Protecting Your Parent from Scams: What Actually Works

There's a particular kind of dread that comes with the phone call that starts, "Mom, why did you send someone $3,000 in gift cards?" It's not just about the money. It's the realization that someone — a stranger, or worse, someone posing as family — reached right into your parent's home and their trust, and took advantage of both.

If you're worried about this, you're not overreacting, and you're not alone. Scammers target older adults deliberately, and the tactics have gotten more convincing, not less. The good news is that a handful of concrete steps can meaningfully lower the risk — and none of them require taking away your parent's independence.

Why older adults are targeted

It isn't that older adults are less capable. Research funded by the National Institute on Aging (NIA) found that a meaningful share of older adults — including many with no cognitive impairment at all — engaged with a simulated scam without suspicion. Scammers know this, and they also know something else: older adults are less likely to report fraud when it happens, often out of embarrassment. That combination — a plausible-sounding scammer and a victim who may stay quiet afterward — is exactly what makes this population a target. If your parent has ever fallen for something and hasn't told you, that silence is common, not shameful.

The scams showing up most often

A few patterns account for the majority of cases the NIA and AARP see reported:

The grandparent scam. A caller claims to be a grandchild in trouble — arrested, hospitalized, stranded — and begs for money to be wired or sent via gift cards immediately, often asking the grandparent not to tell anyone else in the family. The urgency and secrecy are the tell.

Government impersonator scams. Someone claiming to be from the IRS, Social Security Administration, or Medicare says there's a problem with an account and asks for personal information or payment to fix it. Real government agencies don't operate this way over the phone.

Fake prize and lottery scams. Your parent is told they've won something, but first need to pay a fee or "release tax" to collect it.

Tech support scams. A pop-up or phone call warns that the computer has been compromised and offers to fix it — for a price, and often with remote access to the device.

Fake charity requests, which spike around the holidays and after natural disasters, when people are primed to want to help.

What almost all of these share: an unexpected contact, a rush of emotion, and pressure to act *right now*. AARP's Fraud Watch Network calls this combination the moment to take an "active pause" — stop, hang up, and call a family member or the actual institution directly using a number you look up yourself, not one the caller provides.

What you can actually do

You don't need to monitor your parent's every move to meaningfully lower their risk. A few specific steps go a long way:

Set up bank and credit card alerts. Most banks let you turn on text or email alerts for withdrawals, transfers, or purchases over a certain amount. This is one of the simplest ways to catch something unusual quickly, and your parent doesn't have to give up control of the account to do it.

Ask to be added as a "trusted contact." Many banks and investment firms let account holders name a trusted contact — separate from having any access to the money — who the institution can call if they notice suspicious activity. It's a low-friction way to create a safety net without changing who controls the account.

Have the conversation before there's a crisis. It's far easier to talk about scams in a calm moment than after money is already gone. Frame it as something you're doing together, not something you're doing *to* them — "I read about a scam going around and wanted to check in" lands very differently than "I'm worried you can't handle this anymore."

Agree on a family code word or plan. If the grandparent scam relies on urgency and isolation, a simple rule like "we always call each other back on a known number before sending money" removes the scammer's leverage entirely.

Protect their information proactively. Shredding documents with account numbers, freezing credit if it's not actively being used, and being cautious about what's shared on social media (birthdates, upcoming travel, family names) all reduce the raw material scammers use to sound convincing.

Is a Power of Attorney enough protection?

This is one of the questions we hear most, and the honest answer is: it helps, but it isn't a safety net by itself — and it isn't automatic.

A financial power of attorney lets your parent name someone they trust to manage money and property if they're ever unable to do so themselves. Done well, it's one of the most valuable protections a family can put in place. But a few things matter more than simply having the document:

- **The agent has to actually be trustworthy.** This sounds obvious, but financial regulators specifically flag power of attorney as a tool that can be *misused* by the very person entrusted with it — most often, sadly, a family member. Naming someone should be a decision your parent makes deliberately, not by default because they're the oldest child or live closest.
- **It only works if it's in place *before* it's needed.** A POA can't be created once your parent no longer has the capacity to sign one. This is why the conversation is worth having early, even when everyone still feels far from needing it.
- **It doesn't replace day-to-day vigilance.** A POA gives someone the legal authority to step in — it doesn't automatically catch a scam in progress. Pairing it with the practical steps above (alerts, trusted contact status, open conversation) is what actually closes the gap.

If your family is considering this step, an elder law attorney can help build in safeguards — like requiring a doctor's confirmation of incapacity before the POA becomes active, or naming a second person to review the agent's actions — so the document protects your parent rather than simply transferring risk to someone else.

If something has already happened

If you think your parent has been targeted or scammed, the most important thing you can do is respond without shame or panic — for their sake and yours. Report it to the **National Elder Fraud Hotline at 833-372-8311**, contact your bank if money was involved, and consider reporting to the Federal Trade Commission. AARP's Fraud Watch Network Helpline (877-908-3360) also offers free support and can help you figure out next steps, including emotional support groups for families going through this.

There's no shame in any of this — not for your parent, and not for you. Scammers are professionals at what they do. Catching it, reporting it, and putting better guardrails in place afterward is what protecting your family actually looks like.

This article is for general education and isn't a substitute for legal or financial advice specific to your family's situation. For help building a plan that fits your parents' needs, an elder law attorney or financial advisor familiar with elder protections can help.

Sources: National Institute on Aging (nia.nih.gov), AARP Fraud Watch Network (aarp.org), Consumer Financial Protection Bureau (consumerfinance.gov)