Ask It Simply

Free · plain English · keep by the phone

The Scam-Proof Pocket Guide

Spot today's most common scams, know exactly what to do, and report them, wherever you live.

Stop. **Check.** **Ask.**

- ✓ The 9 scams to know right now
- ✓ Check any message with free AI
- ✓ If you've been scammed: what to do first
- ✓ Where to report in the US, UK, Canada and Australia

By Dontè, Ask It Simply
Updated October 2026

askitsimply.com/scam-guide

START HERE

The 10-second version

> If a message **surprises you**, **rushes you**, or asks you to **pay in an unusual way**: stop. Don't click, don't call the number in it, and don't pay. Check with the real company or person yourself, using a number or website you already trust.

$15.9 billion

That's how much people told the U.S. Federal Trade Commission they lost to fraud in 2025, across 3 million reports. That's up from more than $12 billion in 2024. Impostor scams were reported most often. Investment scams cost the most: $7.9 billion.

Source: FTC (full links on page 12)

How to use this guide

- ✔ Learn the 3-step habit (page 3) and the 4 P's (page 4).
- ✔ Look up the scam you're worried about (pages 5 to 9).
- ✔ Check any message with free AI (page 9).
- ✔ Been scammed? Act fast (page 10), then report it (page 11).

YOUR HABIT

Stop. Check. Ask.

Use it on every surprise text, email, call or pop-up.

1 Stop

Don't click, reply, call back or pay. Not yet. A real problem will still be there in ten minutes. The FTC notes that honest businesses give you time to decide.

2 Check

Contact the company or person yourself, using a number or website you already trust: the back of your card, a bill, your contacts, or a web address you type in. Never use the link or number in the message.

3 Ask

Talk to someone you trust before you act: a friend, a family member, your bank, or an AI tool with our scam check. Saying it out loud often makes a scam obvious.

Stop, Check, Ask is our own routine, built on FTC advice. Australia's Scamwatch teaches a similar idea: “Stop. Check. Protect.”

Source: FTC, Scamwatch (full links on page 12)

RED FLAGS

The 4 P's

You'll find at least one in almost every scam.

Pretend

They pretend to be someone you trust: the government, your bank, a delivery company, tech support, or even family. Caller ID and names can be faked.

Problem or prize

There's a scary problem (a charge, a virus, an arrest, an unpaid bill) or an exciting prize you didn't enter to win.

Pressure

You must act now. Don't hang up. Don't tell anyone. Pay today or else.

Pay

They want a hard-to-undo payment: gift cards, cryptocurrency, a wire transfer, a payment app, cash, or “deposit this check and send some back.”

One rule to remember: anyone who demands gift cards, cryptocurrency, a wire transfer or a payment app, and won't take anything else, is almost certainly a scammer.

Adapted, in our own words, from the FTC's four signs of a scam.

Source: FTC (full links on page 12)

01 Toll, package and “you owe” texts

LOOKS LIKE A text says you have an unpaid toll, or a package can't be delivered until you confirm your address or pay a small fee. There's a link and a deadline.

GIVEAWAY A small amount, a late-fee threat, and a link. The U.S. Postal Inspection Service says USPS won't text or email you unless you first asked for tracking with a tracking number, and those messages won't contain a link.

DO THIS Don't tap the link or reply, not even with Y or N. Check your toll account or tracking on the official website you type in yourself. Forward the text to 7726 (SPAM), then delete it.

Source: FTC, FBI IC3, FCC, USPIS (full links on page 12)

02 Fake bank “fraud alerts”

LOOKS LIKE A text or call that seems to come from your bank about a suspicious charge. If you respond, a friendly “fraud team” tells a scary story and offers to help.

GIVEAWAY They contacted you, they're rushing you, and they want a code, your login, or for you to move money. The FTC says scammers posing as your bank promise to help, then drain your account, and that no real government agency will tell you to move your money to “protect it.”

DO THIS Hang up or don't reply. Call the number on the back of your card, or open your bank's app or website yourself. Never call back the number that contacted you.

Source: FTC (full links on page 12)

03 Tech support pop-ups and calls

LOOKS LIKE A loud pop-up says your computer is infected and to call a number now. Or a “technician” calls you. Or an email says a tech support subscription renewed for hundreds of dollars.

