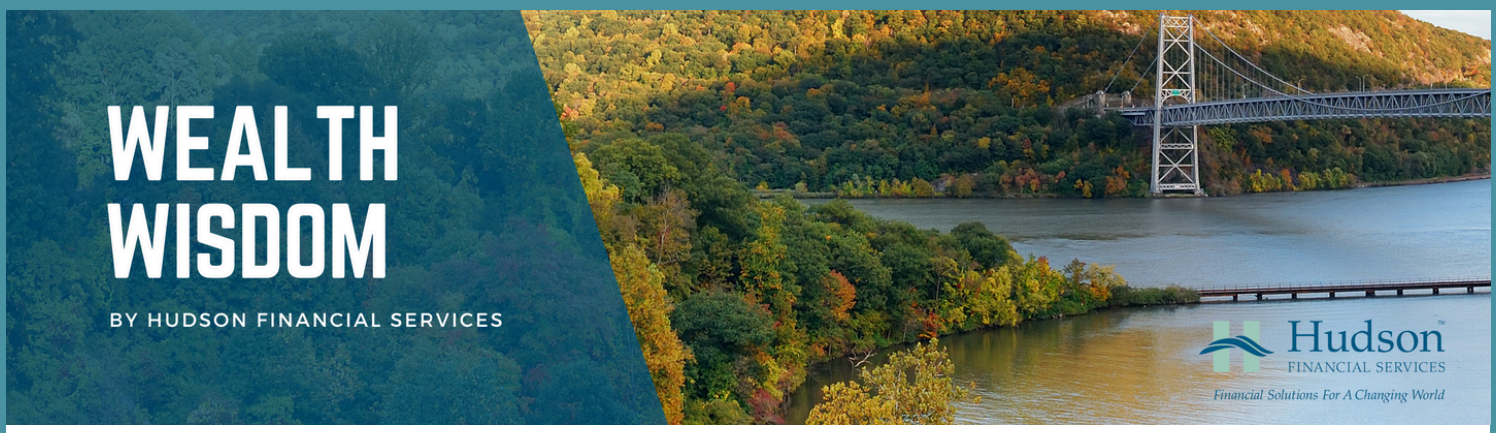


October 1, 2025

A 2025 Guide to Protecting Seniors from Fraud

If you've found yourself stepping into a more active role in your parents' financial lives, you're not alone.

Some of us are helping aging parents navigate everything from healthcare decisions to bill payments—and increasingly, we're also their first line of defense against financial scams.

Fraudsters are getting more sophisticated, and unfortunately, older adults are being targeted more than ever. Whether it's phishing texts, fake tech support calls, or convincing-looking emails, these scams are designed to exploit trust, isolation, and confusion. And they're working; according to the Federal Bureau of Investigation (FBI), losses among older Americans are rising fast.

That's why we've pulled together some practical steps you can take now to help protect the older adults in your life. While we're not cybersecurity experts, we believe understanding these threats is part of protecting the people and personal finances that matter most.

In this blog, we will outline what to watch for and how to help your family and friends feel more confident in spotting red flags before it's too late.

How Big Is the Problem?

In 2024, consumers lost more than a trillion dollars to scams worldwide, according to the Global Anti-Scam Alliance. Over half of all consumers reported encountering fraudsters at least once a week![1]

A recent study found that two out of five seniors (over the age of 60) have fallen victim to some scam. While 37 percent of seniors were victims, 73 percent reported knowing someone who was. Of those scammed, 49 percent reported losing money. The average amount lost was $3,590.[2]

