

Stop. Check. Call.

A 20-minute phishing briefing for **{OFFICE NAME}**

{PRESENTER NAME}, **{DATE}**



Why this matters to us

- Phishing was the most reported type of cybercrime to the FBI in 2025
- Small offices are targets, not too small to notice
- One click or one payment can cost real money, data or days of work



What phishing looks like

- Email, text, social media message or phone call
- Looks like someone you trust: a vendor, a bank, a delivery company, the boss
- Wants you to click, open, pay, or share a password or account details



The three warning signs

1. **Pressure:** "Today", "urgent", "or your account will be closed"
2. **The ask:** money, gift cards, passwords, codes, bank details
3. **Something's off:** the sender, the link or the request doesn't quite fit



Perfect spelling doesn't mean it's real.

Check the sender

- Look at the real address, not just the name
- Lookalike: `billing@cedar1lanesupply.example` vs `billing@cedarlanesupply.example`
- On a computer, right-click or hover over the sender. On a phone, tapping the sender's name usually shows the full address.
- A real address can still be hacked. The request matters most.



Check the link

- Hover over a link before you click (on a computer, the real address appears near the mouse or at the bottom of the window)
- Be wary of shortened links and odd addresses
- Asked to log in? Don't use the link. Go to the site yourself.



Unexpected files and invoices

- Didn't expect it? Don't open it.
- "Invoice attached", "Shared document", "Voicemail received"
- Check with the sender using a number or address you already have
- Opening the wrong file can lock up the whole office



The fake vendor

- "We've changed banks. Please send all future payments to this new account."
- Comes from a vendor's address, or one that looks just like it
- Timed for when an invoice is due
- Never change bank details from an email or text alone



The callback rule

1. Don't reply, and don't use any number, link or contact in the message
2. Call a number you already had: our contact list, an old invoice, the official website you typed in yourself
3. Ask: "Did you send this request?"
4. No confirmation, no payment



Our known-numbers list: {WHERE IT'S KEPT}

Two people for big payments

- Any payment over `{ $X }`: two people approve
- Any new payee or changed bank details: two people approve, after a callback
- Person 1 sets it up. Person 2 checks and releases it.
- "The boss said to skip it" is not an exception



Gift card requests are a scam

- "It's **{OWNER NAME}**. I'm in a meeting. Buy 5 gift cards for clients and text me the codes."
- No real business or government agency asks to be paid in gift cards
- Check with the person on a number you already have
- Never send gift card numbers or photos of cards



Tech support calls and pop-ups

- A call says our computer has a problem? Hang up.
- A pop-up says "Call this number"? Don't call. Close it.
- Never give remote access or a password to someone who contacted you
- Worried? Call **{IT CONTACT}** on the number you already have



"Your password expires today"

- Fake login pages can look just like the real one
- Don't sign in from a link in a message. Go to the site yourself.
- Turn on multi-factor authentication (MFA): a second step after your password
- Never share a login code. Anyone who asks for it is a warning sign.



Texts, calls and familiar voices

- Scams come by text, phone and social media too
- Caller ID and names can be faked
- A voice can be faked with AI. A familiar voice isn't proof.
- Same rule: hang up and call back on a number you already have



If you clicked, tell us right away

- No blame. Speed matters more than embarrassment.
- Tell **{CONTACT PERSON}** at once: **{HOW TO REACH THEM}**
- Change any password you typed in
- Unplug the network cable or turn off Wi-Fi on that computer, but don't switch it off



If money went out

- Call the bank right away and ask them to recall or reverse the payment
- Tell **{CONTACT PERSON}** at once
- Report it: IC3 for business email scams, ReportFraud.ftc.gov for scams
- Gift cards: keep the cards and receipts; contact the card company



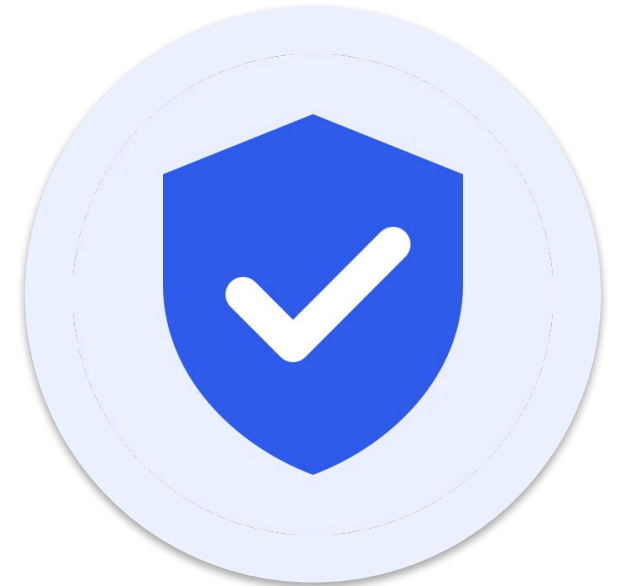
How we report a suspicious message

- Don't reply, click or forward it to coworkers
- Report it: **{OUR REPORTING STEP, e.g. "Report phishing" button or forward to {ADDRESS}}**
- Tell **{CONTACT PERSON}** if it asked for money or a password
- Then delete it



Stop. Check. Call.

- **Stop:** pressure, money, passwords, or something off? Pause.
- **Check:** the real sender and the real link. Log in on your own.
- **Call:** a number you already had. Two people for big payments.
- Clicked? Tell us right away. No blame.
- Next: a 10-minute quiz



Not legal advice. This deck is staff awareness training. It doesn't replace your bank's rules, your IT provider's advice or your insurance policy's terms.

Need help? Visit techcheatcodes.com/support/