

Quiz answer key (for the manager)

Go through the answers out loud with the team. The "why" lines are written to be read as they are. All companies, people and addresses in the quiz are made up.

#	Answer	Why
1	C	A correct address doesn't prove anything: the vendor's real account can be hacked. Our rule: bank changes are confirmed by calling a number we already had. Replying (B) or calling the number in the email (D) can reach the scammer.
2	C	Treat any request to buy gift cards and send the codes as a scam. No real business or government agency will tell you to buy a gift card to pay them. The codes on the back are as good as cash.
3	B	Pressure plus a request for money or a password is the classic pattern. Spelling isn't a reliable sign anymore: with AI writing tools, some scam emails now have perfect spelling and grammar. Logos are easy to copy.
4	B	Never sign in from a link in a message. Go to the site or app yourself. Forwarding (C) spreads the link. Don't reply to a suspicious message or click its "unsubscribe" link (D); report it and delete it.
5	B	The real destination ends in delivery-update.example, not the courier's own site. A familiar word at the start of an address doesn't mean the site belongs to that company.
6	C	A pop-up that tells you to call a number is a classic sign of a tech-support scam. Never give remote access or payment to someone who contacted you.
7	C	Speed matters more than embarrassment, and there's no blame. Disconnect from the network (cable or Wi-Fi) but don't switch the computer off unless {IT CONTACT} says to.
8	B	Voices can be copied with AI, and caller ID can be faked. Call back on a number you already had. Asking for an email (C) can still go to the scammer, and personal details (D) can be stolen.
9	D	Our policy: two people for payments over {\$X}, any new payee and any bank change.
10	B	Never read out a login code to someone who contacted you; the code lets them into the account. Hang up and call the bank on a number from a statement, card or the website you look up yourself.
11	C	Call the bank first. The sooner the bank is asked to recall the payment, the better the chance of reducing the loss. The manager then reports it (IC3 for business email scams; ReportFraud.ftc.gov). Keep the email until the manager has reported it.
12	B	Reporting costs nothing. We'd rather check ten real messages than miss one fake.

Scoring: there's no pass mark. Look at which questions people missed and spend two minutes on those at the next team meeting.

Small-Office Phishing Drill Kit, Tech Cheat Codes, v1.0. Not legal advice. Need help? Visit techcheatcodes.com/support/