The Family Scam Defense Playbook

Protect yourself and the people you love

ZapScam · zapscam.com · Free weekly scam alerts

Set up a family code word

If anyone calls claiming to be family in trouble, the code word is the proof. No code word, no money. You can verify in 10 seconds.

1. Pick a word anyone in the family can remember but no scammer could guess. Two unrelated nouns work great. **"Acorn lighthouse"** or **"banana telescope".**
2. Tell every adult in the family — yourself, your spouse, parents, siblings, kids, grandkids. Not the dog. Real people.
3. Practice once. Have someone pretend to call you in a panic. Ask for the word. Make sure everyone remembers it.
4. Write it on paper and stick it somewhere in the house — not in a text or email. A fridge magnet, a notebook in the kitchen drawer.

Why this works

• Scammers can clone a voice with 30 seconds of audio.

• They can spoof caller ID to look like a real number.

• What they cannot do is guess a word two random family members agreed on at a kitchen table.

Five questions that stop any scam call cold

Memorize these. The scammer is reading from a script — yours just has to be better.

1. "What's our family code word?"

If they don't have it, hang up. End of test. Don't argue, don't apologize.

2. "What's the number you're calling from? I'll call you right back."

A real family member won't mind. A scammer will refuse and pile on urgency. Hang up and call them at the number you already have saved.

3. "Who's the first person we should call together — Mom, the lawyer, or your boss?"

Real emergencies have real people. Made-up emergencies cannot answer follow-up questions.

4. "What's the name of the dog / the grandkid / the restaurant we went to last week?"

Pick something only your family would know. Anything from a public Facebook post is fair game for scammers — pick something off-line.

5. "I'm going to call you back in 5 minutes."

Then hang up and call. If it was real, they'll pick up. If not, you've broken the script — and saved the money.

Red flags cheat sheet

If you see any of these, treat the message as a scam until proven otherwise. It does not matter how official it looks.

Phone

- Pressure to act in minutes.
- Gift card / wire / Zelle / crypto requested.
- "Don't tell anyone — keep it secret."
- Spoofed caller ID matching a known agency.

Email

- Sender domain looks almost right (rn for m, 0 for o).
- Generic greeting (Dear Customer, Dear User).
- Attachment you didn't expect.
- Login link in the body of the email.

Text

- Shortened or odd-domain links (.xyz, .top, .info).
- "Package undeliverable" / "unpaid toll" / "USPS update".
- Bank fraud alert with a link instead of a phone number.
- Sender is an email address, not a 10-digit number.

Web

- HTTPS lock alone doesn't mean safe — scammers have certs too.
- Pop-up that won't close, or a number to call for tech support.
- Login page that arrived from a link, not your bookmark.
- Any site asking for SSN, banking, or 2FA codes by chat.

More signals worth memorizing

These are the patterns scammers reuse across phone, email, text, and in-person.

1. **They invented the urgency.** Real agencies — IRS, Medicare, Social Security, your bank — almost never call out of the blue demanding immediate action. Anything urgent gets mailed.
2. **They picked the payment method.** Gift cards, wire transfers, crypto, and Zelle to a stranger are all scammer-preferred. Real organizations accept normal payment.
3. **They asked you to keep it secret.** The single strongest red flag. Real emergencies want family involved. Scams need isolation.
4. **The story keeps changing.** First it was a kidnapping, now it's a lawyer fee, now it's bail. Real situations don't shape-shift while you're on the phone.
5. **They knew something about you.** A name, a relative, a recent purchase. Most of that comes from breached data — it does not prove they are who they say.
6. **They told you not to use the bank's number on the back of your card.** They will always have a *different* number for you to call. Hang up. Use the number from the card.

The first 60 minutes if you or someone you love sent money

Speed matters. Some of these can claw money back. Most need to happen within an hour. Don't waste time on shame — work the list.

0–10 minutes · Stop the bleeding

1. Call your bank's fraud line — the number on the back of your card, **not one from the email or website**. Report wire / ACH / Zelle / debit and ask for an immediate freeze on the account.
2. If a gift card was used, call the card issuer right away. Apple, Google Play, Amazon, Target, Walmart — all have fraud lines. Sometimes they can refund unredeemed cards.
3. If a wire was sent, ask the bank to attempt a recall. Most wires can be reversed within 30–60 minutes if the receiving bank hasn't released the funds.
4. If your computer was accessed (remote-access scam), unplug it from the internet right now. Don't run scans yet — preserve evidence first.

10–30 minutes · Lock everything down

1. Change passwords on the email account that received the scam, your bank login, and any account you reused that password on. Use a password manager if you have one.
2. Turn on two-factor authentication everywhere it isn't on already.
3. Place a free fraud alert with one of the credit bureaus — they'll notify the other two. Equifax, Experian, or TransUnion. Takes 5 minutes.

