Mesirow

Be safe out there

How to protect yourself from online financial theft

Online scams are nothing new. But with the advent of AI and new sophisticated techniques being employed by scammers, they are becoming more widespread and harder to spot. Total losses reported to IC3 by elderly victims increased 11% from 2022, with victims losing an average of $33,915.[1] But it's not just the elderly who are vulnerable. Any investor can become a victim regardless of age.

The good news is that by staying vigilant and exercising good judgement, you can stop most scams before they start. In this article, we'll touch on some of the most prevalent types of scams and provide action steps you can take to help protect yourself, your family and your legacy.

Main points

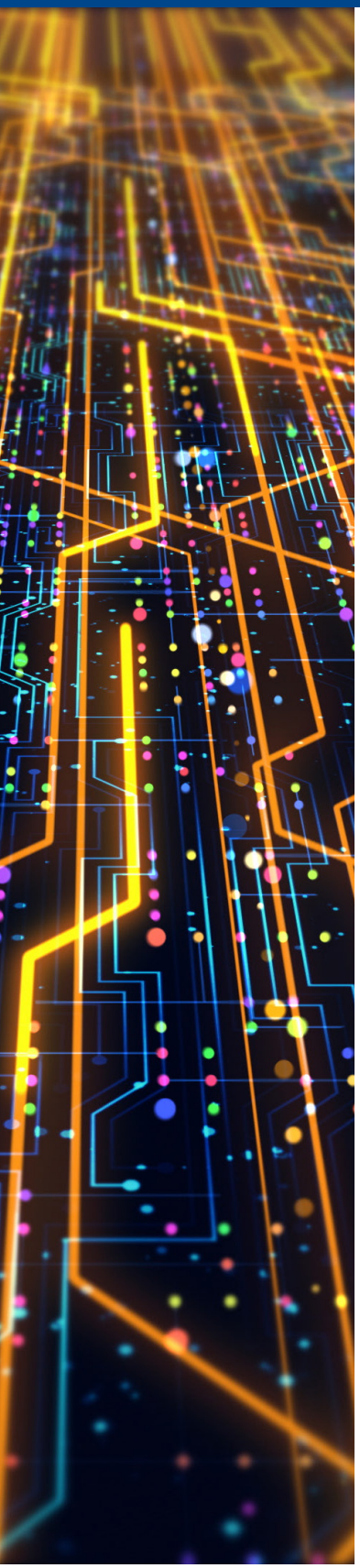
- Not just elderly are targeted, but seniors are most at risk for several reasons
- Knowing the techniques scammers use is the best protection
- Action steps you can take to protect yourself
- How Mesirow Wealth Advisors help protect you

Seniors are most at risk

Older adults are targeted by criminal perpetrators for several reasons, among them loneliness, cognitive decline, access to a large amount of accrued funds and a real or perceived lack of technological savvy. Often, scammers attempt to exploit these vulnerabilities by gaining the trust of their victims and convincing them to "invest" in fraudulent schemes.

Scammers specialize in using persuasive emotional tactics with elder victims. What's more, many crimes likely go underreported, because victims are embarrassed to admit they fell prey to a scammer.

You can protect yourself by knowing the tactics that scammers typically use to snare their victims and by exercising common sense online behavior to stop them in their tracks.



Knowing the techniques scammers use is the best protection

The best way to defend yourself and your family against scams is to spot them before you fall victim. Here are several of the more common ones.

- **Grandparent scam |** Perpetrators acquire personal information about grandchildren (or other relatives) through social media or by purchasing stolen data from cyber thieves. They use that information to impersonate the victim's relative. The scammer may request immediate financial assistance to resolve an emergency (an accident that resulted in personal injury or an arrest). The more sophisticated criminals may even use AI technology and voice cloning to impersonate the voice of the grandchild over the phone.
- **Romance scams |** These scams often involve fraudsters contacting targets seemingly at random, then gaining trust before ultimately manipulating targets into phony investments and disappearing with the funds. Criminal perpetrators often use social media and/or text messages on encrypted messaging platforms to contact seniors, befriend them and form a relationship. The scammer then will present an investment scheme with a promise of high profits. These tactics are commonly called romance scams.
- **Firm and Registered Representative imposter scams |** Perpetrators obtain information from BrokerCheck or online searches to impersonate a legitimate registered representative and/or member firm and use that information to create a fictitious website that appears legitimate. They then induce seniors or vulnerable adults to send money, posing as a financial professional who appears to be offering legitimate investments.
- **FINRA or other Federal Agency imposter scams |** Perpetrators pretend to be government or FINRA staff to obtain sensitive information, such as account information.
- **Computer takeover |** Perpetrators employ cyber tactics such as computer viruses or pop-up screens on a victim's electronic devices. In these cases, the criminal acts as though they are assisting the victim to resolve a virus, instructing them to download a program so that "tech support" can assist in removing it. When the victim complies, the perpetrator gains full access to their computer, including access to passwords or login credentials for financial accounts. With this information, the scammer can make withdrawals and transfers from the victim's accounts, sending the money to third parties.

