Security Awareness Quiz

Corporate Training Edition

Contents

Introduction 3

Section 5: Data Protection 6

15. What should you do if you accidentally send sensitive data to the wrong recipient? 6

Introduction

Security awareness doesn't have to be complicated and it definitely doesn't have to be boring. This quick quiz is designed to test the everyday decisions that protect your organisation: spotting phishing attempts, handling data safely, challenging suspicious behaviour, and keeping systems secure.

It's not about catching people out. It's about reinforcing the habits that stop real attacks, helping everyone build confidence, and showing where a little extra awareness can make a big difference.

Use this quiz as part of your training day, team briefing, or onboarding programme. Each question reflects common scenarios we see during penetration tests and social engineering engagements, the same areas attackers target most often.

Section 1: Phishing & Email Security

1. You receive an email saying *"Your mailbox is full, click here to upgrade storage"*. What's your first step?

A. Click the link to fix it
B. Ignore it
C. Check the sender and report it if suspicious
D. Forward it to colleagues

2. Which of the following is a common sign of a phishing email?

A. Perfect grammar
B. Urgent language asking you to act quickly
C. Sent from a known colleague
D. Contains company branding

3. You get an invoice for a service your team doesn't use. What should you do?

A. Pay it immediately
B. Reply and ask for details
C. Report it to IT/security
D. Delete it without telling anyone

Section 2: Passwords & Access

4. Which is the best password approach?

A. Your pet's name + birth year
B. A long, memorable passphrase
C. Same password for multiple services
D. A short password with numbers

5. Which account type should you *never* use for email or web browsing?

A. Standard user
B. Admin/privileged account
C. Guest account
D. Temporary account

6. MFA (Multi-Factor Authentication) helps protect you even if…

A. Your password is leaked

B. Your computer is old

C. You forget your username

D. You don't trust your antivirus

Section 3: Physical Security & Social Engineering

7. Someone tailgates behind you while entering the building. What do you do?

A. Hold the door open, it's polite

B. Challenge them or direct them to reception

C. Assume they work here

D. Ignore them and hope security notices

8. A visitor says they have a meeting but can't remember the host's name. What's the right action?

A. Let them in anyway

B. Escort them to the office

C. Direct them to reception

D. Ask them to wait alone in a meeting room

9. A person wearing a high-visibility vest asks for access to the server room "just to check something quickly." What's the correct response?

A. Let them in, they look official

B. Ask for their ID and confirm with the IT team

C. Follow them into the room

D. Assume they're from maintenance

Section 4: Office & Device Safety

10. Leaving your laptop unlocked when you walk away is…

A. Fine if it's only for a minute

B. OK if you trust your colleagues

C. A security risk

D. Harmless if your desk is tidy

11. What should you do if you plug in a USB drive and see unexpected files appear?

A. Open them to see what they are

B. Scan with antivirus

C. Report it immediately

D. Plug it into another device to check

12. You receive a phone call from someone claiming to be IT support asking for your password. You should:

A. Give it to them

B. Ask for their number and call back

C. Report the call immediately

D. Tell colleagues first

Section 5: Data Protection

13. Sensitive information should be:

A. Emailed to your personal account for convenience

B. Stored only in approved systems

C. Shared freely with colleagues

D. Saved on a USB drive

14. When sending a document externally, what's the safest approach?

A. Attach it directly

B. Use an approved secure sharing method

C. Share via social media

D. Use your personal Gmail account

15. What should you do if you accidentally send sensitive data to the wrong recipient?

A. Hope they delete it

B. Email them and ask politely

C. Report it immediately

D. Delete the message and move on

Scoring (Optional)

- **13–15 correct:** Security Champion
- **10–12 correct:** Strong Awareness
- **7–9 correct:** Needs a refresher
- **0–6 correct:** Book a BlackBox Pentesters training day immediately