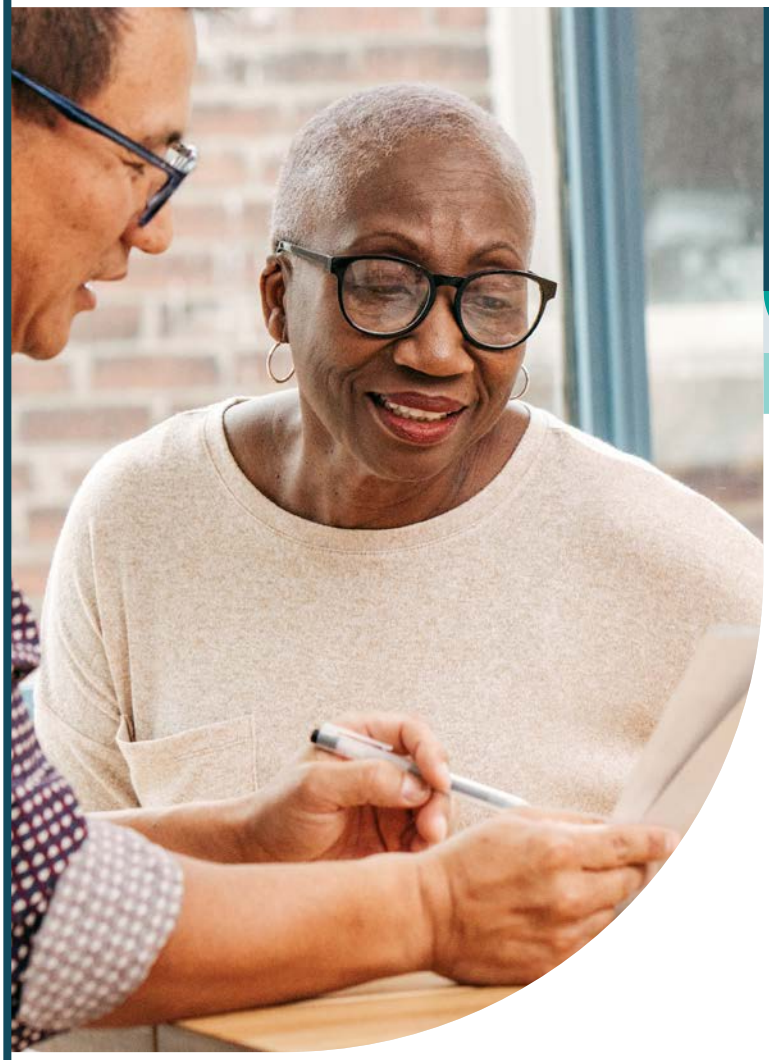
PARTICIPANT HANDBOOK

Savvy Saving Seniors®



Steps to Avoid Scams

BANK OF AMERICA

nco national council on aging®

CONTENTS

How Much Do You Know?

QUIZ: How Much Do You Know About Scams?

1. **What makes financial crimes against older adults so devastating?**
   a. Losing a large sum in retirement is difficult or impossible to recoup.
   b. Many older adults are already living on fixed or limited incomes.
   c. Victims may not realize they have been scammed due to the use of artificial intelligence (AI) tools.
   d. All of the above

2. **Can you estimate how much total money older Americans lost in 2023 to financial scams?**
   a. $5.2 million
   b. $650 million
   c. $3.4 billion

3. **What financial status makes an older adult a prime target for financial scams?**
   a. Having a high income and/or substantial wealth
   b. Having a low income and little savings
   c. All of the above

4. **It is safe to confirm or provide your personal identification information, such as your Social Security number, over the phone as long as your caller ID shows it is the Social Security Administration calling.**
   a. True
   b. False

5. **Which type of scams use AI technology?**
   a. Romance scams
   b. Tech support scams
   c. Investment scams
   d. All of the above

6. **The term "phishing" refers to:**
   a. Performing a search on the internet
   b. The transfer of cryptocurrency from victim to scammer
   c. How Gen Z writes "fishing"
   d. Methods used to trick you into sharing personal identification or account information

7. **You got a great quote for some much-needed home repairs. The contractor was kind enough to share that material prices are expected to skyrocket any day. Paying in full up front is the best choice because the contractor says it is the only way to lock in the price.**
   a. True
   b. False

8. **The usual suspects who might want to scam you include:**
   a. Strangers
   b. Family members
   c. Caregivers
   d. All of the above

Quiz Answers:

1. **D.** All of the above. Financial crimes against older adults can be devastating, often leaving victims with no way to recoup their losses. This can be especially detrimental if the older adult is already living on a fixed or limited income. AI tools have added a level of sophistication to scam tactics, and you may not even realize you have been scammed, potentially allowing it to continue.

2. **C.** According to the Federal Bureau of Investigation (FBI), in 2023, more than 101,000 adults age 60 and older reported being victims of financial fraud and scams. The damage? More than $3.4 billion in losses, an increase of approximately 11% from the year prior.[1] The average monetary loss for a victim of elder fraud in 2023 totaled $33,915.

3. **C.** All of the above. Scams are targeted at people of all income levels. Older adults control a substantial amount of personal wealth. Con artists, as well as family members and caregivers, are aware of the wealth and vulnerabilities of those who hold it. Those with lower incomes are often targets because they may be more willing to take a risk if something sounds too good to be true.

4. **B.** False. Using special technology, scammers can "spoof" the actual phone number of a government agency or call from the same area code (202 for Washington, DC, for example). Seeing the government agency's real phone number or name on caller ID can trick you into thinking the caller is who they say they are. As a rule of thumb, government agencies like the Social Security Administration, the Internal Revenue Service, and Medicare will never call you or contact you online to ask for personal identification information.

