

Stop the Scam

A text from your bank. An urgent email from your boss. An unbelievable online deal.

They might be legitimate—or they might be scams.

Basic Safety Steps

Remember to:

STOP → CHECK → ACT

STOP — Don't let urgency push you into acting immediately.

CHECK — Verify the sender, link, request, or offer independently.

ACT — Delete, report, or respond using a trusted channel.

Here are the warning signs:

Urgency — “ASAP” pressures you to act before checking.

Unusual request — Gift cards are difficult to recover once the codes are sent.

Secrecy/lack of context — “I'll explain later” discourages normal verification.

Challenge 1 — The suspicious text

You receive the following text:

Fraud Alert: A charge of \$849.00 was made to your account. If you did not authorize this transaction, verify your account immediately:

What should you do?

Tap the link immediately

Reply and ask whether it's legitimate

Use a known bank office phone number to check the account.

Challenge 2 — Spot the warning signs

From: CEO Office

Subject: Need your help ASAP

I'm heading into a meeting and need you to purchase four \$100 gift cards for a client. Send me the codes as soon as you have them. I'll explain later.

Select the warning signs. Select all that apply.

Urgency

Unusual request

Secrecy/lack of context

Challenge 3 — What Should You Do First?

You receive this text:

Bank Security Alert: We detected a suspicious \$1,275 purchase on your account. Your account will be locked unless you verify your information immediately.

VERIFY ACCOUNT

Order these. What should you do first, then second, then third.

Stop

Check

Act