Safe Browsing Quiz

Quiz · Test The In-Browser Decisions That Stop Most Infections.

Most browser-borne attacks are stopped by 30 seconds of awareness. Test whether your instincts are sharp on URLs, downloads, warnings, public Wi-Fi, and extensions.

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. Hovering over a link in an email shows a URL that doesn't match the displayed link text. You should:

- **A.** Click anyway — the displayed text is what matters
- **B.** Treat it as suspicious — mismatched URLs are a phishing hallmark
- **C.** Open the link in incognito mode
- **D.** Right-click and copy to test

Q2. What does the lock icon next to a URL guarantee?

- **A.** The site is verified safe
- **B.** Your traffic to the site is encrypted (HTTPS) — but the site could still be a scam
- **C.** The site can be trusted with your password
- **D.** The site is approved by your government

Q3. A pop-up tells you 'Your computer is infected — call this number now!' The right response is:

- **A.** Call the number — they want to help
- **B.** Close the browser, restart, run your own antivirus, and ignore the number
- **C.** Allow remote access if they call back
- **D.** Pay the requested fee to remove the virus

Q4. Which of these URLs is a typosquat?

- **A.** amazon.com
- **B.** arnazon.com
- **C.** amazon.co.uk
- **D.** music.amazon.com

Q5. Should you install browser extensions from outside the official extension stores?

- **A.** Yes — anywhere on the internet is fine
- **B.** No — only install from official browser stores, and even then review carefully
- **C.** Only on Tuesdays
- **D.** Only if friends recommend

Q6. When your browser shows 'Your connection is not private' / 'Deceptive site ahead,' you should:

- **A.** Click 'Advanced' and 'Proceed anyway'
- **B.** Back out — believe the warning
- **C.** Continue if the site is small and unknown
- **D.** Reload until the warning goes away

Q7. Free 'PC optimisers,' 'driver updaters,' and 'free VPNs' you find online are usually:

- **A.** Genuinely free useful tools
- **B.** Malware delivery in the vast majority of cases
- **C.** Required for your operating system
- **D.** Trial versions of legitimate software

Q8. URL shorteners (bit.ly, tinyurl) hide the destination. Should you click them from unknown sources?

- **A.** Yes — they're shortened so they're safe
- **B.** No — without seeing the destination you can't evaluate the link
- **C.** Yes if they're under 30 characters
- **D.** Only on Twitter / X

Q9. Which of these provides the most privacy protection while browsing?

- **A.** Default Chrome settings
- **B.** Firefox (Strict tracking) + uBlock Origin extension
- **C.** Internet Explorer 11
- **D.** Browsing in airplane mode

Q10. On public Wi-Fi (coffee shop, hotel), what's the safest practice?

- **A.** Browse anything — the network is anonymous
- **B.** Use a VPN, OR avoid sensitive activity until trusted Wi-Fi
- **C.** Only browse with the lock icon visible
- **D.** Just lower your screen brightness

Answer Key

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

Q1: B — Mismatched URLs are one of phishing's strongest signals. The displayed text and actual link should match.

Q2: B — HTTPS = encryption only. Phishing sites have HTTPS too. Lock = private channel, not legitimate destination.

Q3: B — Tech-support scams. The pop-up is fake. Real OS errors don't include phone numbers. Close and restart.

Q4: B — 'rn' looks like 'm.' Typosquatting is one of the most common phishing techniques. Always read domain names carefully.

Q5: B — Even official stores have malicious extensions sometimes. Outside-store sources are far worse. Stick to official, review reviews.

Q6: B — Browser warnings are based on real threats. Clicking through is how breaches happen. Trust the warning.

Q7: B — Vast majority of 'free utility' downloads are malware or adware. Built-in tools (Defender, Windows Update) are sufficient.

Q8: B — Shortened URLs hide destinations — opaque to inspection. Use a link expander (unshorten.it) if you must click.

Q9: B — Firefox Strict + uBlock Origin blocks 90% of trackers automatically. Brave is similar. Default Chrome is the worst privacy environment.

Q10: B — Public Wi-Fi can be sniffed or impersonated. VPN encrypts your traffic. Skip banking/password changes until trusted networks.

Scoring

Score	Level	What it means
0–4	Beginner	Browser habits are exposing you. Read the Safe Browsing Cheat Sheet and the Browser Privacy Settings
5–7	Intermediate	Decent browsing instincts. Run the Browser Privacy Settings Tool to lock down further.
8–10	Advanced	Strong browser hygiene. Forward this quiz to less-savvy family members.