5. **D.** All of the above. AI is not limited to computer or tech-related crimes. The use of AI has greatly accelerated the scale, speed, and sophistication of all types of financial scams, making them more difficult to detect and defend against. Data mining to better target potential victims, AI-generated content to fake credibility, voice cloning and deepfake videos to trick the viewer—these are just a few AI tools employed by scammers today.

6. **D.** Phishing is a type of attack that uses various methods to try to obtain your sensitive identification information, financial account information and passwords. Emails, text messages, and phone calls will appear to be from a legitimate source, often prompting you to click a link or otherwise confirm or provide the information they seek. AI technologies have made phishing more effective, bypassing spam filters and fooling many.

7. **B.** False. This sounds like the classic home repair version of a confidence scam, in which the offender first gains the trust of their target, makes them an offer that is too good to be true, but then does not deliver the service or goods. Never move forward with a contractor without a signed contract and never pay in full upfront. Wait until the work is complete and passes inspection.

8. **D.** All of the above. While many scammers are strangers or members of a larger crime organization, people you know can be financial abusers, too. This does not mean you should isolate yourself, but it does mean you should remain alert to the motivations and actions of those around you. Monitor your accounts, and limit other people's access to your accounts.

Fraud:

A broad legal term that encompasses dishonest activities for financial or personal gain

Scam:

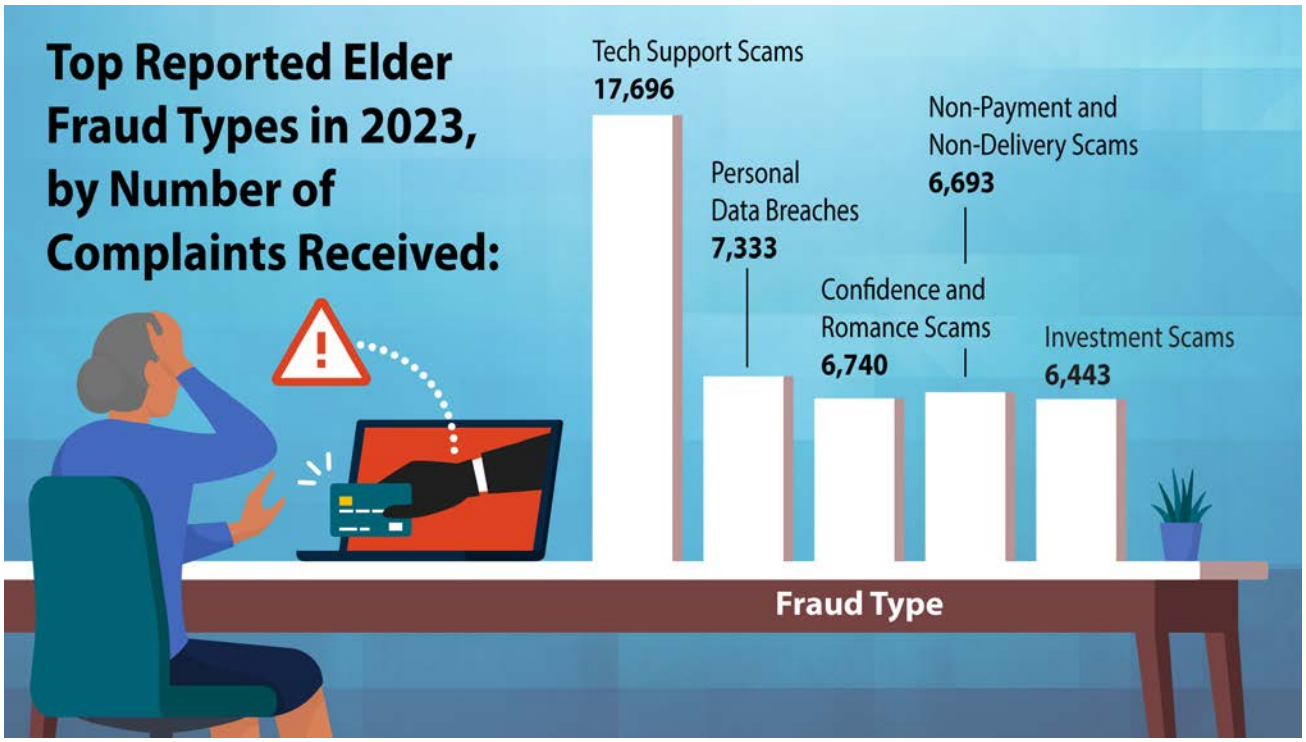
A type of fraud that involves tricking someone into giving up money or personal information

The Dirty Dozen: Top 12 Scams Targeting Older Adults

Every day, the FBI's Internet Crime Complaint Center, also known as IC3, logs thousands of complaints about a wide array of scams, many of them targeting older adults.

While call center/tech support scams were the most widely reported kind of elder fraud in 2023 with nearly 18,000 complaints to IC3, investment scams were the costliest. This type of financial crime alone cost older victims more than $1.2 billion in losses in 2023.[1] Here we'll learn how to recognize these types of scams, along with the rest of the dirty dozen—the top 12 most reported scams targeting older adults.

We'll also put AI in the spotlight to shine light on how rapidly evolving technologies are helping power these scams.



Source: FBI Internet Crime Complaint Center, https://www.fbi.gov/news/stories/elder-fraud-in-focus

Source: FBI Internet Crime Complaint Center, https://www.fbi.gov/news/stories/elder-fraud-in-focus

1. Call Center and Tech Support Scams

Illegal call centers defraud thousands of people each year and purposefully target older adults. In fact, people age 60+ lost more money to these scams than all other age groups combined and report having to remortgage/foreclose homes, drain retirement accounts, and borrow from family and friends as a result. This scam works in a variety of ways.

In many tech support scams, the caller pretends to be a tech support representative—often from a well-known company—and offers to fix a nonexistent computer issue. Other times, they may offer you antivirus protection programs. To do either, the scammer often asks for your computer password and gains remote access. Once in, they can install malware that provides long-term access to your personal and financial information on your computer.

