SENIOR & FAMILY

How To Spot Grandparent Scam Phone Calls

Plain-English how-to. ~20 minutes. The exact playbook scammers use — and the family password that stops them cold.

The call usually comes between 10 PM and 2 AM. The voice is urgent, hushed, sometimes crying — and it sounds enough like a grandchild that the grandparent's heart skips. "Grandma, it's me. I'm in trouble. Please don't tell mom and dad." Within forty-five seconds the story is on the table: a car accident, a DUI in another state, a hospital, a lawyer who needs bail money wired tonight or the grandchild stays in jail. The scammer hands the phone to an accomplice playing the lawyer. The lawyer is professional, calming, and very specific about how much and where to send.

By the time the sun comes up, the money is gone. Wire transfers and gift cards don't reverse. The FBI's Internet Crime Complaint Center attributed more than $3.4 billion in losses to elder fraud in its most recent annual report, with the grandparent scam consistently in the top five tactics. The average loss per victim is in the thousands. Some lose tens of thousands in a single night.

The reason this scam works is not that older adults are gullible. It's that the script is engineered to short-circuit careful thinking. Late-night panic, a familiar-sounding voice, a request for secrecy ("don't tell mom and dad"), strict time pressure, and an unusual payment method are designed to make the grandparent skip the one phone call that would unravel everything — a call to the actual grandchild or to another family member who would know where the grandchild actually is.

AI voice cloning has made this scam dramatically more convincing in the last two years. Scammers used to rely on a vague "it sounded like him" effect, banking on a sleepy grandparent's pattern-matching. Now they only need three seconds of public audio from TikTok, YouTube, or a voicemail to clone a voice well enough to fool a parent or grandparent in a stressed phone call. The technology is cheap and improving fast. Assuming "I would recognize my own grandchild's voice" is no longer a safe defense.

Most security advice for older adults is either condescending ("just hang up on strangers!") or vague ("be careful out there"). Neither works in the moment because the moment is engineered specifically to defeat that advice. What does work is a small set of concrete habits practiced in advance: a family password every member knows, a strict "I will always call you back" rule, and a short verification script. Practiced once, these habits run automatically when the panic call lands.

By the end of this guide you'll know exactly what the scam looks like at every step, the one question that breaks it, the family password system that prevents the scam from working even when the voice is a perfect clone, and a one-page reference card you can post by the phone — yours, your parents', your grandparents'. The whole system takes thirty minutes to set up and stops a scam that costs Americans billions of dollars a year.

Quick snapshot

What you'll learn	The exact grandparent-scam script, the verification questions that break it, and a family password system that stops it cold.
Skill level	Beginner-friendly · Family-focused
Time required	30 minutes to read and set up; lifetime payoff
What you'll need	A short family meeting, a chosen 'family password', a printed reference card
Risk if you skip this	Thousands to tens of thousands lost in a single late-night call; emotional aftermath that lasts years
PDF kit	■ Download at the bottom of this page

Why this matters

The grandparent scam is the single most successful tactic against Americans over 60. The FBI's IC3 reports show consistent year-over-year growth, with the average per-victim loss in the thousands and the worst losses in the tens of thousands. AARP, the FTC, and state attorneys general all rank it among the top three frauds reported by older adults.

The cost isn't only financial. Many victims describe shame and fear afterward that lead to social withdrawal, depression, and reluctance to trust phone calls from real family members. The damage compounds. Some never recover the money; almost none recover the confidence.

Prevention works because the scam relies on a single point of failure: the grandparent making a payment before calling anyone to verify. Every successful defense in this guide breaks that point of failure. Pattern recognition, a family password, and a "call back" rule remove the scam's leverage entirely.

Before you start

Have a 30-minute family conversation. Loop in parents, grandparents, and any adult children. Everyone needs to be on the same page about the password and the verification rules — including the people who might be impersonated. The scam targets the older relative, but the younger ones are the ones whose voices get cloned.

Choose a family password together. It should be a short phrase nobody outside the family would know — not a pet's name (often on social media), not a child's middle name, not anything that appears in a public obituary. Something like "green tractor July" works well: random, memorable, three words.

Print the reference card at the bottom of this article and place it by every phone in the older adult's home. The act of glancing at the card during a stressed call is what saves them. The card is the circuit-breaker.

