

Stop. Check. Call. Staff quiz

Name: _____ · Date: _____
Name Date

12 questions, about 10 minutes. Circle one answer for each. This isn't a test of anyone's job; it shows what stuck from the briefing. All companies, people and web addresses below are made up.

1. An email from "Cedar Lane Supply" says they've changed banks and asks you to send this month's payment to a new account. The address is `billing@cedarlanesupply.example`, the same one they always use. What do you do?
 - A. Update the details. The address is correct, so it's really them.
 - B. Reply and ask them to confirm the new account.
 - C. Call Cedar Lane on the number in our contact list before changing anything.
 - D. Call the phone number in the email's signature.
2. A text arrives: "It's {OWNER NAME}. In a client meeting, can't talk. Please buy six \$100 gift cards for client thank-yous and text me photos of the backs. I'll pay you back today." What's the right move?
 - A. Buy the cards. The owner needs help.
 - B. Text back to ask which kind of gift card.
 - C. Treat it as a scam. Call the owner on the number you already have, and report it.
 - D. Buy the cards but only send the codes, not photos.
3. Which of these is the strongest sign an email is a scam?
 - A. It has spelling mistakes.
 - B. It pressures you to act now and asks for money or a password.
 - C. It has a company logo.
 - D. It was sent early in the morning.
4. An email says: "Your mailbox password expires today. Click here to keep your current password." What's the safest response?
 - A. Click and type your password quickly before it expires.
 - B. Don't use the link. Open the email site or app yourself, or ask {IT CONTACT}, and report the message.
 - C. Forward it to the whole office to ask if anyone else got it.
 - D. Reply "unsubscribe".
5. You hover over a "View invoice" button in an email from Bluepine Couriers. The address that appears is `http://bluepine-couriers.delivery-update.example/inv`. What does that tell you?
 - A. Nothing. Hovering doesn't show anything useful.
 - B. It goes to a different site from the one you'd expect. Don't click; report it.
 - C. It's safe because it starts with "bluepine".
 - D. It's safe because it says "invoice".
6. A pop-up on your screen says "Virus detected! Call Support now" and shows a phone number. What do you do?
 - A. Call the number so they can fix it.
 - B. Let them connect to the computer if they sound professional.
 - C. Don't call. Close the window, and tell {IT CONTACT} if it won't close.
 - D. Pay with a card, because it's a one-time fee.

7. You opened an attachment and now the computer is acting strangely. What's the first thing to do?
- A. Say nothing and hope it goes away.
 - B. Switch the computer off at the wall and go home.
 - C. Tell **{CONTACT PERSON}** right away, and disconnect the computer from the network without switching it off.
 - D. Run every program on the computer to see what broke.
8. A caller sounds exactly like a regular client, Marisol from Harbor Point Realty, and urgently asks you to send her deposit refund to a new account today. What do you do?
- A. Send it. You recognize her voice.
 - B. Hang up and call Marisol back on the number we already have for her.
 - C. Ask her to email the new details instead, then send it.
 - D. Ask for her date of birth to check it's her.
9. Under our policy, which of these needs two people to approve?
- A. Any payment over **{\$X}**.
 - B. Any new payee, at any amount.
 - C. Any change to bank details, at any amount.
 - D. All of the above.
10. Someone who says they're "from the bank's fraud team" calls and asks you to read out the login code that just arrived by text. What do you do?
- A. Read it out. They're protecting the account.
 - B. Never share the code. Hang up and call the bank on the number on our statement or card.
 - C. Read out only the first half.
 - D. Text it to them instead.
11. You realize a payment you sent this morning went to a scammer's account. What's the most urgent step?
- A. Wait until tomorrow to see if it bounces.
 - B. Email the scammer and ask for it back.
 - C. Call our bank right away and ask them to recall or reverse the payment, then tell **{CONTACT PERSON}**.
 - D. Delete the email so nobody else falls for it.
12. You're not sure whether a message is a scam. What should you do?
- A. Ignore it and don't tell anyone, in case you're wrong.
 - B. Report it the way we do here: **{OUR REPORTING STEP}**. Reporting a real message by mistake is fine.
 - C. Click the link to see where it goes.
 - D. Forward it to coworkers to get opinions.

Small-Office Phishing Drill Kit, Tech Cheat Codes, v1.0. Not legal advice.