



Defending Your Nest Egg from Elder Financial Fraud

October marks Cybersecurity Awareness Month, and for retirees and near-retirees, that awareness matters more than most people realize. Scammers increasingly target older adults because they tend to have more savings and, unfortunately, are seen as easier targets. Last year, Americans age 60 and older filed more than 201,000 fraud complaints with the FBI's Internet Crime Complaint Center, reporting losses of \$7.7 billion. That's a 59% jump from the year before, and the average loss per victim topped \$38,500.¹ These aren't small numbers, and they're not slowing down.

Investment Scams Are the Biggest Threat

Of all the tactics scammers use, fake investment opportunities cause the most financial damage to older adults, accounting for roughly 45% of all elder fraud losses reported last year.² Many of these schemes start on social media or dating apps, where a stranger builds trust over weeks or months before introducing a "can't miss" cryptocurrency platform. The pitch usually promises unusually high, guaranteed-sounding returns, and the platform itself often looks polished and legitimate, complete with fake account dashboards showing rising balances. By the time a victim tries to withdraw funds, the platform disappears, along with the money. If someone you've never met in person is urging you to move money into an unfamiliar platform, treat that as a signal to slow down and call your financial professional before doing anything else.

Tech Support Scams Are a Growing Problem

Investment fraud gets the headlines, but tech support scams quietly crossed the billion-dollar mark last year, with reported losses of \$1.041 billion.² These scams typically start with a pop-up warning on your computer screen, or an unexpected call from someone claiming to be from Microsoft, Apple, or your bank's fraud department. The caller says your device or account has been compromised and asks for remote access to "fix" the problem. Once granted, that access can be used to view your accounts, install malicious software, or transfer money directly. Reputable companies generally do not request remote control of your device without a prior service interaction, so unexpected requests should be treated as an immediate red flag.

Watch for AI-Powered Scams

Technology has given scammers new tools. Voice cloning software can now mimic a family member's voice convincingly enough to appear that a loved one is in trouble and needs money wired immediately. The FBI logged more than 3,100 elder fraud complaints referencing AI-related tactics last year, with losses exceeding \$352 million.³ If you get a distressing call from someone claiming to be family, hang up and call that person back directly using a number you already have saved, rather than one provided by the caller.

A Few Habits Go a Long Way

You don't need to become a tech expert to protect yourself. Simple habits, such as verifying requests through a second channel, avoiding sharing account numbers over the phone, and taking the time to confirm unusual requests can help reduce exposure to common scam tactics. It also helps to loop in a spouse, adult child, or trusted friend on any request that feels rushed or unusual. A second set of eyes may notice details that are easy to overlook when a situation feels urgent.

Staying alert doesn't mean living in fear. It means building a few pauses into your routine so a moment of pressure doesn't turn into a costly mistake.

To learn more about protecting your finances from fraud, contact the office to schedule a time to talk.



¹Federal Bureau of Investigation. "Elder Fraud Report." 2026, IC3.gov, https://www.ic3.gov/Outreach/Brochures/elder_fraud_tri-fold.pdf.

²HCSK. "Elder Fraud Statistics 2026: FBI IC3 + FTC Data." 2026, seniors.hcsk.org, <https://seniors.hcsk.org/elder-fraud-statistics-research/>.

³Delozier, Jonathan. "FBI: Seniors lost \$7.75B to cybercrime in 2025." 13 APR 2026, HousingWire, <https://www.housingwire.com/articles/fbi-seniors-cybercrime-2025/>.

Tech Habits for a Safer Retirement

Most scams succeed not because people aren't smart, but because a handful of small habits were never in place. Here are a few worth building into your routine.

- **Lock down your passwords.** Use a different password for every financial account, and consider a password manager so you're not stuck memorizing a dozen combinations.
- **Turn on two-factor authentication.** This adds a second step, usually a text code, when you or anyone else tries to log into your accounts.
- **Update your devices regularly.** Those software update notifications you keep dismissing often contain security fixes.
- **Hang up and call back.** If someone calls claiming to be your bank, the IRS, or a family member in distress, hang up and dial a number you already trust.
- **Never give remote access.** No legitimate company will ask to take control of your computer to "fix" a problem you didn't report.
- **Check your accounts weekly.** Regularly reviewing your accounts may help you identify unfamiliar charges before they snowball.
- **Talk about it.** Tell your kids or a trusted friend when something feels off. A second opinion can catch what you might miss.

The opinions expressed and material provided are for general information and should not be considered a solicitation for the purchase or sale of any security. The content is developed from sources believed to be providing accurate information.

Cetera Financial Group (Cetera) is a network of independent retail firms, including those that are members of FINRA/SIPC: Cetera Advisors LLC; Cetera Wealth Services, LLC (formerly known as Cetera Advisor Networks); Cetera Investment Services LLC (marketed as Cetera Financial Institutions or Cetera Investors); and Cetera Financial Specialists LLC. Entities registered as investment advisers with the Securities and Exchange Commission include Cetera Investment Management LLC and Cetera Investment Advisers LLC. Cetera's principal office is located at 655 W. Broadway, 11th Floor, San Diego, CA 92101.

Avantax Planning Partners, Inc. is an SEC registered investment adviser within the Aretec Group, Inc. (dba Cetera Holdings, an affiliate of Cetera). All the referenced entities are under common ownership.

Individuals affiliated with Cetera firms are either Registered Representatives who offer only brokerage services and receive transaction-based compensation (commissions), Investment Adviser Representatives who offer only investment advisory services and receive fees based on assets, or both Registered Representatives and Investment Adviser Representatives, who can offer both types of services.

This communication is designed to provide accurate and authoritative information on the subjects covered. It is not, however, intended to provide specific legal, tax, or other professional advice. For specific professional assistance, the services of an appropriate professional should be sought. For a comprehensive review of your personal situation, always consult with a tax or legal advisor. Neither Cetera firms nor any of its representatives may give legal or tax advice.