

How to use ScamDrill

Your quick guide to spotting scams — and what to do when one shows up.

Don't worry: ScamDrill sends you safe, pretend scams so you can practice spotting the real ones. Nothing it sends can hurt your computer or your money.

Three things to remember

1 Think it's a scam? Report it.

If it feels off, report it — you don't have to be sure.

- Suspicious email — forward to **spam@scamdrill.com**
- ScamDrill practice text — reply **SCAM** (only texts labeled [ScamDrill Training])

Never reply to a real scam text — just delete it, or forward it to check (step 2). Only reply SCAM to ScamDrill practice texts.

2 Not sure if it's real? Check it.

We reply with a plain-language verdict — and the reasons why.

- Email — forward to **check@scamdrill.com** (up to 10 a day)
- Text — forward to **(571) 582-4381** (if texts are on for you)
- A link, or anything else — open **smdl.app/check** and paste it in

3 Make sure drills reach you.

Our practice scams look real, so spam filters may hide them.

- Save **sim@scamdrill.app** to your contacts — it's the address drills come from
- Allow **scamdrill.app** in safe senders — full steps at app.scamdrill.com/whitelist

A few golden rules

- ✓ Slow down. Scammers rush you with “act now” or “final notice.” Real businesses give you time.
- ✓ Don't click links or open attachments you weren't expecting — even from someone you know.
- ✓ Never share passwords, security codes, or payment details by email or text.
- ✓ Be very suspicious of anyone who wants gift cards, cryptocurrency, or a wire transfer.
- ✓ When unsure, contact the company yourself using a number you look up — not the one in the message.