Small Business Cybersecurity Quiz

Quiz · 20 Questions Every SMB Owner Should Be Able To Answer.

Small businesses (1-25 employees) are the sweet spot for cyber attackers — valuable enough to extort, often without dedicated IT. Test your knowledge across the basics every SMB needs.

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. What's the #1 cause of small business breaches?

- **A.** Sophisticated nation-state attacks
- **B.** Phishing emails to employees, often resulting in credential theft or wire-transfer fraud
- **C.** Physical break-ins
- **D.** Brute-force password attacks

Q2. Should every employee have their own login (vs sharing one)?

- **A.** No — sharing is more efficient
- **B.** Yes — accountability, audit trails, and immediate offboarding all require individual accounts
- **C.** Only senior employees
- **D.** Only when convenient

Q3. An employee receives an urgent email from the CEO asking them to wire $50K to a vendor. The CEO is in a meeting and unreachable. What should the employee do?

- **A.** Wire the money — the CEO is urgent
- **B.** Verify the request via a separate, known channel before acting (callback, in-person)
- **C.** Wait for the CEO to email confirmation
- **D.** Process the wire and ask the CEO to confirm afterwards

Q4. What's the minimum viable data backup strategy for a small business?

- **A.** Hope nothing breaks
- **B.** 3-2-1 — three copies, two media, one offsite, automated, tested quarterly
- **C.** One USB drive in the office
- **D.** Email backups to the owner

Q5. Which of these is a basic minimum for SMB cybersecurity?

- **A.** Hiring a CISO
- **B.** Built-in OS security + endpoint protection + MFA on critical accounts + employee training + automated backups

C. Buying a $500K cyber insurance policy

D. Storing all data on paper

Q6. Should personal devices be used for work email and applications?

A. Yes, with no restrictions

B. Only with documented BYOD policy: MDM enrollment, security baseline, defined boundaries

C. Never — only company-issued devices

D. Only on weekends

Q7. What should happen when an employee leaves the company?

A. Their accounts are immediately disabled, MFA tokens removed, devices reclaimed, knowledge transfer documented

B. Their accounts are kept active 'just in case'

C. Nothing — they'll forget the passwords eventually

D. Only a friendly farewell

Q8. How often should employees complete cybersecurity awareness training?

A. Once when hired and never again

B. At hire AND annually thereafter — at minimum — plus after major incidents

C. Only after a breach

D. Whenever the boss feels like it

Q9. Cyber-liability insurance for a small business:

A. Is unnecessary if your security is good

B. Provides financial protection AND access to incident-response resources during a crisis

C. Is only for huge enterprises

D. Replaces the need for actual security controls

Q10. What should an SMB do BEFORE a cyber incident happens?

A. Wait until something happens, then react

B. Document an incident response plan, test backups, train employees, identify legal/regulatory notification requirements

C. Avoid thinking about it — bad luck

D. Just buy more insurance

Answer Key

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

Q1: B — Phishing-induced credential theft and wire fraud are by far the most common SMB breach vectors. Everything else is rare in comparison.

Q2: B — Shared logins make audits impossible and offboarding dangerous. Individual logins are non-negotiable for any business serious about security.

Q3: B — CEO-fraud / business email compromise is one of the most common SMB scams. Out-of-band verification is the universal defence.

Q4: B — 3-2-1 is the standard. Without it, ransomware = catastrophic. The restore-test is the part most businesses skip.

Q5: B — Defender + Malwarebytes + MFA + training + backups is achievable for any SMB. CISO and high-end tools are nice-to-haves; baseline first.

Q6: B — BYOD without policy is risky. With clear MDM-based controls, BYOD can be safe and cost-effective.

Q7: A — Offboarding is when many breaches happen — leftover accounts get exploited weeks/months later. Document and execute the offboarding checklist.

Q8: B — Annual training is the floor. Many regulations require it. Real awareness comes from regular reminders.

Q9: B — Cyber insurance often includes incident-response services, forensics, legal counsel — invaluable in a crisis. Combine with strong controls.

Q10: B — Pre-incident preparation determines outcome. Plan, test, train, document — when (not if) something happens, you'll execute, not panic.

Scoring

Score	Level	What it means
0–4	Beginner	Your SMB has significant gaps. Use the Small Business Cybersecurity Checklist and the Small Business S
5–7	Intermediate	Solid foundation. The Incident Response Plan Template and Cybersecurity Action Plan Template will harde
8–10	Advanced	Strong SMB posture. Make sure to also test your incident response plan annually with a tabletop exercise.

SCAM ALERT

Toll-Road SMS Scam Is Spreading Across The U.S.

Texts claiming you owe a small toll fee link to fake DMV-style sites. They steal card numbers and SSNs. Never click a 'toll' link — go to the toll authority directly.

Visit Making Sense Of Security →