Similar tech support scams come in the form of emails or pop-up windows that simulate virus-scanning software. These trick victims into clicking a link and downloading a fake antivirus program or an actual virus that will allow the scammer to access the user's information on the computer.

A newer form is the Phantom Hacker scam. It starts with the tech support scam but adds imposters from a financial institution and government agency to add legitimacy to their claims and convince you to comply. The phantom hacker scam has three phases:

1. **Phase 1:** After the tech support scammer has access to your computer, they will claim your accounts are at risk and ask you to log in to your financial accounts, which allows them to identify your most lucrative accounts for the second phase. The tech support person tells you a banking official will now contact you to secure your at-risk accounts.
2. **Phase 2:** A second scammer calls pretending to be from your financial institution and describes a threat to your accounts, such as a foreign hacker. They will claim the only way to secure your money is to move it to a "safe" account with the Federal Reserve or other government agency. The scammers often ask you to move your money via wire transfer, cash, or cryptocurrency.
3. **Phase 3:** The third scammer claims to be with the Federal Reserve or a government agency, acting as an utmost authority to get you to comply. If you express doubt, the scammer will provide fake "official" documents on authentic-looking letterhead to support their claim.

AI Spotlight: Tech support scams have been around a long time but have recently been given a big boost thanks to AI technology. With AI, scammers can create emails that appear completely authentic, bypass spam filters, and contain personalized information gathered about you from various online sources. That is what is so tricky about AI-supported scams. It adds a level of sophistication to the attack, which helps mask the red flags.

2. Personal Data Breach Scams

Using similar tactics to the call center and tech support scams, personal data breach scams differ in that they are a crime of opportunity. Taking advantage of cases of real data breaches, the criminals will exploit people's real-world concerns by sending emails or text messages that look like legitimate alerts.

These messages, which warn your personal information was compromised in a data breach, often prompt immediate action to secure your accounts. In reality, these scammers use links or fake websites to steal your sensitive personal information or install malware onto your devices.

If you were part of the original data breach and your phone number was leaked, the scammer may call you directly to phish for additional personal information or obtain access to your computer.

AI Spotlight: Generative AI aids these opportunists by creating messages that can go undetected through your first lines of defense, such as email spam filters. AI also helps these scammers overcome the last line of defense—you! AI algorithms can locate and analyze enormous amounts of data on countless targets to produce highly personalized, legitimate-looking phishing messages. If you were part of the initial data breach, AI also can incorporate the stolen data to make it even more convincing.

3. Confidence Scams

Confidence scams can be particularly painful due to the added layer of betrayal on a personal level. This type of financial crime typically occurs when a scammer defrauds a person after first gaining their trust, often using emotional manipulation and exploitation. It also can happen when the offender impersonates someone the older adult cares about, and AI has made this even more feasible. Let's take a look at some examples of this type of scam:

- **Romance Scams:** There is no love lost for fraudsters who create fictitious characters on dating sites and social media to lure older adults into romantic relationships. Offenders often "love bomb" their targets to gain affection and trust quickly. They then create scenarios where they need money from their victims or need travel expenses covered to visit them. Scammers also may ask older adults to deposit checks or ship packages for them. However, the victim may be unknowingly participating in illegal activity.

Romance scams also can evolve into "sextortion" cases if the scammer comes into possession of intimate photos. In 2023, people age 60+ reported 3,318 sextortion complaints with reported losses topping $6 million.

- **The Grandparent Scam:** The grandparent scam is so successful because it uses one of older adults' most reliable assets: their hearts. Criminals will call impersonating a younger loved one—such as a grandchild, niece, or nephew—and claim to be in trouble. They will create a sense of urgency needed to rescue them from the situation, requesting money immediately. A tell-tale sign that such a situation is a scam is that the person in trouble will ask you to send the money via Western Union or MoneyGram, through a friend, or by some other odd payment method.
- **Home Repair/Contractor Scams:** Knock, knock. Who's there? A scammer. Scammers will drive around neighborhoods seeking homes that may need repairs and are occupied by older adults. Once the victim has been targeted, the scammer provides an affordable quote for the proposed work—work they have no intention of doing right or at all. After the victim pays for the work in cash or with a check, the offender will either provide sloppy repairs, start but not finish the repairs, or disappear altogether. These individuals are very difficult to locate afterward, leaving the older adult out of money and sometimes with a home in worse condition than before.
- **Spousal Death/Funeral Scams:** Sadly, many scammers see tragedy as an opportunity and will take advantage of older adults at their most vulnerable. Some scammers will read obituaries and then call or attend the funeral to take advantage of the widow or widower. The scammer will claim the deceased had an outstanding debt that must be paid. Other times, unscrupulous funeral homes will add unnecessary charges or use hard sales tactics to push for more expensive services than are necessary.

AI Spotlight: AI has become a tool of choice for many confidence scams for its ability to create hyperrealistic impersonations, manipulated videos, and voice-cloned audio. Only a few seconds of audio is needed for AI to clone a person's voice, which scammers then use to call older adults while impersonating family members, friends, or even celebrities and public figures in phone calls or video messages.

AI also can generate true-to-life videos of people doing or saying virtually anything the scammer can imagine. Called deepfake videos, they are then used to deceive the person, who may believe they are in a new romantic relationship, have befriended a celebrity, or need to help a loved one. Convincing photos, scripts, websites, business materials, and more are all much more easily employed in confidence scams with the use of AI technologies.

4. Nonpayment/Nondelivery Scams

Put simply, nonpayment and nondelivery scams occur when a transaction ends up being one sided. For example, a good or service is provided but never paid for or a good or service is paid for but never received. Bait and switch scams—where a seller baits the buyer with an attractive offer or product but then switches to a different or an inferior product when they deliver—fall in this category, as well.