GIVEAWAY The FTC says real tech companies won't call, email or text you about a problem with your computer, and real security warnings never ask you to call a phone number.

DO THIS Don't call, and never give anyone remote access to your computer. Close the page. If you're worried, update your security software and run a scan, or ask someone you trust. Check your card statement yourself for any “renewal.”

Source: FTC (full links on page 12)

04 Family emergencies and AI voice clones

LOOKS LIKE A panicked call from a grandchild or relative: an accident, an arrest, they need money right now, and “don't tell Mom.” A fake lawyer or officer may get on the line.

GIVEAWAY Urgency, secrecy, and payment by wire transfer, gift card, crypto, a payment app, or cash picked up in person. The FTC warns a scammer can clone a loved one's voice from a short audio clip, maybe from a video posted online. So the voice alone proves nothing.

DO THIS Hang up and call your loved one on the number you already have. Call another family member too, even if you were told to keep it secret. Pick a family safe word today: the FBI recommends a secret word or phrase to confirm who's really calling.

Source: FTC, FBI IC3, FCC (full links on page 12)

05 Fake shopping deals (Black Friday and holidays)

LOOKS LIKE A social media ad shows brand-name goods at amazing prices and links to a shop you've never heard of. You pay, then get a fake, something different, or nothing at all.

GIVEAWAY Prices that are too good to be true, a web address you don't recognize, and a seller who only takes gift cards, wire transfers, payment apps or crypto.

DO THIS Before you buy, search the store's name and web address plus “review,” “complaint” or “scam.” Pay by credit card when you can, so you can dispute the charge. Keep your receipt and order number.

Source: FTC (full links on page 12)

06 “Pay me with gift cards”

LOOKS LIKE Someone (the “government,” a utility, tech support, a prize office, a new love interest) tells you to buy gift cards and read them the numbers, or send a photo of the back. They may stay on the phone while you shop.

GIVEAWAY The FTC is clear: only scammers ask you to pay with a gift card and give them the numbers. No real business or government agency will.

DO THIS Stop and hang up. If you already paid, call the gift card company right away using the number on the card, tell them it was a scam, ask for your money back, and keep the card and receipt.

Source: FTC (full links on page 12)

07 Romance scams

LOOKS LIKE A charming match online who can't meet in person: working overseas, in the military, on an oil rig. After weeks of sweet messages comes an emergency that needs money, or an offer to teach you crypto investing.

GIVEAWAY They can't meet you in person, they soon want to move the chat off the dating site, and sooner or later they need money or want to “help you invest.”

DO THIS The FTC's bottom line: “Never send money or gifts to a sweetheart you haven't met in person.” Talk to a friend, and try a reverse image search of their profile photo.

Source: FTC (full links on page 12)

08 Crypto and investment scams

LOOKS LIKE A stranger, a so-called investment manager, a celebrity post, or an online friend promises big, guaranteed, low-risk returns, often in crypto. A slick website shows your “profits,” but you can't take money out.

GIVEAWAY Guaranteed profits. The FTC says only scammers guarantee returns or demand payment in cryptocurrency. Investment scams caused the biggest reported losses in 2025: $7.9 billion.

DO THIS Don't send money or crypto to anyone you've only met online. Search the company or person's name plus “review,” “scam” or “complaint,” and talk to someone you trust first.

Source: FTC (full links on page 12)

09 Fake jobs

LOOKS LIKE An easy, high-paying job, often from home: reshipping packages, “mystery shopping,” or an offer by text. Then they charge you for training, or send a check and ask you to send part of it back.

GIVEAWAY The FTC says honest employers never make you pay to get a job, and “deposit this check and send some back” is a fake check scam. The check bounces and you owe the bank.

DO THIS Never pay to get a job and never forward money from a check. Look up the company yourself. For U.S. federal jobs, use the official site, USAJOBS.gov.

