

THE SCAM-PROOF CHECKLIST

Five rules and four warning signs from ten real cases. Print it. Pin it up. Send it to your team.

FOUR WARNING SIGNS

URGENCY

"Your VPN is about to be deactivated." Time pressure is there to stop you checking.

SECRECY

"Don't tell anyone." A request that cannot survive being checked.

A NEW ACCOUNT

Same supplier, new bank details. Same colleague, new number.

A FEE TO GET PAID

Pay a tax, then a late fee, to withdraw your own money.

FIVE RULES

☐ 1 Check on a channel you chose

Hang up and call back on a number you already have. Confirm any change of payment details the same way. Verify the person, not just the paperwork.

Seen in: the fake supplier invoice, the Twitter help-desk call, the North Korean IT workers.

☐ 2 Never type a login or read out a code because someone asked

Open the site yourself or use a bookmark. Nobody who legitimately works there needs you to read them a code.

Seen in: Twitter, the Cloudflare and Twilio texts, Retool.

☐ 3 Use a key, not a code

A password can be typed into a fake site, a code can be relayed, a tap on Approve can be worn down. A hardware security key checks the site's address. Where you can't use one, prefer number matching to a bare tap.

Seen in: Cloudflare (three clicked, nothing lost), Uber, Twitter.

☐ 4 Two people for big actions, least access for everyone

Two approvals for payment-detail changes, large payments and risky admin actions. Give each account only the access it needs, so one mistake does not travel far.

Seen in: Twitter (1,000+ people with access), RSA, the invoice fraud.

☐ 5 Report in minutes, and make it safe to report

Over-report. Do not blame the person who clicked. Cloudflare went from first text to takedown in under 40 minutes; the employee who reported a \$1 million offer helped stop an attack before it began.

Seen in: Cloudflare, the insider offer, the invoice recovery.

IF IT ALREADY HAPPENED TO YOU

1. Stop paying. Do not pay any fee to "release" your money.
2. Call your bank right away. Speed is what gets money back.
3. Keep every message, app name, website, wallet address and transfer record.
4. Report it to your local authority. In the US, that is the FBI's IC3 (ic3.gov). Tell someone you trust.