FOR GRANDPARENTS, PARENTS AND ANYONE WITH A PHONE

The family safe word

One free habit that beats a cloned voice.

A scammer can copy a person's voice from a few seconds of audio. A video on social media is enough. Then your phone rings and it sounds exactly like your grandchild, and she's crying, and she needs money right now. This page gives you a defense that costs nothing and takes one family dinner to set up.

How the call goes

"Grandma, I've been in an accident. I need bail money. Please don't tell Mom." The panic feels real because the voice sounds real. The voice is a copy, and the grandchild is fine.

It comes in other shapes. The call may go to a parent, in a child's voice. A second voice may come on the line as a lawyer or a police officer. And the crew may send somebody to your door. In a federal case where two men were sentenced (U.S. Department of Justice, September 8, 2026), the callers posed as grandchildren in a crisis and then "arranged for rideshare drivers to pick up cash from the grandparents." (Nothing in that case involved a cloned voice. The old version of the trick still works, and the same defense stops both.)

What the record says

- The FBI recommends this exact defense: "Create a secret word or phrase with your family to verify their identity." (FBI public service announcement I-120324-PSA, December 3, 2024.)
- How little audio it takes, in the words of the American Bar Association's senior lawyers division: "With a few seconds of real audio," today's tools "can create eerily accurate voice replicas." (September 2025.)

- Cloned family voices get the headlines, and most impostors pretend to be somebody else. Of the impostor scams reported to AARP's fraud helpline in 2025, about 20,400 posed as a business or a government office and about 700 posed as family. (AARP, March 19, 2026, reporting a Microsoft study. Microsoft sells fraud detection.) So use the habits on this page for every urgent call about money, whoever it claims to be.

Set it up at the next family dinner

1. **Pick a word or short phrase nobody could look up.** No pet names, streets, schools, teams or birthdays. Odd is good. "Blue toaster waffle" is good.
2. **Say it out loud, in person.** Never text it, email it or post it.
3. **Tell everyone whose voice could be used.** Grandchildren, grown children, a brother or sister, a close friend.
4. **Practice once.** Have a grandchild call and ask you for money, and ask them for the word. A word you've used once is a word you'll remember when you're frightened.
5. **Agree on the rule.** No safe word, no money. And nobody in the family ever gets upset about being asked.

In the moment

Stay as calm as you can and say:

"I want to help you. First, tell me our safe word."

If the caller stalls, makes an excuse ("I can't remember, I'm hurt"), gets angry or hangs up, you have your answer. You just stopped a scam.

Can't remember the word yourself? Ask something only the real person would know, something that has never been online. Then hang up and call them back anyway.

Four habits that work with or without a safe word

1. **Hang up and call back** on the number you already have for that person. The number on your screen proves nothing. The Federal Trade Commission: "Scammers can make any name or number show up on your caller ID."

2. **Call one other person before any money moves.** "Don't tell anyone" is in the script because a second person ends the scam. In a Stanford, FINRA Foundation and Better Business Bureau study of 1,408 people who had reported scams, people "were more likely to be victimized if they did not have anyone to discuss the offer with."

3. **Know how scammers want to be paid.** The FTC's list is wire transfers, gift cards, cryptocurrency and payment apps, and its verdict is "Anyone who insists that you can only pay that way is a scammer." Cash handed to a driver at your door belongs on the same list. And on gift cards: "No real business or government agency will ever tell you to buy a gift card to pay them."

4. **Let the phone screen strangers.** On an iPhone: **Settings > Apps > Phone > Screen Unknown Callers > Ask Reason for Calling**. The phone asks unknown callers why they're calling before it rings. Most Android phones have a spam filter in the Phone app's settings.

If money already left

Move fast. Speed is the only thing that has ever gotten any of it back, and often it doesn't, so go in knowing the money may be gone.

- **Bank, card or payment app:** call the number on the back of your card right now and say "fraud."
- **Gift cards:** call the company on the card. Keep the card and the receipt. The FTC keeps the phone list at consumer.ftc.gov (search "gift card scams").
- **Cash in the mail:** U.S. Postal Inspection Service, 1-877-876-2455. They can sometimes stop the package.
- **Report it:** ReportFraud.ftc.gov, the FBI at ic3.gov, and your local police.

People who will pick up the phone

- **AARP Fraud Watch Network Helpline, 877-908-3360.** Monday to Friday, 8am to 8pm Eastern (6am to 6pm Mountain). Free, and you don't have to be a member. AARP says plainly what it is: "guidance and support for your situation, not investigation or case recovery."
- **National Elder Fraud Hotline, 833-372-8311.** Run by the U.S. Department of Justice for people 60 and older. Monday to Friday, 10am to 6pm Eastern (8am to 4pm Mountain).
- **In Colorado:** Stop Fraud Colorado, the Attorney General's line, 1-800-222-4444.

Watch for the second scam

People who've lost money get called again, this time by someone offering to get it back for a fee. The FBI warned on July 20, 2026 about fake agents and a copy of its own reporting website. The FBI's complaint center says it "will never directly contact you for information or money." Anyone who contacts you out of the blue offering to recover your money, for a fee, is running the next scam.

These crews are professionals and they fool smart people every day. Report it, tell your family, and you've protected the next person they call.

CUT OUT AND KEEP BY THE PHONE

Before any money moves

1. Ask for the family safe word.
2. Hang up. Call them back on the number I already have.
3. Call my person (below) before I do anything else.
4. No gift cards, no crypto machines, no wires, no cash to a driver.

My person: ______________________ **Phone:** ______________________

My bank's fraud line (from the back of my card): ______________________

> [Note: This touches on legal and financial territory. This handout is educational. If you have lost money, check your next steps with your bank and with law enforcement or a licensed professional before acting on it.]

Sources

- FBI Internet Crime Complaint Center, "Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud," alert I-120324-PSA, December 3, 2024. Checked September 17, 2026.
- U.S. Attorney's Office, Western District of Pennsylvania, "Two Dominican Republic Men Each Sentenced to Two Years in Prison for Roles in Grandparent Fraud Scheme," September 8, 2026. The release does not mention AI.
- American Bar Association Senior Lawyers Division, "The Rise of the AI-Cloned Voice Scam," Voice of Experience, September 2025.
- AARP, Sari Harrar, "AI Makes It Next to Impossible to Detect Scams. Now What?", March 19, 2026, reporting a December 2025 Microsoft AI for Good Lab analysis of AARP helpline and BBB Scam Tracker reports.
- Federal Trade Commission, Consumer Advice, "Phone Scams" and "Avoiding and Reporting Gift Card Scams." Checked September 17, 2026.
- DeLiema, Fletcher, Kieffer, Mottola, Pessanha and Trumpower, "Exposed to Scams: What Separates Victims from Non-Victims?", Stanford Center on Longevity, FINRA Investor Education Foundation and BBB Institute for Marketplace Trust, September 2019.
- Apple Support, "Manage unknown callers on iPhone," article 111106, September 14, 2026.
- FBI Internet Crime Complaint Center, alert I-072026-PSA, July 20, 2026, and ic3.gov. Helpline hours and numbers checked against AARP, the U.S. Department of Justice Office for Victims of Crime and the Colorado Attorney General on September 17, 2026.