Larson Gross

Protecting Your Parents from Financial Scams

Financial scams targeting older adults move billions of dollars every year, and the tactics keep getting more convincing. If you have a parent who isn't especially tech savvy, the odds are good they've already been targeted, even if they haven't told you. Today, I'll walk through the four scam patterns that show up most often and the specific steps you can take to protect your parents even if a convincing call gets through.

The patterns your parents need to recognize

Let's start with the patterns themselves, because four of them repeat in nearly every case we see.

The first is impersonation. Someone calls claiming to be the IRS, the bank's fraud department, or even a grandchild in trouble. They often already know small details about the family, which makes the call feel real.

The second is urgency paired with secrecy. Your parent is told to act immediately and not tell anyone, not even you. That combination is the biggest red flag in the playbook. Legitimate institutions don't ask people to keep them secret.

The third is the payment method. Gift cards, wire transfers, cryptocurrency, and payment apps like Zelle show up in nearly every successful scam, because money sent those ways is almost impossible to get back. If anyone asks for those, the call should end.

The fourth is a request for remote access to the computer. The caller asks your parent to install a program to fix a problem or verify an account. Once that program is running, they can see everything on the screen, including bank logins. No legitimate company asks for that kind of access on an unsolicited call.

Here’s how these pieces fit together. The phone rings, and it sounds exactly like a grandchild. Scammers can now clone a voice with AI from just a few seconds of social media audio. The voice says they’ve been arrested, they need $3,000 right away, and please don’t tell my parents. Every part of that call is designed to stop your parent from pausing to check the story.

The best defense against that call is simple. Agree on a family code word ahead of time. If a caller claiming to be family can’t say it, your parent should hang up.

Two more things are worth mentioning here. These same tactics show up in texts and emails, not just phone calls. A common one mimics a delivery notice with a link to fix a package problem, and the link leads to a fake site that collects personal information. The rule is simple. Don’t click links in unsolicited messages, even when the sender looks familiar. Type the company’s web address yourself.

And watch for the second wave. Once someone has been scammed, they often hear from a new caller posing as a recovery specialist who can get the money back for an upfront fee. That call deserves the same skepticism as the original, not less.

What you can help set up

Now let’s talk about the safeguards you can help put in place, because the conversation is only one layer of protection.

Start with the basics. Help them set strong, unique passwords for their financial accounts and turn on two-factor authentication, where a code is texted to their phone before a login goes through. Text codes aren’t the most sophisticated option, but they’re the most manageable, and they stop most unauthorized logins.

Next, set up credit monitoring. If someone uses stolen information to open an account in your parents’ name, monitoring across all three credit bureaus catches it early. Several services offer this at no cost, and their bank or credit card may already include it.

They can go a step further by placing a credit freeze with each of the three bureaus. A freeze doesn't affect existing accounts or credit scores, but it blocks anyone from opening new credit in your parents' name. It costs nothing, and it can be lifted any time they need to apply for something.

Then ask their bank about a trusted contact designation. A trusted contact is simply someone the institution can call if they notice something unusual. That person can't make transactions or touch the money, which is what makes this different from a cosigner. If the bank doesn't offer it, ask whether you can receive copies of transaction alerts instead.

Speaking of alerts, make sure they're turned on for any transfer above a threshold that fits your parent's normal spending. A text when a large wire goes out creates a window to catch a problem in minutes rather than weeks.

If your parents' accounts are held in a trust, ask whether the institution can require dual approval for large transfers. With dual approval, one person can initiate a transfer, but a second person must approve it before the money moves. Availability varies by institution, so confirm it's actually built into the account agreement.

Finally, set a regular time to review statements together. Patterns that a single alert might miss tend to show up when someone looks at the account history with fresh eyes.

The bottom line

If you're not sure where to begin, start with the conversation. Walk your parents through the four patterns: impersonation, urgency with secrecy, irreversible payments, and remote access requests. Make sure they know to hang up and call back using a number from a statement or the official website, never a number the caller provides. Then work through the setup: two-factor authentication, credit monitoring, a trusted contact, and transaction alerts. The goal isn't to make your parents feel watched. It's to make sure that if a convincing call ever gets through, the structure limits how much damage it can do.

Next Step

And if a scam does succeed, act fast. Call the bank right away, and report it to the Federal Trade Commission at ReportFraud.ftc.gov. Quick reporting is the best chance of limiting the loss.

If you have questions or would like to discuss your unique situation, please contact our office to speak with one of our expert advisors.

About Larson Gross

Ted Larson and Dennis Gross founded our firm in 1949. They built the business based on excellence, passion, integrity, trust and pro-action — values still important to us more than seven decades later.

Even well into their retirement years, Ted Larson and Dennis Gross continued to have the best interest of the firm at heart. Mr. Larson would come into the office on a regular basis to meet every new face and make a personal connection with each of our team members. He remembered the name of every employee, as well as the names of their spouses and children, and would greet clients by name as he passed by the reception desk. Sometimes, you'd even find a newspaper clipping on your desk that Mr. Larson dropped off, highlighting that your son made the honor roll. This is the example of a genuine relationship we strive to embody with our people and clients.

Today, we're led by ten partners who are growing our firm with respect for where we've come from and a new vision for future success. Our 120-plus team members and three offices located in Bellingham, Lynden and Burlington make us the 10th largest public accounting firm in the Puget Sound region. While we're determined to expand our impact and help strengthen as many businesses and individuals as we can, we're also committed to remaining a locally-owned organization. We're incredibly proud of where we've come from and look forward to a future of possibility

Larson Gross
2211 Rimland Dr.
Suite 422
Bellingham, WA 98226

(800) 447-0177

contact@larsongross.com

https://larsongross.com