Step 1 — Recognize the script

The script is nearly identical every time. A panicked young voice says they're in trouble: jail, hospital, accident, abroad. They beg for secrecy: "please don't tell mom and dad." Then a second adult takes the phone — a "lawyer," "police officer," "bail bondsman," or "hospital administrator" — who is calm, official-sounding, and very specific about how much money to send and how to send it.

Knowing the script in advance is half the defense. When the call lands and matches the script you've read, the recognition itself breaks the spell. The grandparent's brain switches from **panic mode** to **pattern mode**.

Step 2 — Use the one-question test

Before saying anything substantive, ask one question only the real grandchild would know — not something they've ever posted publicly. Good: "What's the family password?" or "What did we eat at the last birthday dinner?" Bad: "What's your dog's name?" (often on Facebook) or "What high school did you go to?" (LinkedIn, obituaries).

The scammer cannot answer. They will stall, pivot, get angry, or claim the connection is bad. **Any non-answer is the answer.** Hang up.

Step 3 — Always call back on a known number

Never act on the inbound call. Hang up and call the real grandchild on the number you already have saved in your phone. If you can't reach them, call their parents. Call any other relative. Do not call any number the scammer gave you.

Scammers sometimes stay on the line silently after you "hang up" — on older landlines, the line doesn't actually disconnect until both parties hang up. If something feels off, wait a full minute or use a different phone to call out.

Step 4 — Recognize the payment red flags

The payment method gives the scam away every time. **Legitimate emergencies never require gift cards, wire transfers, cryptocurrency, or money sent via apps to strangers.** Real lawyers, hospitals, and jails do not accept Apple gift cards.

If the caller specifies an unusual payment method, that alone is sufficient to know it's a scam. Hang up.

Step 5 — Set up the family password

Pick a 2–4 word phrase together as a family. Random nouns work best: "green tractor July" or "cinnamon paper bicycle." Avoid anything findable online, on Facebook, or in obituaries.

Practice using it. Call your grandparent and ask "hey, what's our family password?" so the habit is established. The first real use shouldn't be the panic call.

Step 6 — Lock down voice-cloning sources

AI voice clones need only 3–10 seconds of audio. Limit how much of your family's voice exists publicly: tighten TikTok / Instagram privacy, avoid leaving long voicemails, and consider muting voicemail greetings that include the family name.

If you record a custom voicemail greeting, keep it short and use a generic phrase: "Hi, leave a message" instead of "Hi, this is John Smith."

Step 7 — Train the older adult on "slow it down"

Every grandparent-scam call relies on speed. Teach the rule: **any caller asking for money or claiming an emergency gets a callback, no exceptions.** Hang up, breathe, call back on a known number.

Print the reference card. Tape it to the wall next to the phone. The card removes the need to remember anything in a stressed moment.

Step 8 — Report the call

If you receive a scam call, report it: FTC at reportfraud.ftc.gov, FBI IC3 at ic3.gov, and your state's attorney general.

Reporting helps build the case against the operations behind these scams. Even small reports add up to law-enforcement action.

PRO TIP

One Password. One Callback Rule. Zero Wires.

Pick a family password tonight. Use it once a month so everyone remembers.

Every claim of emergency from a phone call gets a callback on a known number. Always.

Gift cards, wire transfers, and crypto are never used by real lawyers, hospitals, or jails.

Print the reference card. Tape it to the wall next to the phone.

If you want to go further: power-user upgrades

Power-user upgrade #1 — Set up call screening

iPhone Silence Unknown Callers (Settings → Phone) and Google Pixel Call Screen route unknown numbers to a screening prompt. Most scam calls die at the screen.

Trade-off: occasional friction with legitimate unknown callers (doctors, deliveries).

Power-user upgrade #2 — Use a designated 'family emergency' phone tree

Document a written order: who calls whom first in any real emergency. Everyone knows the order. Any call that skips the order is suspicious.

Trade-off: 15 minutes to document; needs reviewing yearly.

Power-user upgrade #3 — Add a financial 'cooling off' rule

Talk to the older adult's bank about a same-day-transfer hold or a trusted-contact alert. Many banks will flag unusual large transfers or call a designated family member.