Source: FTC (full links on page 12)

Check it with free AI

Copy this into Grok, ChatGPT, Gemini, Copilot, Claude or Perplexity. Paste the message where it says to. Or use the one-tap version at **askitsimply.com/scam-guide**.

```
Please help me check if this message is a scam. I removed my personal details first.

1. Rate the scam risk as Low, Medium or High, and tell me why in one plain sentence.
2. List the red flags you see (for example: pressure to act fast, a strange link, a prize or a problem I didn't expect, or a request to pay with gift cards, crypto, a wire transfer or a payment app).
3. Give me safe next steps. Don't tell me to click any link, call any number or reply to anything in the message. Tell me how to check with the real company or person using their official website or app, or a number I already trust, like the one on my card, bill or contacts.
4. Remind me what I should never share: passwords, one-time codes, PINs, Social Security or ID numbers, and account numbers.

Here is the message (a text, an email, or what a caller said):
"""
[Paste the suspicious message here]
"""

Please answer in plain English, like you're helping a friend who is new to this.
```

Before you paste: delete passwords, PINs, one-time codes, ID numbers and account numbers. AI is a second opinion, not proof.

IT HAPPENS TO SMART PEOPLE

If you've been scammed

Act fast, and don't be embarrassed. Find how you paid or what you shared:

Credit or debit card	Call the number on the back of your card right away. Ask them to reverse the charge.
Bank transfer or Zelle	Call your bank or credit union immediately. Ask them to reverse the payment.
Payment app (Venmo, Cash App, PayPal)	Report it in the app right away and ask for a reversal.
Wire transfer (Western Union, MoneyGram)	Call the wire company immediately. Say you were scammed and ask for a refund.
Gift card	Call the gift card company using the number on the card. Keep the card and receipt.
Cryptocurrency	Contact the exchange or crypto ATM company right away. Crypto is hard to get back, so act fast.
Your Social Security number	Go to IdentityTheft.gov. If it was used, you'll get a step-by-step recovery plan; if you're not sure, see IdentityTheft.gov/databreach.
A password	Change it right away, and anywhere else you used it. Turn on two-step verification.
Access to your computer	Update your security software, run a scan, and change your passwords.

Source: FTC, IdentityTheft.gov, IdentityTheft.gov/databreach (full links on page 12)

Watch out for “recovery” scams. Scammers often come back, pretending they can get your money back for a fee. Australia's Scamwatch says 1 in 3 scam victims are scammed more than once, and the FBI's IC3 says it will never contact you directly for information or money.

Source: FTC, Scamwatch, FBI IC3 (full links on page 12)

HELP STOP THE NEXT ONE

Report it

In danger right now? Call your local emergency number first.

United States

Federal Trade Commission
ReportFraud.ftc.gov

FBI Internet Crime Complaint Center (online crimes)
ic3.gov

Scam texts
Forward to 7726 (SPAM)

AARP Fraud Watch Network Helpline (free)
877-908-3360 · Mon–Fri, 8 a.m.–8 p.m. ET

United Kingdom

Report Fraud (replaced Action Fraud on Dec 4, 2025) · England, Wales, N. Ireland
reportfraud.police.uk · 0300 123 2040

Scotland
Police Scotland on 101

Canada

Canadian Anti-Fraud Centre
1-888-495-8501 · reportcyberandfraud.canada.ca

Australia

Scamwatch (National Anti-Scam Centre)
scamwatch.gov.au/report-a-scam

IDCARE (free identity and cyber support)
1800 595 160

Everywhere else

Your bank first, then your local police
Call your bank's official number to stop payments, then report the scam to the police where you live.

✂ cut out and keep

Stop. Check. Ask.

- Don't click, call back or pay. Hang up.
- Call the number on your card or bill yourself.
- Gift cards, crypto or wire only? Scam.
- Never share codes, PINs or passwords.

US: ReportFraud.ftc.gov · AARP 877-908-3360
UK: 0300 123 2040 · CA: 1-888-495-8501 · AU: scamwatch.gov.au

Sources

Every fact and number in this guide comes from these official pages, checked October 18, 2026. The writing, routine and design are our own.