Action steps you can take to protect yourself

One of the reasons these approaches work is because legitimate marketers use some of them too. To help you identify which contacts are genuine and which ones aren't, here are some best practices you can follow to protect yourself.

- **Don't be pressured into making immediate decisions.** A key tipoff of a scam is an urgent deadline. If you get a communication from a grandchild begging you for a quick response, ask a question that only that grandchild would be able to answer. Or contact the grandchild directly. If offered an investment opportunity, respond: "I never make investing decisions without first consulting my wealth manager/attorney/tax advisor." Or simply tell the person "I'm not interested. Thank you." Few legitimate offers — or calls where a relative needs money — are contingent upon you ACTING NOW! Good investments will still be there tomorrow.
- **Be picky about who you engage with.** Better yet, refuse to engage from the outset, especially if the pitch comes over the internet or via an unsolicited telephone call. Let the call go to voicemail. If you talk to the potential scammer, ask questions. A legitimate investment professional must be properly licensed, and his or her firm must be registered with FINRA, the Securities and Exchange Commission (SEC), or a state securities regulator—depending on the type of business the firm conducts. Even then, be skeptical. More sophisticated scammers may use information from BrokerCheck or online searches to impersonate a legitimate registered representative and/or member firm. A bona fide investment professional will not be put off by your caution.
- **NEVER click on an unsolicited link, no matter who it seems to come from.** This is probably the most important practice you can follow. Computer takeovers or password phishing scams need you to follow a link to initiate the infection of your computer. If you don't give them the "in" they need, they can't reach you.
- **Talk to someone first.** Be extremely wary if the person promoting an investment says, "Don't tell anyone else about this special deal!" A legitimate investment professional won't ask you to keep secrets. Even if the seller and the investment are registered, it's always a good idea to discuss these sorts of decisions with family or a trusted financial professional that is not connected to the offer.
- **Don't trust but verify.** Verify anything you're told by checking the seller's background. While some scammers may co-opt information from FINRA's BrokerCheck, it remains a great resource. It can tell you if an individual or firm is registered, provide an overview of an individual's work history and the firm's history. BrokerCheck also provides other important information such as regulatory actions, criminal convictions, and customer complaints involving the investment professional or firm. Using BrokerCheck is easy and it's free. Visit brokercheck.finra.org or call 800.289.9999 to learn more.

  Check out the investment and confirm what the salesperson tells you using the SEC's EDGAR database of company filings at sec.gov/edgar.shtm.

  Contact your state securities regulator to find out what they know about the company: You can find resources at North American Securities Administrators Association, nasaa.org.

How Mesirow helps protect you

One great reason to work with a Mesirow Wealth Advisor is that he or she can be a valuable resource to help assess the validity of investments or determine if an investment opportunity is a scam. As your fiduciary, your Mesirow Wealth Advisor has a duty to act in your best interests and help protect you, including alerting you if there's any suspicious activity among your accounts.

Beyond that, it's always good to take steps that help reduce potential security threats. That includes:

- Multi-factor authentication & transaction verification
- Secure passwords and careful online chatting
- Procedures that help protect your personal information

You can get details in our article: "Three ways to protect yourself from online theft and fraud."

Be safe out there

Modern technology helps make life easier for all of us. But that comes at a cost: we must be vigilant and maintain a health skepticism, especially anytime someone wants us to do something with our money. By following the action steps listed above and maintaining best practices in your digital behavior, you can greatly reduce your chances of falling victim to scammers.

To learn more, visit mesirow.com/wealthmanagement, call 847.681.2300 or email wealth@mesirow.com.

About Mesirow

Mesirow is an independent, employee-owned financial services firm founded in 1937. Headquartered in Chicago, with locations around the world, we serve clients through a personal, custom approach to reaching financial goals and acting as a force for social good. With capabilities spanning Global Investment Management, Capital Markets & Investment Banking, and Advisory Services, we invest in what matters: our clients, our communities and our culture.

Mesirow Wealth Management is the firm's founding capability. We are the initial namesake business of Norman Mesirow, whose vision was to serve with purpose, applying the highest standards of professionalism in advising individuals and families on their most important life goals.

We look forward to having an opportunity to serve you and your family.

1. 2023 FBI IC3 Elder Fraud Report