is a top SMB scam. Always verify urgent money requests via a different channel (in person, phone, separate chat).

Q6: B — HTTPS = encryption only. Phishing sites use it. The lock means your traffic is private; it doesn't mean the site is legitimate.

Q7: C — Verify out-of-band, always. Use a known-good channel (app you've used before, number on your card).

Q8: B — Spear phishing uses personal details (name, role, recent events) to seem more legitimate. Often harder to spot than mass phishing.

Q9: B — Speed matters. Change the password before the attacker uses it. From a clean device, in case the original device was also compromised.

Q10: C — Phishing exploits urgency, fear, authority, threats, and curiosity. Friendly normal communication is — well, friendly normal communication.

Scoring

Score	Level	What it means
0–4	Beginner	Phishing is the #1 cause of account takeovers — and you're vulnerable. Read the Phishing Beginner's Gui
5–7	Intermediate	You catch most phishing but might miss sophisticated attempts. Run the Scam Survival Field Guide for upg
8–10	Advanced	You're a hard target. Help your less-savvy family members run this same quiz to spread the awareness.