scammer checker

The Family Scam Safety Guide

Eight pages to read together, and one to stick on the fridge.

From Scammer Checker · scammerchecker.com

START HERE

Pause before acting

Scams work on careful, capable people every day. They are written by professionals and tested on thousands of people until they feel convincing. Nobody is too clever or too experienced to be caught on a busy afternoon.

Almost every scam needs the same thing from you: a quick decision. So the most useful habit is a small one.

1. **Stop**
   Do not click, reply, or pay yet. Ten minutes will not hurt anything real.
2. **Check**
   Contact the person or company yourself, using a number or website you already had.
3. **Talk**
   Tell someone you trust what is going on before you do anything.

A real bank, agency, or relative will still be there after you check. Someone who punishes you for checking has told you what they are.

WHAT TO LOOK FOR

Common warning signs

The Federal Trade Commission boils scams down to four signs. Once you know them, you will see them everywhere.

1. **They pretend**
   The contact claims to be from an organization you know: a bank, a delivery company, a government office. The name and number on your caller ID can be faked.
2. **A problem or a prize**
   Your account is locked, you owe a fine, a relative is in trouble. Or you have won something and only need to pay a fee.
3. **Pressure**
   Act now. Do not hang up. Do not tell anyone. Honest organizations give you time.
4. **A specific way to pay**
   Gift cards, cryptocurrency, a wire service, a payment app, or a check you deposit and partly send back.

And three requests that are never normal

- Read me the code we just sent to your phone.
- Move your money to a safe account.
- Let me connect to your computer to fix it.

EXAMPLES

Texts and emails, marked up

Text message ILLUSTRATIVE EXAMPLE

USPS: Your parcel could not be delivered due to an incomplete address. Update within 12 hours to avoid return: hxxps://usps.parcel-redelivery.example[.]com/track

1. A 12 hour deadline. Carriers hold parcels for days.
2. Read the link from the right: the real domain is example[.]com. The word "usps" is just a label in front.
3. No tracking number you could look up yourself.

Email ILLUSTRATIVE EXAMPLE

Your streaming membership is on hold. We could not process your last payment. Update your billing details today to keep watching: hxxps://billing-update.example[.]net/login

1. A greeting with no name, and nothing about your actual plan.
2. The link does not go to the company's own domain.
3. The safe route: open the app you already have and look at your account there.

These examples are illustrations written for this guide. The links use reserved example domains and lead nowhere.

ON THE PHONE

Calls and family impersonation

Caller ID proves nothing. It can be set to show any name or number, including your bank's or a relative's.

When a caller says they are your bank or a government office

- Say you will call back, and hang up. It is not rude.
- Call the number on your card, a statement, or the official website you typed yourself.
- Courts, police, and agencies do not take payment by phone or threaten arrest on a call.

When a caller or text says they are family in trouble

- Notice the pattern: a new number, money needed today, and "please don't tell anyone".
- Call them on the number you already have. Then try someone who would know where they are.
- Ask a question only they could answer. Voices can be imitated, so a familiar voice alone is not proof.

A family phrase is a useful extra check. It is not foolproof: people forget it under stress, and it can be overheard. Use it alongside calling back, never instead.

Payment and shopping traps

How someone wants to be paid tells you a great deal. Some methods are hard or impossible to undo, which is exactly why scammers ask for them.

Stop if an unexpected contact asks for

- Gift cards, or the numbers on the back of them.
- Cryptocurrency, including a trip to a crypto ATM.
- A wire through Western Union or MoneyGram.
- A payment app transfer to someone you have not met.
- Cash or gold handed to a courier.

When buying and selling online

- Keep the chat and the payment inside the marketplace.
- An email saying "payment received" is not a payment. Open the app yourself and look.
- Never refund an overpayment. Never send money to receive money.
- A deposited check can bounce a week later, and the bank will want the money back from you.

None of these payment methods is bad in itself. Paying a friend by app is fine. The warning sign is an unexpected contact who insists on one.

FILL THIS IN TOGETHER

Our family verification plan

Write on the printed page, not on a screen. This page is yours and is not stored anywhere.

Trusted contact 1

Name

Phone (from your own contacts)

Trusted contact 2

Name

Phone (from your own contacts)

My bank's fraud line

Number copied from the back of my card

Date I checked it

Our family phrase (optional extra check)

Keep it off social media and do not text it

What we agree

- If one of us is asked for money urgently, we hang up and call back on the saved number.
- Nobody in this family will be upset about being double-checked.
- We tell each other about odd calls and messages, including the ones we nearly fell for.

IF IT HAS ALREADY HAPPENED

What to do if you already acted

It happens to people of every age and background. Acting quickly helps, and there is no shame in asking for help.

1. **Paid money**
   Contact the bank, card issuer, payment app, gift card company, or wire service you used, right now. Say it was a scam and ask them to reverse it. Refunds are not guaranteed, and asking fast gives you the best chance.
2. **Gave a password or code**
   Change that password from the real site or app, and anywhere else you use it. Turn on two-factor authentication.
3. **Shared a Social Security number**
   Go to IdentityTheft.gov for a recovery plan made for your situation.
4. **Let someone into your device**
   Disconnect from the internet, update your security software, run a scan, then change passwords from another device.
5. **Only clicked**
   If you typed nothing and installed nothing, close the page. Clicking alone rarely causes harm.

Report it at ReportFraud.ftc.gov, and internet crime at ic3.gov. Be wary of anyone who charges a fee to recover lost money. That is usually a second scam.

Where this guide comes from

FTC: How To Avoid a Scam: consumer.ftc.gov/articles/how-avoid-scam · FTC: What To Do if You Were Scammed: consumer.ftc.gov/articles/what-do-if-you-were-scammed · FTC: How To Recognize and Avoid Phishing Scams: consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams · ReportFraud.ftc.gov: reportfraud.ftc.gov · IdentityTheft.gov: www.identitytheft.gov · FBI Internet Crime Complaint Center: www.ic3.gov

CUT OUT AND KEEP

The fridge checklist

- [ ] **Was I expecting this?**
- [ ] **Are they rushing me?**
- [ ] **Do they want a code, a password, or into my computer?**
- [ ] **Do they want gift cards, crypto, a wire, or a payment app?**
- [ ] **Did they ask me to keep it secret?**

One yes is enough. Stop, hang up, and call someone on this list.

I will call

Name and number

Name and number

My bank (number from my card)