Is This a Scam?

How to spot one before you click, pay, or reply

Four common signs of a scam

1. **Pretend.** They pretend to be your bank, the government, a company you know, or family.
2. **Problem or prize.** Your account is locked, you owe money, or you won something.
3. **Pressure.** Act right now. Don't hang up. Don't tell anyone.
4. **Pay.** Gift cards, wire transfer, payment app, crypto, cash, or a check you send money back from.

See one? Pause. Hang up. Look up the real number yourself, like the one on the back of your card.

FTC rules worth memorizing

- A caller who asks for a verification code sent to your phone is a scammer.
- Anyone who demands payment by gift card is a scammer.
- Anyone who tells you to move your money to protect it is a scammer.
- Real security pop-up warnings never ask you to call a number.

What to do

- Don't tap the link or reply. Go to the company's app, or type the web address yourself.
- Forward scam texts to 7726 (SPAM).
- Report any scam at ReportFraud.ftc.gov. Age 60 or older? The Elder Fraud Hotline is 833-372-8311.

Spot the red flags

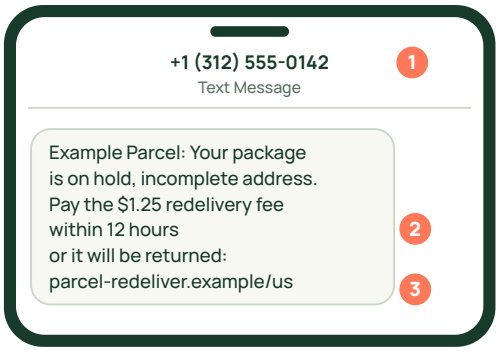


Illustration. Example Parcel, the number, and the link are made up.

1. A number you don't know. Did you ever sign up for texts from them?
2. A tiny fee plus a deadline. The real target is your card number.
3. A link to "fix" it. USPS only texts if you asked for tracking updates, and those texts have no links.

Read the web address, not the logo

Find the first single slash after https://. The name just before it is the real owner.

https://www.**examplebank.example**/login ✓

The real site. The name right before the first single slash is the bank's own.

https://examplebank.example.**account-check.example**/login ✗

The bank's name is there, but it's a decoy. The owner is account-check.example.

https://www.**examp1ebank.example**/sign-in ✗

A look-alike. The letter l was swapped for the number 1.

https://**examplebank-secure.example**/verify ✗

An extra word tacked on. Not the bank's address.

Ask an AI for a second opinion

> I got this text and I have not tapped anything in it. I took out my personal details. In plain words, tell me: who it says it's from, what it wants me to do, and any signs it could be a scam. Then tell me how I could check it myself without using any link or number in the text. Here is the text: **[paste the text]**

Take out your name, account numbers, and any codes first. AI can be wrong, so always check with the real company yourself.

The full guide, **Is This a Scam?**, explains a dozen common scams with marked-up examples, plus a recovery plan, printable cards, and 25 AI prompts. Find it at aiveryhuman.com.

General information, not legal or financial advice. Facts checked with FTC, FBI, CISA, USPIS, and Social Security sources on October 23, 2026. No guarantee. If you were scammed, contact your bank and report it. Examples are made up. Trademarks belong to their owners; aiveryhuman is not affiliated with or endorsed by any agency or company named.

aiveryhuman