With nonpayment scams, offenders will secure the goods from you first and then never pay. They may initially provide payment that turns out to be a stolen credit card or fake check, continually delay payment with a parade of excuses, or disappear entirely. Requesting unusual payment methods or terms or having a lack of communication from the buyer are red flags for this type of scam.

Hallmarks of nondelivery scams include deals that seem too good to be true, listings that disappear after purchase, pressure to buy quickly, unusual payment methods, and a buyer left without a product or refund.

AI Spotlight: Scammers can use AI to easily create fake online storefronts and populate them with phony product listings. Often, they post popular products that are hard to find elsewhere or expensive products that are discounted to incredibly low prices. Either way, the products don't exist or will be replaced with poor substitutions without your consent.

5. Investment Scams

From Ponzi schemes like the one made famous by Bernie Madoff (who defrauded thousands of people, including celebrities, out of billions of dollars) to emails from a fabled Nigerian prince looking for a partner to claim his inheritance money to complex financial products that many economists do not even understand, investment schemes have long been a successful method to take advantage of older adults. This type of scam often plays out as advanced fee schemes, Ponzi schemes, pyramid schemes, market manipulation fraud, real estate investing, and trust-based investing such as cryptocurrency investment scams.

Think it couldn't happen to you? Think again. Interestingly, these scams often start with a confidence scam. The offender knows they must gain your trust for you to invest large sums of your hard-earned money with them, and they do so via friendship, romance, and professional networking. In 2023, the FBI's IC3 received more than 6,400 investment scam complaints from people age 60+ with reported losses of more than $1.2 billion.[1]

Described as socially engineered and trust enabled, investment scammers may work alone or with others. It could even be another new acquaintance you met through the scammer who plays the role of one of the investor's success stories. They might let you in on the secret, or they may accidentally let information about their success slip in front of you. Sometimes, they will flaunt what appears to be extravagant wealth, goading you to finally ask how they are doing so well. Of course, they are all calculated methods to introduce their investment scheme.

So how do you recognize these schemes before it is too late? Is the investment complex and difficult to understand? Is it presented as having little to no risk involved? Is it presented as having guaranteed or exceptionally high rewards? Is it suggested by someone fairly new in your life? A good rule of thumb to follow: If it sounds too good to be true, it probably is!

AI Spotlight: Investment fraud is particularly bolstered by both generative and predictive AI technologies. Scammers are using deepfake videos, voice cloning, and AI-generated content to deceive investors. Fake identities, nonexistent companies, and convincing endorsements—such as deepfake videos showing a celebrity or trusted figure endorsing an investment opportunity—are all tools of the trade. The DC Department of Insurance, Securities and Banking notes it regularly finds criminals impersonating U.S. Securities and Exchange Commission staff and other government officials in such scams.[3]

It is not only impersonations and fake websites, either. AI-generated fake news articles, social media posts, and reports and portfolios breathe life into these illusions. AI can even artificially inflate the price of an asset before selling it off, leaving investors in the red. Sometimes, investment scammers' use of AI is simply in claims, banking on AI's reputation to substantiate their lies of AI-powered trading bots and advanced algorithms.

6. Extortion Scams

Extortion scams might be the dirtiest of the dirty dozen types of scams against older adults. Where other scams aim to trick, extortion scams are marked by direct threats. The scammer will claim to have evidence that could embarrass or incriminate the older adult, and they will threaten to make that evidence public or share it with the older adult's contacts if they don't pay the hush money demanded.

While the scammer is bluffing in some instances, at other times, they truly have gathered private information to use against their target. Scammers who can get malware onto an older adult's computer may be able to record keystrokes, watch the webcam, and track online history that may be private—all of which they will use to blackmail the victim. And as mentioned previously, older adults who find themselves in a romance scam could be vulnerable to sextortion—where they are threatened with intimate images or details being released if they don't pay.

In other extortion scams, the offender will impersonate a government employee and allege the older adult is under government investigation. They will demand payment under threat of arrest or prosecution.

AI Spotlight: While AI technology can be used in some of the more common ways to help scammers impersonate government officials, another way it is being used is to create fake evidence to use against their targets. They may use generative AI to produce deepfake videos or lookalike compromising photos of the older adult that they can use to extort money from the victim.

7. Government Impersonation Scams

As described with some extortion schemes, government impersonation scams feature fraudsters who co-opt the authority of government agencies to scare their victims into paying them money. Typically claiming to be from the Internal Revenue Service (IRS), Social Security Administration (SSA), or Medicare, these criminals then allege false claims, make demands, and threaten a devastating consequence if the older adult doesn't comply.

For example, the fake IRS agent may threaten arrest or deportation if the older adult doesn't send money for their supposed unpaid taxes. Or the fake SSA representative may threaten to cut off the older adult's benefits unless the person provides personal identifying information, which is then used for nefarious purposes. Another common setup: The imposter health insurance agent who collects your personal information under the guise of helping you with your Medicare or Medicaid coverage.

An easy-to-spot red flag for this scam is that the government imposters often demand payment via prepaid debit cards, cash, or wire transfers. It is also important to note that as a rule, government organizations do not usually call you, email you, or show up at your home. They also would not threaten you or request personal information via email.

AI Spotlight: Using special technology, scammers will spoof the actual phone number of a government agency or call from the same area code (202 for Washington, DC, for example). Seeing the government agency's real phone number on caller ID can help trick you into thinking the caller is who they say they are. AI tools also can forge government identification and mimic official email designs to make the scammer and their messages appear more credible.

8. Credit Card/Check Scams

In an age where credit cards and digital transactions abound, credit card fraud has remained a steady method for scammers to steal money. It encompasses theft using not only credit cards but similar payment methods—such as ACH, EFT, and recurring charges—as well.