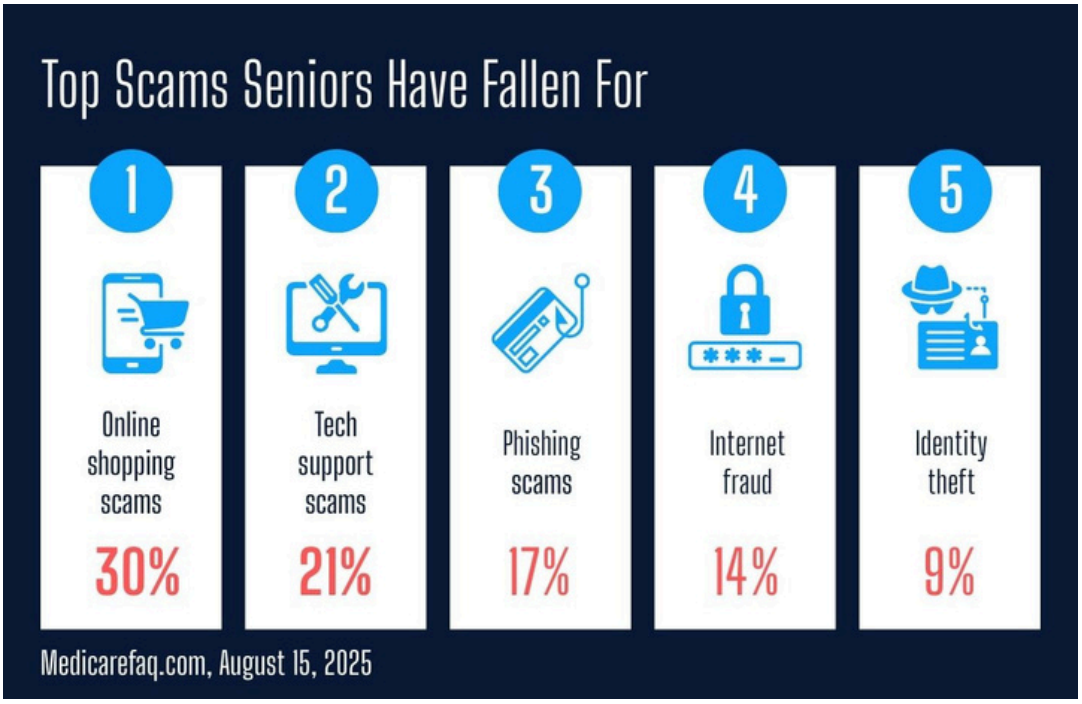
Identity theft involving sensitive, personally identifiable information such as Social Security numbers can have long-lasting effects. Thieves may wait months or even years to use the information, or they might sell it on the dark web, requiring you to stay vigilant indefinitely. Legal fees and other costs could add to the financial

impact if the identity theft issue is complex. Some victims even need to seek government assistance during recovery, highlighting the potential magnitude of identity theft hardships.

While there may be considerable inconvenience and real financial ramifications to fraud, there is also a psychological impact, including feelings of shame, safety concerns, and worries about lost independence.

What Scams Are Working the Best?

Some of the scams senior citizens have fallen victim to include online shopping scams, tech support scams, phishing scams, internet fraud, and identity theft.[1]



1. **Online shopping scams** occur when cybercriminals portray themselves online as legitimate sellers of services or merchandise to steal personal information or money. They create fake websites that look genuine or impersonate legitimate retailers. Other cybercriminals will create fake accounts on well-established online marketplaces and sell items that are "too good to be true."[3]

   Consider the following information:[3]

   - Avoid clicking on suspicious links from unsolicited messages or questionable social media ads. To be careful, type in the URL instead of clicking on search results or unsolicited messages.

   - Use a credit card over a debit card because credit cards are more secure and may provide better fraud protection if a scam occurs.

   - Only shop on reputable websites, avoiding sites with discrepancies, poor reviews, and unrealistic offers.

   - Help manage financial accounts by using strong and unique passwords for each, enabling Multi-Factor Authentication (MFA), setting up financial alerts, and creating accounts with reputable retailers.

2. **Tech support scams** can begin with a pop-up message featuring a logo from a well-known tech company, claiming that your computer has a virus and instructing you to click a link or call a supposed support number. Criminals request remote access to your computer, where they can access all of your data and install malware. These scammers may also try to sell useless software, maintenance, or warranty programs.[4]

AARP notes that consumers aged 60 and older are five times more likely than their younger counterparts to lose money to tech support scams, which cost older Americans more than $175 million in 2023, the Federal Trade Commission (FTC) reported in October 2024.[4]

Remember that legitimate technology providers don't call, email, or text about computer problems and won't ask you to make a call or click a link. The FTC states that if a supposed tech support person calls unexpectedly, be skeptical. So, if this should happen, hang up the phone, avoid clicking on pop-ups, refuse remote access, and never share your password.[4]

3. **Phishing scams** are a broad term for cybercrimes in which targets are contacted by email, telephone, or text message by someone posing as a legitimate person or institution. Victims are then lured into providing sensitive data such as identity details, banking and credit card numbers, and passwords. The information is then used to access accounts and can result in identity theft and financial loss.

While phishing can be targeted at anyone, seniors should be on the lookout for some specific elderly scams, including the following:5

- **Medicare/Health Insurance Scams -** Fraudsters pose as Medicare representatives to steal personal information or offer fake services. Don't give out your Medicare numbers to anyone suspicious and never pay for services not received.