1. **FTC** 2025 fraud reports and losses, from FTC testimony to Congress
   ftc.gov/news-events/news/press-releases/2026/03/ftc-testifies-joint-economic-committee-agencys-efforts-combat-fraud
2. **FTC** How to avoid a scam (the four signs, payment red flags)
   consumer.ftc.gov/articles/how-avoid-scam
3. **Scamwatch** Stop. Check. Protect.
   scamwatch.gov.au/stop-check-protect
4. **Scamwatch** Help to spot and avoid scams
   scamwatch.gov.au/stop-check-protect/help-to-spot-and-avoid-scams
5. **FTC** How to recognize and report spam text messages
   consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages
6. **FTC** Got a text about unpaid tolls? It's probably a scam (Jan 2025)
   consumer.ftc.gov/consumer-alerts/2025/01/got-text-about-unpaid-tolls-its-probably-scam
7. **FBI IC3** Smishing scam regarding debt for road toll services (Apr 12, 2024)
   ic3.gov/PSA/2024/PSA240412
8. **FCC** How to spot and avoid toll road payment scam texts
   fcc.gov/consumer-governmental-affairs/how-spot-and-avoid-toll-road-payment-scam-texts
9. **USPIS** Smishing, package tracking text scams
   uspis.gov/news/scam-article/smishing-package-tracking-text-scams
10. **FTC** Three ways scammers try to steal your money (fake fraud alerts, fake investments, fake invoices)
    consumer.ftc.gov/consumer-alerts/2024/10/three-ways-scammers-try-steal-your-money
11. **FTC** How to spot, avoid and report tech support scams
    consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams
12. **FTC** Scammers use fake emergencies to steal your money
    consumer.ftc.gov/articles/scammers-use-fake-emergencies-steal-your-money
13. **FTC** Scammers use AI to enhance their family emergency schemes (Mar 2023)
    consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes
14. **FBI IC3** Criminals use generative AI to facilitate financial fraud (Dec 3, 2024)
    ic3.gov/PSA/2024/PSA241203
15. **FCC** 'Grandparent' scams get more sophisticated (safe word tip)
    fcc.gov/consumers/scam-alert/grandparent-scams-get-more-sophisticated
16. **FTC** How to avoid an online shopping scam this holiday season (Nov 2025)
    consumer.ftc.gov/consumer-alerts/2025/11/how-avoid-online-shopping-scam-holiday-season
17. **FTC** Avoiding and reporting gift card scams
    consumer.ftc.gov/articles/avoiding-and-reporting-gift-card-scams
18. **FTC** What to know about romance scams
    consumer.ftc.gov/articles/what-know-about-romance-scams
19. **FTC** What to know about cryptocurrency and scams
    consumer.ftc.gov/articles/what-know-about-cryptocurrency-scams
20. **FTC** Job scams (warning signs and how to avoid them)
    consumer.ftc.gov/articles/job-scams
21. **FTC** What to do if you were scammed (how to try to get money back, by payment type)
    consumer.ftc.gov/articles/what-do-if-you-were-scammed
22. **IdentityTheft.gov** IdentityTheft.gov (report identity theft and get a recovery plan)
    identitytheft.gov/
23. **IdentityTheft.gov/databreach** IdentityTheft.gov data breach help (if your information was exposed but not used)
    identitytheft.gov/databreach
24. **FTC** Refund and recovery scams
    consumer.ftc.gov/articles/refund-and-recovery-scams
25. **FTC** ReportFraud.ftc.gov
    reportfraud.ftc.gov/
26. **FBI IC3** file a complaint
    ic3.gov/
27. **AARP** 877-908-3360
    aarp.org/money/scams-fraud/helpline/
28. **CFPB** Fraud and scams (resources, and help for older adults)
    consumerfinance.gov/consumer-tools/fraud/
29. **Report Fraud UK** What is Report Fraud?
    reportfraud.police.uk/what-is-report-fraud/
30. **Report Fraud UK** Report Fraud service goes live, replacing Action Fraud (Dec 4, 2025)
    reportfraud.police.uk/news/report-fraud-service-goes-live/
31. **CAFC** Report fraud and cybercrime
    antifraudcentre-centreantifraude.ca/report-signalez-eng.htm
32. **Scamwatch** Report a scam
    scamwatch.gov.au/report-a-scam

Get the latest version, free

askitsimply.com/scam-guide

General safety education, not legal or financial advice. Scams change fast: follow official sources if anything differs. Free to share; please don't sell or change it. © 2026 Ask It Simply. Written by Dontè, Ask It Simply.