Scammers may use phishing tactics and other common schemes to gain access your credit card number and other personal identifiable information that can help them carry out this type of fraud. In one method, the scammer calls and almost immediately asks, "Can you hear me?" When the older adult answers, their "yes" is recorded and then used as voice verification for the scammer to authorize charges on the credit card.

However they obtain the credit card information, they then typically max out your credit cards with purchases, or they may set up a smaller recurring charge that they hope goes unnoticed. With enough of your personal data, they can also open new lines of credit in your name, amassing enormous debt.

Older adults are often seen as attractive targets for credit card fraud because many have good credit scores, established savings, and an expected high level of trust. And speaking of trust: While many of these dirty dozen types of scams are committed by unknown culprits, credit card fraud is a crime that is also sometimes carried out by people older adults know, including family members or trusted caregivers. It makes it even more important for older adults to protect their personal information and regularly review their accounts, transaction histories, and credit scores.

AI Spotlight: Scammers will use their full arsenal of schemes supported by a mix of AI technologies—advanced phishing messages, voice cloning, deepfakes, and more—to acquire credit card and personal information.

9. Business Email Compromise Scams

In 2023, 11.2 million (19.2%) of Americans age 65 and older were still working or actively seeking work.[2] And scammers took aim at older adults at work via business email compromise scams, also known as email account compromise scams.

Depending on the fact that most people rely on email to conduct professional business, scammers send email messages that appear as normal job tasks from known sources, but the truth is it's anything but business as usual. For example, the scammer may email an invoice while posing as a vendor your company regularly works with. Except this time, they have sent an updated payment link or perhaps a new mailing address for you to mail the check.

That alone may not raise a red flag when everything else about the communication looks legitimate. Scammers may spoof the email account, website, or email design, or they may change a small, unnoticeable detail in the email address. At a glance, it could appear to be sent from a company or person you communicate with regularly.

Similarly, spear phishing emails are messages that appear to be from known, trusted senders and manipulate the receiver into discussing otherwise confidential information. This helps the cybercriminal get their foot in the door to access company accounts, contacts, and other information. These seemingly innocent business emails may also trick the receivers into downloading malicious software onto company computers, which can go undetected.

There have also been cases where the scammer impersonates someone within the company, such as the CEO or other authority figure. It may appear your boss is asking you to cut a check to a vendor or buy and mail gift cards to clients. But in reality, the company you work for is getting swindled. These scams are even easier to carry out when the company's workforce is remote or there is a hybrid work environment that limits face-to-face interactions.[4]

AI Spotlight: AI capabilities—which can be used with speed, scale, and virtually no cost—have scammers creating more elaborate multistage, multichannel business email compromise strategies, extending to text messages, business communication apps, cloned voice calls, and even deepfake Zoom calls.

10. Identity Theft Scams

Did you know your personal information is often more valuable than all the money in your account? While many scams steal money in one-and-done deals, identity theft scams put the victim at repeated risk, making this type of fraud especially insidious.

Once a scammer obtains enough of your personal identifying information—such as your name, birth date, Social Security number, and passwords—they can usually gain access to your accounts and rob you of your security. Worse yet, some scammers then use your information to open new accounts and rack up astounding amounts of debt that can take months or years to discover and just as long to unravel.

So how do they do it? They go phishing. Phishing is a practice of posing as a reputable source, usually through messages like emails or texts, and prompting individuals to reveal sensitive personal and financial information, such as identifying information, credit card numbers, and passwords. While AI has greatly improved the believability of many phishing messages, there are some telltale signs you can learn to spot:

- Offers that seem too good to be true
- High-pressure sales pitches that stress urgency
- Alerts that there's a problem with your account
- Shortened or misspelled links
- Emails that don't address you by name
- Messages with poor grammar and spelling
- Direct requests or demands for payment
- Requests to confirm personal information

The phone, too, remains a weapon of choice when targeting older adults, and perhaps the most prevalent scam involves fake telemarketing calls. With no face-to-face interaction and no paper trail, these scams are incredibly hard to trace. Many of these calls begin as robocalls, an automated recorded message that plays when you answer the phone, instructing you to speak aloud or push buttons to answer questions and/or be connected to a live person. Your contact information can easily spread among these scheming organizations, making the phone ring incessantly.

Signing up for the National Do Not Call Registry can help reduce the number of telemarketers calling.

AI Spotlight: Just as the public was becoming more aware of phishing tactics and getting better at recognizing them, AI came into play and changed the game. Using information found across the internet, AI programs can mine a target's public information and analyze their online behavior. This allows AI to then produce highly specific personalized phishing campaigns that are incredibly successful at inducing people to reveal information they normally protect. AI technology also has automated this process, allowing cybercriminals to commit identity theft on a larger scale and at a greater speed.

Laws often lag behind technology, but government agencies are working diligently to catch up to AI-integrated scams. In early 2024, the Federal Communications Commission deemed all calls with AI-generated voices "artificial" under the Telephone Consumer Protection Act. The ruling made voice cloning technology used in robocall scams targeting consumers illegal and gave State Attorneys General across the country new power to prosecute robocall operations.[5]

11. Advanced Fee Scams

Advance fee scams are a game of give to get, but you should know that if you play, the scammers always win. Using a variety of approaches, the offenders persuade their targets to pay upfront fees after misleading them to believe that they would receive something of value in exchange. The scammers often leverage basic wants and needs, making it more likely their target will be willing to give to get what they need. Here are some examples:

- **Rental Scams:** With housing demand high and inventory low, securing an affordable place to live is a difficult task in many areas of the country and has spurred an increase in rental scams. Scammers will offer rental properties they don't own or that aren't available or real, requiring upfront deposits or fees to secure the property before the renter has even visited the property. The fake landlord pressures interested renters into paying the advance fee with threats that they will be forced to give the lease to one of the many other people interested in it.

