

Tabletop drill: three scenarios in 15 minutes

A tabletop drill is a talk-through. Nobody gets a fake email, and nothing is sent to anyone's inbox. The manager reads each scenario aloud, the team says what they'd do, and you compare it with "what good looks like." Run it a week or two after the training deck, then again every few months with the names changed.

You need: the team (in person or on a call), this sheet, a printed callback card for each person, and a timer. **Facilitator:** _____ . **Date:** _____ .
Name Date

How to run it (read this out first, 1 minute)

"This is practice. There are no wrong answers and nobody is being graded. I'll read a situation. Tell me what you'd do, step by step, as if it were happening right now. I'll add details as we go."

All companies, people and addresses below are made up. Swap in your own vendors' types (not real names) and your own roles if that makes it feel more real.

Scenario 1: The fake invoice (4 minutes)

Read aloud: "It's Thursday afternoon. An email arrives from accounts@northfieldpaper.example, which looks like our paper and supplies vendor. It says: 'Please find attached invoice 4471, now overdue. Note our new banking details below; our old account is closed. Kindly pay today to avoid a late fee and a hold on your next order.' The attached invoice looks right. {Name of the person who pays bills}, what do you do?"

Add after the first answers: "You call the number in the email signature, and a friendly person confirms the new account."

Ask: Was that callback good enough? Who else needs to be involved before this payment goes out?

What good looks like: don't pay and don't change the bank details from the email. Don't reply, and don't use the signature number; it can go straight to the scammer. Call Northfield on the number in our known-numbers list or on an old invoice. Because it's a bank change, a second person checks the callback before anything is released. Report the email to {CONTACT PERSON} even if it turns out to be real.

Scenario 2: The "CEO" gift card text (4 minutes)

Read aloud: "It's 8:15 on a Monday. A text from a number you don't recognize: 'Hi, it's {OWNER NAME}, this is my personal number. Are you free? I need a quick favor, I'm stuck in back-to-back meetings. Please pick up five \$200 gift cards for some clients on your way in, scratch the backs and text me the photos. Keep it quiet, it's a surprise.' {Front desk person}, what do you do?"

Add after the first answers: "A minute later: 'Are you on it? I need them in 20 minutes.'"

Ask: What are the warning signs? Who do you tell?

What good looks like: treat it as a scam. Warning signs: a new number, urgency, "keep it quiet", and a request for the codes. Don't reply. Check with the owner on the number you already have for them, or in person. Tell **{CONTACT PERSON}**, because others in the office may get the same text. If anyone had already bought cards: keep the cards and receipts, contact the gift card company right away to ask for the money back, and report it at ReportFraud.ftc.gov.

Scenario 3: "Your password expired" (4 minutes)

Read aloud: "An email that looks like it's from our email provider: 'Your password expired at 9:00 AM. To avoid losing access to your mailbox, sign in within 2 hours to keep your current password.' There's a big blue 'Keep my password' button. **{Any staff member}**, what do you do?"

Add after the first answers: "Say someone already clicked and typed their password in, then the page just went blank."

Ask: What happens now, in order? Who does what?

What good looks like: don't use the button. Hover over it to see where it really goes. If you're worried about your account, open the email site or app yourself, or ask **{IT CONTACT}**. Report the message and delete it. **If someone typed their password in:** tell **{CONTACT PERSON}** at once (no blame), change that password right away, and change it anywhere else the same password was used. Make sure multi-factor authentication is on for that account.

Wrap-up (2 minutes)

Ask the team, and write the answers down:

1. Was there any step today where we weren't sure who to call or where the numbers are kept?

Answer

2. One thing we'll change after today: _____

Answer

3. Next drill date: _____

Date

Timing: 1 min intro + 3 × 4 min scenarios + 2 min wrap-up = 15 minutes. Not legal advice. Small-Office Phishing Drill Kit, Tech Cheat Codes, v1.0. Need help? Visit techcheatcodes.com/support/