- **Grandparent Scams -** A caller pretends to be a grandchild in trouble (e.g., in jail or injured) and asks you to send money urgently. The criminal will usually insist on secrecy and ask for wire transfers or gift cards.

- **Sweepstakes/Lottery Scams -** Individuals are contacted and informed that they've won a prize but must pay fees upfront to claim it. Again, hang up the phone, discard the letter, and/or delete the email.

- **IRS or Government Impersonation Scams -** Some scammers attempt to intimidate older individuals by pretending to be from the IRS or another government agency and demanding immediate payment, threatening jail time if payment is not made. Know that the government will never use high-pressure tactics and threats over the phone or by email.

- **Charity Scams -** Fake charities can deceive people by soliciting donations. This can happen especially after highly publicized natural disasters. Caution your family to stick with charities they know and trust and avoid those that have vague missions, pressure them to donate immediately, or refuse to provide documentation.

- **Financial services scammers -** use various methods, including calls, texts, and email messages, to impersonate legitimate banks, mortgage companies, or debt collectors. They may claim that a checking or savings account has been compromised and ask for personal information, such as passwords or Social Security numbers, to resolve the issue. They may even threaten arrest for unpaid bills.[6]

Technology and Artificial Intelligence Make Scamming Easier

Technology has made scams more commonplace, enabling fraudsters to create increasingly sophisticated digital scams. Bad actors don't even need to be tech professionals to develop large-scale cyber-fraud operations. Innovative tools can be used to easily generate millions of highly convincing emails, text messages, and websites that can successfully trick even the most careful individuals.2 If they can fool the digital natives out there, think what they can pull on your family.

Artificial intelligence scams are on the rise, with AI-enabled tools capable of targeting consumers in highly sophisticated and personalized ways. Some of the latest AI scams include **voice cloning, deepfake scams, and phishing email attacks.**[7]

Unlike traditional scams, which employ more generic tactics, AI enables criminals to create websites, emails, and impersonations that appear, feel, and sound incredibly authentic and believable. Leveraging AI, scammers can quickly, easily, and cheaply launch large-scale fraud campaigns or target specific people using information gathered from social media or other platforms.

The FBI has warned that AI scams are on the rise, saying, “as technology continues to evolve, so do cybercriminals' tactics.”[7]

Here are a few of the latest **AI scams**:[7]

- **Voice cloning**. AI can be used to clone a person's voice using just a short audio sample. Voice cloning is often used in scams where the fraudster impersonates a family member in trouble or financial distress who urgently needs money sent to them. As you can imagine, this can be especially effective on older adults.

- **Deepfake scams**. Deepfake technology utilizes AI to create realistic videos, photos, and audio clips that appear to depict someone saying or doing something they didn't. This technology is being used to impersonate public figures or celebrities to promote fraudulent products or persuade consumers to take specific actions. Deepfakes are becoming increasingly sophisticated, exacerbating this growing problem throughout society.

- **Phishing email attacks**. While phishing emails to steal personal information have been around for a while, AI has allowed crooks to ramp up the deception. An article from the May 2024 issue of the Harvard Business Review says, “With AI, scammers can generate very authentic phishing emails that bypass spam filters. These emails often appear to be genuine account notifications or urgent requests from reputable companies. What's more, their content is often very personalized.”

Many Scams Go Unreported

Many people don't report scams, making these crimes hard to prosecute and even harder to get reliable statistics. Elderly victims may also be too embarrassed to admit they were taken advantage of, even to family members. Others don't know where to turn to report the crime. The bad guys know this and consider elderly people "low risk." By discussing the risks of scams with your family, you can help remove the stigma and equip them with the tools to better manage cyber threats.[1]

Actions to Protect Your Family

You can take several steps to help your family manage attempted scams. Some involve technology, while others are low tech and require a conversation and perhaps a slight adjustment in habits.

- Make sure they know to confirm any request or message before acting, especially if it's unexpected or unusual. If someone claims to be a relative or authority figure looking for immediate cash, have them call you or another trusted source who can confirm if it is a legitimate request.

- An effective way to avoid theft is to have your family create different passwords for their accounts and change them frequently. Many people use the same password for multiple accounts and fail to update it, which can be problematic.

- Install trusted security technology on your family's devices, such as antivirus software or other tools that help protect against phishing scams, deepfakes, and spam text messages. Other options include password managers, identity theft protection, virtual personal networks, and two-factor authentication on devices and accounts.