- **Loan and Employment** Scams: People in need of income are more susceptible to loan scams and employment scams. In the former, scammers falsely promise loans or lines of credit to get their targets to pay upfront fees or insurance. For the latter, sham employment opportunities will require advance fees for things like employee training, background checks, supplies, or other expenses. It's only after you pay that you find out there is no real job. The scammers often tailor employment offers to appeal to older adults, with promises of easy work-from-home jobs or incredible benefits.

  Some scammers keep the farce going until after they have pretended to hire you, taking the opportunity to obtain your personal identifying information as part of their fake onboarding. This is one of the ways advance fee scammers also utilize their oldest trick in the book: phishing for information.

- **Lottery Scams:** Another type of scam involves tricking the older adult into believing they have won money or a prize. The U.S. Embassy in Jamaica receives frequent reports of citizens losing money to advance fee fraud perpetrated by scammers in Jamaica. The most prevalent scenario: The scammer leads someone to believe they have won a drawing or lottery but must pay upfront fees or taxes to claim the prize or cash.[6]

AI Spotlight: Like with other types of scams, advance fee fraudsters use AI tools to create a mirage of legitimacy for their claims, identity, and job offers. AI technology can scrape data from job boards and LinkedIn profiles to precisely target job seekers likely to take the bait. AI can be used to submit fake employment offers, conduct automated interviews, gather personal information, and collect advance fees.

12. Windfall Scams

Everyone dreams of winning big, but you may find yourself in the very real nightmare of losing big if your unexpected windfall turns out to be a scam. These types of scams capitalize on the common hope of coming into money—such as winning the lottery or a sweepstakes or receiving an unexpected inheritance—a hope that can be particularly enticing to older adults who may be living on a fixed or limited income.

Typically, scammers will inform an older adult that they have won the lottery or a sweepstakes but need to provide personal information and/or make a payment to unlock the prize. Often, older adults will receive a check that they can deposit in their bank account, knowing that while it shows up in their account immediately, it will take a few days before the fake check is rejected. During that time, the scammers will quickly collect money for supposed fees or taxes on the prize, while the victim has the pretend prize money removed from their bank account when the check bounces.

In recent years, foreign crime organizations from Jamaica in particular, have earned a reputation for windfall scams. Identifying themselves as lawyers, customs officials, or lottery representatives, these scammers congratulate you on winning a sweepstakes, foreign lottery, or other high-value prize. Then comes the but … but you must first pay fees for shipping, insurance, customs duties, and/or taxes before they can release your prize. These international crime organizations will even use U.S.-based money mules to be the middleman for your payments, making it even more difficult to track them.[6, 7]

AI Spotlight: Scammers working the windfall angle employ many of previously discussed AI tools to impersonate authority figures such as lawyers or well-known organizations, state lotteries, and Publishers Clearing House. They also use AI to scan vast amounts of demographic data to more precisely close in on their prime targets.

Case Study: A Closer Look at Common Scams

Maggie, a 72-year-old widow, met James through an online dating site for older adults. He quickly charmed her with attention, affection, grand gestures, and promises for the future. It was a whirlwind romance, and she scarcely had time any longer to visit her kids, attend her church group, or go on her daily walk with her neighbors.

Within a few short months, their relationship grew more serious, and James convinced Maggie to invest a large sum in a lucrative opportunity he claimed was guaranteed to secure her—and their—financial future. Feeling pressured, she was about to send money when she hesitated.

In retaliation, James threatened to expose intimate messages and images, obtained through manipulated online conversations, unless Maggie complied. Fearing disgrace, she relented and wire transferred the money to James. Maggie was left heartbroken, scared, in dire financial straits, and feeling very alone to process what happened to her.

- Can you identify what type (or types!) of scams took place in this scenario?
- What were some of the red flags you noticed as this scenario progressed?
- Do you think there is anything Maggie could have done differently?

Tips to Avoid Scams

Tips to Avoid Call Center and Tech Support Scams

- Do not click on unsolicited pop-ups, links, or attachments, and do not call phone numbers provided in unsolicited texts or emails.
- Do not download software from an unknown person who contacted you.
- Never allow an unknown person access to view or control of your computer remotely.
- Never send money, cryptocurrency, or gift cards to tech or customer support agents who contact you unsolicited.
- Never share your password or other personal information with a person who contacted you unsolicited.
- Do not engage. It is ok to delete emails without response and to simply hang up the phone.
- Sign up for the National Do Not Call Registry (DoNotCall.gov) to reduce the number of telemarketers calling. You can also take yourself off multiple mailing lists.
- If you are experiencing actual computer issues, you can contact the computer or software company directly or check the Better Business Bureau (bbb.org) for local trusted tech support businesses.

Tips to Avoid Personal Data Breach Scams

- Do not click on pop-ups, links, or attachments warning that your data has been breached.
- Look for red flags, such as grammar and spelling errors, prompts to provide or confirm your personal information, and pressure to act quickly.
- Do not engage with text or email message or phone calls alerting you to a data breach. Instead, contact the named company directly using a confirmed phone number or website.
- Use strong passwords and enable multifactor authentication to protect your information from real data breaches.

Tips to Avoid Confidence Scams

- Be aware that you are at risk from both strangers and people close to you.
- Don't mix dating and dollars. Set strong boundaries between your finances and romantic partners.
- Create a secret family password to outsmart voice cloning. If a family member ever calls requesting money for an urgent situation, ask them for the password to confirm their identity.
- Take time to confirm the caller's identity and/or the situation. Ask personal questions a scammer would not be able to answer or hang up and call another close relative who could help confirm the situation.
- Always tell salespeople who come to your door or call you on the phone: "I never buy from or pay anyone who calls or visits me unannounced. Please send me your information in writing."
- For home repairs, get quotes from multiple companies to confirm there is consensus on what work is needed and ensure you are getting a fair price.
- Never move forward with a contractor without a signed contract and never pay in full upfront. Wait until the work is complete and passes inspection.
- For contractors, funeral homes, or any type of business, ensure they are reputable by calling the Better Business Bureau at 804-648-0016 or checking online at bbb.org.
- Don't concede to high-pressure sales tactics. Get everything in writing and take your time to contemplate any costly decisions.
- Consider carefully who you grant durable powers of attorney and include safeguards to prevent those being misused by your named agent.