30–60 minutes · Build the paper trail

1. File a report at **ReportFraud.ftc.gov**. Free. Generates a report number you can give to your bank, employer, or insurance.
2. If a wire or large transfer is involved, file at **ic3.gov** (the FBI's complaint center). Required for some bank reimbursements.
3. Call your local police non-emergency line and file a report. Many banks ask for a police report number before they'll process a fraud claim.
4. Save every text, email, voicemail, and screenshot. Don't delete anything. Forward scam texts to 7726 (SPAM) and scam emails to reportphishing@apwg.org.
5. Tell at least one trusted family member or friend. The shame of being scammed makes people delay — that delay is what makes the damage worse.

Print this and keep it by the phone

Print this page. Cut along the dashed line at the bottom. Stick it on the fridge, tape it next to the home phone, or fold it into a wallet.

FAMILY SCAM DEFENSE — FRIDGE CARD

If something feels off — STOP. Call your family.

OUR FAMILY CODE WORD

(write it here, then memorize it)

_____

The 5 red flags that mean it's a scam

Red flag	What it means
Asks for gift cards, wire, crypto, or Zelle	Always a scam.
Pressure to act NOW or keep it secret	Real agencies don't do this.
Caller knows your name from "the file"	Breached data, not proof.
Different phone number than the one on your card	Hang up. Use your card.
"Don't tell Mom and Dad / your spouse / your bank"	Always tell them.

Emergency contacts

Who to call	Number / site
Your bank's fraud line	______________________________
Your local police (non-emergency)	______________________________
FTC fraud reporting	ReportFraud.ftc.gov · 1-877-382-4357
FBI IC3 (online crime)	ic3.gov
AARP Fraud Watch Helpline	1-877-908-3360 (free for anyone)
Credit freeze (free)	Equifax · Experian · TransUnion

✂ -
Cut along this line and stick it on the fridge.

How to talk to your family about scams

Without anyone feeling talked down to. Works in either direction — an adult child raising it with a parent, a parent raising it with a spouse, or a grandparent raising it with the grandkids.

Lead with respect, not warning

Don't start with "you need to be careful." That puts whoever you're talking to on defense, regardless of which way the conversation is going. Start with: "Hey, can you help me figure out our family's plan if any of us gets a weird call?" You're inviting them in as a peer, not flagging them as a target.

Frame it around the family, not the person

Scammers don't pick on individuals — they pick on families. The whole point of the code word is that it protects everyone, in both directions. Anyone in the family could be the one who gets the call. Talking about it as a *shared* defense, not a *protection scheme for one person*, is what gets buy-in.

If they push back, don't argue

Common pushback: "I'd never fall for that." The right answer is not to prove them wrong — it's to flip the frame. "Of course you wouldn't. The code word is more for me. If *I* ever get a call about you in trouble, I want to know it's really you." Now they're protecting you, which is the dynamic anyone is happy to take.

Set it up while you're together

Don't try to do this over the phone — it sounds urgent and weird. Wait until you're at the same kitchen table. Bring this PDF. Pick the code word together. Take five minutes. It will be the most useful five minutes anyone in your family ever spends.

Make it routine, not a one-time talk

Bring a fresh scam example up at family dinners — "did you see this one going around?" Forward the ZapScam newsletter. Talking about scams the same way you talk about weather makes the next call easier to spot, no matter who picks up the phone.

Tools we recommend

These are the tools we use ourselves. Affiliate links — ZapScam earns a small commission at no cost to you. The recommendations are real.

Aura — Identity protection & alerts

Monitors your identity, finances, and online accounts. Alerts you in real time if your info shows up on the dark web. Includes up to $1M identity theft insurance.

aurainc.sjv.io/c/7218994/899264/12398

NordVPN — Encrypted connection & threat protection

Encrypts the data leaving your devices and blocks known phishing and malicious domains before your browser ever loads them. Single biggest technical layer for anyone who clicks a link they shouldn't have.

go.nordvpn.net/aff_c?offer_id=15&aff_id=146276

NordProtect — Identity monitoring

Watches for breaches and dark-web listings of your email, SSN, and credit data, with plain-English alerts.

go.nordprotect.net/aff_c?offer_id=973&aff_id=146276

About ZapScam

ZapScam is a free scam-research project. We run a free AI scam checker, a 100+ entry library of scam breakdowns, and a once-a-week newsletter — for anyone who wants to keep themselves and their family safe.

What you get if you subscribe

1. One scam breakdown per week — the one that's spreading right now.
2. The exact red flags to watch for, written in plain English.
3. Real numbers from the FTC, FBI IC3, and BBB. No fluff, no fear-mongering.
4. Forward-friendly so you can pass it along to anyone who needs it.

Run a message through the free checker:

zapscam.com/check

Get the weekly newsletter:

zapscam.com/subscribe

Follow on Facebook:

facebook.com/ZapScam

Stay safe. Forward this PDF to anyone who needs it.