Trade-off: occasional inconvenience for legitimate transfers.

Power-user upgrade #4 — Subscribe to a scam-alert service

AARP, FTC, and state AG offices send free scam alerts. Forward them to family group chats so everyone stays current on emerging tactics.

Trade-off: occasional email.

Power-user upgrade #5 — Practice the scam with the family

Once a year, role-play a fake panic call so everyone — including the older adult — practices the response. Practice converts knowledge into reflex.

Trade-off: feels awkward; works.

Power-user upgrade #6 — Lock down the older adult's social media

Make Facebook friends-only, remove birthday year, scrub family photos publicly visible. Less public information means less material for impersonation.

Trade-off: 30 minutes of profile review per year.

Common mistakes & pitfalls

Mistake — Mistake

Fix — Believing the voice. AI cloning means voices alone are no longer proof of identity. Always verify with the password or a callback.

Mistake — Mistake

Fix — Following the 'don't tell mom and dad' instruction. That instruction is the scammer protecting their window. Always tell mom and dad.

Mistake — Mistake

Fix — Sending gift cards or wires before verifying. By the time you've sent, the money is unrecoverable.

Mistake — Mistake

Fix — Calling back the number the scammer gave you. Always use a known number from your own contacts.

Mistake — Mistake

Fix — Trusting caller ID. Numbers are trivially spoofed; caller ID is not verification.

Mistake — Mistake

Fix — Skipping the family password because 'we'd know.' You wouldn't, in the moment, with a perfect AI clone.

Pro tips

Pro tip 1. Post the reference card by every phone in the older adult's home.

Pro tip 2. Make the family password a phrase, not a single word — harder to guess, easier to remember.

Pro tip 3. If you can't reach the supposed caller, call a sibling, cousin, or any other relative for a sanity check before doing anything.

Pro tip 4. Real emergencies don't require secrecy. "Don't tell anyone" is a scammer's tell.

Pro tip 5. Banks, hospitals, and lawyers all have callback verification protocols. Use them.

Frequently asked questions

What if the voice really does sound exactly like my grandchild?

It can. AI voice clones from 3–10 seconds of public audio are convincingly accurate. Trust the password, not the voice.

Should I tell the scammer I know it's a scam?

No. Hang up. Engaging gives them information about what works and what doesn't, and marks you as a willing target for future calls.

What if my grandchild really is in trouble?

Hang up and call them on a known number. If they're really in jail or the hospital, you'll reach them or their actual contacts.

What about email versions of this scam?

Same playbook, same defense: don't reply, call the real person on a known number. Email and SMS variants are increasingly common.

Do I need to report the call?

Yes — FTC, FBI IC3, and your state AG. It takes 5 minutes and helps build the case against these operations.

Can I get the money back if I already sent it?

Wire transfers and gift cards almost never reverse. Bank-to-bank transfers sometimes can be recalled within hours if you act fast. Call your bank immediately.

What if the scammer threatens me with police if I don't pay?

Real police don't call demanding money over the phone. Hang up and call your local police non-emergency line if you're worried.

Quick recap — do these in order

DO THIS RIGHT NOW

The 8-step recap.

Pick a 3-word family password tonight; share with every adult relative.

Print the reference card. Tape it to the wall next to every phone.

Save the real number of every grandchild in the older adult's contacts.

Practice the password once a month so the muscle memory holds.

Set up Silence Unknown Callers or Call Screen on the older adult's phone.

Talk to the bank about trusted-contact alerts on large transfers.

Report any scam calls received to the FTC and FBI IC3.

Re-do this whole process annually. The scams evolve; your defenses should too.

Mini glossary

Grandparent scam: Impersonation scam targeting older adults via late-night panic call from a fake grandchild.

Voice cloning: AI generation of a near-identical copy of someone's voice from a few seconds of audio.

Family password: A pre-arranged phrase used to verify a caller's identity during a stressed call.

Wire transfer: Bank-to-bank money transfer; effectively irreversible once sent.

Gift-card scam: Any request for payment via gift cards, especially from authority figures, is a scam.

Trusted contact: A designated family member your bank can alert if it suspects fraud.

Spoofed caller ID: A faked phone number on caller ID; trivially done by scammers.