Tips to Avoid Nonpayment/Nondelivery Scams

- Don't provide personal or payment information on unfamiliar or unverified websites.
- Opt for secure payment methods like credit cards that offer buyer protection.
- Take time to research websites or individual sellers before moving forward with a purchase.
- Check the quantity and content of the customer ratings and reviews.

Tips to Avoid Investment Scams

- Always keep in mind the number one rule to avoid investment scams: If it sounds too good to be true, it probably is!
- Be wary of investment opportunities claiming no risk, quick profits, or guaranteed returns.
- Ignore unsolicited offers asking you to invest money.
- Do your homework to verify the credibility of investment opportunities and the people promoting them from multiple reputable sources.
- Consult with a registered investment professional before making any decisions. Visit Investor.gov to confirm the status of any investor's legally required registration and check for disciplinary history.[3]

Tips to Avoid Extortion Scams

- Keep online profiles such as a Facebook page private, making it viewable only to connections you approve. Likewise, only friend or connect with people on social media who you know and you have met in person.
- Limit how much personal identification information—such as your birthday, address, and phone number—you share on social media, dating profiles, and other public sites.
- Reconsider sharing overly personal stories on these online public platforms, as they could be used against you by extortionists.
- Strongly rethink posting, emailing, texting, or sharing intimate photos or videos, which can be used in sextortion scams.
- Keep in mind that a real government official or law enforcement officer will not threaten you for money.
- Don't panic—block and report. Blackmailers bank on scaring you into compliance. Don't respond, don't try to negotiate your way out of it, and don't pay. Block them from further communication and immediately report the crime.

Tips to Avoid Government Impersonation Scams

- Government agencies will never threaten you with arrest or loss of benefits as a consequence for not making a payment you have not confirmed.
- Government agencies will never call, email, text, show up unannounced, or message you on social media to ask for money or personal identification information.
- Know that the government will never ask you to pay via money wire, gift cards, cryptocurrency, or other unusual payment methods.
- Don't rely on your caller ID because scammers can spoof, or fake, a government agency's name and/or real phone number when they call.
- Do not engage with these requests. You can always contact the agency directly to determine if there is a real issue or action needed. Only use verified phone numbers found on government websites—never call a number provided by the original contact.
- Keep your Medicare number as private as your credit card number and regularly review your Medicare statements.

Tips to Avoid Credit Card and Check Scams

- Don't click on anything in an unsolicited email or text message asking you to update or verify account information. Call the bank or company via a verified number to ask if the request is legitimate.
- Shred all documents that show your credit card or bank account number.
- Use direct deposit for benefits checks to prevent physical checks from being stolen.
- Never give personal or account details to someone who contacts you from a credit card company. Hang up and call the company directly using a phone number listed on your account statement or on the back of your card.
- Protect your account logins with strong passwords and enable two-factor authentication for your account logins.
- Use your debit card like a credit card at gas stations to avoid your PIN being stolen by a skimming device.
- Ensure you are set up to receive fraud alerts from your bank and credit card company.

Tips to Avoid Business Email Compromise Scams

- Check invoices and emails requesting payment carefully, confirming exact email addresses, websites, and details for known contacts. Scammers change minor details—such as adding a period in an email address or changing ".com" to ".co" on a website—to make them appear correct.
- For unknown contacts, confirm the validity of the request and the provided payment details with your company's accounting department.
- Follow safe email practices. Don't open email attachments from unknown senders and proceed with caution with forwarded attachments.
- Use strong passwords and set up two-factor or multifactor authentication on any business-related account login that allows it.
- For payment or purchase requests that are new or unusual, verify their validity in person or by calling a confirmed number yourself.
- Pause on any payment or purchase request that comes with pressure to act quickly.

Tips to Avoid Identity Theft Scams

- Know that an identity thief's goal is to gain access to bank or other accounts, lines of credit, and other financial resources.
- Be cautious and protective of your personal information wherever it is being used or written down, as thieves are always coming up with new methods to steal your identity.
- Never share your personal or financial details on the phone or online unless you initiated the call to a verified number or logged in to a verified, secure site.
- Avoid connecting your phone or computer to the internet using unsecured public WiFi networks, as it leaves your device vulnerable to access by cybercriminals.
- Collect your mail regularly to lessen the chance of it—along with your personal identification or account information—being stolen.
- Shred documents containing sensitive personal identification or account information before throwing them away.
- Consider employing an identity theft monitoring service with identity theft insurance to help cover financial losses in a worst-case scenario.
- If you suspect you may be a victim of identity theft, report it as quickly as possible and freeze your credit with all three credit bureaus to prevent new accounts from being opened in your name.

Tips to Avoid Advance Fee Scams

- Never pay upfront fees for anything, especially for employment applications or training, loan processing, or to claim a prize.
- Practice the pause. Scammers pressure you to act quickly before you have time to think about or research a situation. Never pay a fee under pressure; instead, pause and do your due diligence.
- Heed caution with companies that are difficult to locate, lack a physical address, or are not easily verifiable from multiple trusted sources.
- Judge all requests for unusual payment methods as red flags. These include wire transfers, gift cards, and money orders—all of which are difficult to track or recover.
- If you must pay an upfront fee that you believe to be legitimate, use a secure payment method and then monitor your accounts closely.