- Caution your family about sharing too many personal details online. Scammers can use any information you provide to personalize their attacks.

- Review your credit card and bank statements to spot any suspicious activity.

- Consider freezing all of your family's credit files so no one can look at or request their credit report, open an account, apply for a loan, or get a new credit card while their credit is frozen.

- Another way to protect against scams is to register your family's numbers on the National Do Not Call Registry. This should decrease the unsolicited calls they receive, potentially lowering the risk of falling victim to phone scams.

- Your bank accounts should have automatic fraud prevention and detection tools to alert you if they identify a fraud attempt. Online banking notifications are one of the fastest ways to receive these alerts. If your family hasn't already, you can help them set up their online bank accounts.

- Consider adding a "trusted contact" to your family's investment accounts. This is a person whom the financial institution is authorized to contact if there is a concern about fraudulent activity in the account. A trusted contact may be a family member or another trusted third party. A trusted contact provides an additional layer of safety on your family's accounts and puts your financial firm in a better position to help manage your accounts.[8]

We Are Here for You

By implementing these preventive measures and staying vigilant, you can help your family manage the risk of becoming a victim of increasingly sophisticated and persistent criminals.

If you have additional questions or concerns, please do not hesitate to contact us.

Sources

1 Medicarefaq.com. May 20, 2024
https://www.google.com/url?q=https://www.medicarefaq.com/blog/senior-citizen-scam-statistics/%234&sa=D&source=editors&ust=1758746132294083&usg=AOvVaw0YqgLmoNtm6tJFiJfwZJdy

2 Forbes, March 18, 2025
https://www.google.com/url?q=https://www.forbes.com/sites/mastercard/2025/03/18/scams-in-the-digital-era-how-technology-is-changing-fraud/&sa=D&source=editors&ust=1758746132294919&usg=AOvVaw0TclchRJ9wGkiJkANGMf0b

3 Keeper, January 08, 2024
https://www.keepersecurity.com/blog/2024/01/08/what-to-do-if-you-get-scammed-while-shopping-online/

4 AARP, December 16, 2024
https://www.aarp.org/money/scams-fraud/biggest-scams-2025/?cmp=AEBOV2C44X&gclid=7514ebeda34614b2c6c083a2a06fc8e4&gclsrc=3p.ds&msclkid=7514ebeda34614b2c6c083a2a06fc8e4&utm_source=bing&utm_medium=cpc&utm_campaign=Fraud-TopScams-NonBrand-Exact&utm_term=tech%20support%20scams&utm_content=Tech%20Scams

5 Consumer Affairs, June 11, 2025
https://www.consumeraffairs.com/news/the-top-10-scams-that-target-seniors-061125.html

6 National Council on Aging, February 20, 2025
https://www.ncoa.org/article/top-5-financial-scams-targeting-older-adults/

7 National Council On Aging, October 31, 2024
https://www.ncoa.org/article/what-are-ai-scams-a-guide-for-older-adults/

8 NASAA, June 2025
https://www.nasaa.org/investor-education/investor-library/trusted-contact/

Disclosures

Kathryn Palao and Joseph Passaniti are Investment Advisor Representatives offering securities and advisory services through Cetera Advisor Networks LLC, member FINRA/SIPC, a broker/dealer and Registered Investment Advisor. Cetera is under separate ownership from any other named entity. Tax planning services offered through Hudson Tax Services, LLC.

The views stated in this piece are not necessarily the opinion of Cetera Advisor Networks LLC and should not be construed directly or indirectly as an offer to buy or sell any securities. Due to volatility within the markets mentioned, opinions are subject to change without notice. Information is based on sources believed to be reliable; however, their accuracy or completeness cannot be guaranteed. Past performance does not guarantee future results. All investing involves risk, including the possible loss of principal. There is no assurance that any investment strategy will be successful. Investors cannot invest directly in indexes. The performance of any index is not indicative of the performance of any investment and does not consider the effects of inflation and the fees and expenses associated with investing. The S&P 500 is a capitalization-weighted index of 500 stocks designed to measure performance of the broad domestic economy through changes in the aggregate market value of 500 stocks representing all major industries.

Cetera does not offer direct investments in gold/silver or other commodities. Commodities are volatile investments and may not be suitable for all investors.

A diversified portfolio does not assure a profit or protect against loss in a declining market.

For a comprehensive review of your personal situation, always consult your legal advisor. Neither Cetera Advisor Networks, LLC nor any of its representatives may give legal advice.

Rebalancing may be a taxable event. Before you take any specific action be sure to consult with your tax professional.