Tips to Avoid Windfall Scams

- It bears repeating: If it sounds too good to be true, it probably is!
- Remember: You can't win if you did not play. Do not believe claims you won a lottery or sweepstakes you never entered yourself.
- U.S. citizens can't play and win foreign lotteries. It is illegal, so hang up on anyone calling about the Jamaican lottery or any others you have not played.
- Never pay an upfront fee to claim a prize or inheritance. Legitimate lotteries and sweepstakes take taxes and fees out of prize money before your payout.
- Do not share your personal or financial information with anyone claiming to need it to confirm an inheritance.

Protecting Yourself and Others

Now that you know more about the most common scams targeting older adults and how to avoid them, you can share that knowledge with family and friends who may also be at risk or being targeted. You can also stay alert for signs that someone you care about may be experiencing a financial-related scam or other problem. Here are some signs to take notice of:

- Unusual recent changes in personal accounts, including atypical withdrawals, new individual(s) added, or sudden use of a debit or credit card
- A person suddenly seeming confused, unkempt, or fearful
- A caregiver not allowing others access to an older adult
- Piled up sweepstake mailings, magazine subscriptions, or "free gifts," indicating the person's name has been added to a list

Reporting Scams and Other Steps for Financial Fraud Victims

How to Report Financial Scams

Older adults should report financial-related scams to the National Elder Fraud Hotline or file a complaint with the FBI's IC3. Here are the details for these and other reporting resources:

- National Elder Fraud Hotline: 833-FRAUD-11 (833-372-8311)
- FBI's IC3: ic3.gov
- Federal Trade Commission: ReportFraud.ftc.gov
- Adult Protective Services: napsa-Now.org/Help-in-Your-Area
- Medicare: 800-MEDICARE

Other Smart Steps You Can Take

- Contact all your banks and credit card companies immediately.
- Cancel any debit or credit cards linked to the stolen account. Reset personal identification (PIN) numbers and passwords.
- Put out a fraud alert to all three credit reporting agencies (Experian, Equifax, and TransUnion) and consider a credit freeze.
- File a report with the police. The police may not be able to do much themselves, but you may need a police report in order to clear up the problem.

Helpful Resources

Administration for Community Living's Legal Services for Older Americans Program
acl.gov/Programs/Legal-Help/Legal-Services-Elderly-Program

Better Business Bureau Resources for Older Adults
804-780-2222
bbb.org/all/older-adult-resources

Consumer Financial Protection Bureau
ConsumerFinance.gov/Consumer-Tools/Educator-Tools/Resources-for- Older-Adults/

National Center on Elder Abuse
ncea.acl.gov

National Center on Law and Elder Rights
ncler.acl.gov

National Council on Aging
ncoa.org

Senior Medicare Patrol
smpResource.org

Social Security Fraud Reporting
800-269-0271
oig.ssa.gov

Adult Protective Services Locator by State
napsa-Now.org/Help-in-Your-Area/

Appendix A

Attorneys General – States

Alabama
334-242-7300

Alaska
907-269-5100

Arizona
602-542-5025

Arkansas
800-482-8982

California
916-445-9555

Colorado
720-508-6000

Connecticut
860-808-5420

Delaware
302-577-8600

Florida
850-414-3300

Georgia
404-651-8600

Hawaii
808-586-1500

Idaho
208-334-2400

Illinois
312-814-3000

Indiana
317-232-6330

Iowa
515-281-5044

Kansas
785-296-3751

Kentucky
502-696-5300

Louisiana
225-326-6465

Maine
207-626-8800

Maryland
410-576-6300

Massachusetts
617-727-2200

Michigan
517-335-7622

Minnesota
651-296-3353

Mississippi
601-359-3680

Missouri
573-751-3321

Montana
406-444-2026

Nebraska
402-471-2682

Nevada
702-486-3132

New Hampshire
603-271-3658

New Jersey
609-292-8740

New Mexico
505-490-4060

New York
518-776-2000

North Carolina
919-716-6400

North Dakota
701-328-2210

Ohio
614-466-4986

Oklahoma
405-521-3921

Oregon
503-378-4400

Pennsylvania
717-787-3391

Rhode Island
401-274-4400

South Carolina
803-734-3970

South Dakota
605-773-3215

Tennessee
615-741-3491

Texas
512-463-2100

Utah
800-244-4636

Vermont
800-649-2424

Virginia
804-786-2071

Washington
360-753-6200

West Virginia
304-558-2021

Wisconsin
608-266-1221

Wyoming
307-777-7841

Attorneys General – Territories

American Samoa
684-633-4163

District of Columbia
202-442-9828

Guam
671-475-2720

Northern Mariana Islands
670-237-7600

Puerto Rico
787-721-2900

U.S. Virgin Islands
340-774-5666

Sources

1. 2023 Elder Fraud Report, Internet Crime Complaint Center, Federal Bureau of Investigation.
https://www.ic3.gov/AnnualReport/Reports/2023_IC3ElderFraudReport.pdf

2. 2023 Profile of Older Americans, Administration for Community Living.
https://acl.gov/sites/default/files/Profile%20of%20OA/ACL_ProfileOlderAmericans2023_508.pdf

3. Artificial Intelligence and Investment Fraud, DC Department of Insurance, Securities and Banking.
https://disb.dc.gov/page/artificial-intelligence-ai-and-investment-fraud

4. Phishing Guidance: Stopping the Attack Cycle at Phase One, National Security Agency, 2023.
https://media.defense.gov/2023/Oct/18/2003322402/-1/-1/0/CSI-PHISHING-GUIDANCE.PDF

5. Declaratory Ruling, Federal Communications Commission, 2024.
https://docs.fcc.gov/public/attachments/FCC-24-17A1.pdf

6. Lottery Scams, U.S. Embassy in Jamaica.
https://jm.usembassy.gov/lottery-scams/?_ga=2.158491258.19693272.1674836526-841878856.1674836526

7. Senior Scam Alert, U.S. Department of Justice.
https://www.justice.gov/elderjustice/senior-scam-alert

Notes

@NCOAging | ncoa.org
251 18th Street South, Suite 500, Arlington, VA 22202