AUGUST 2025

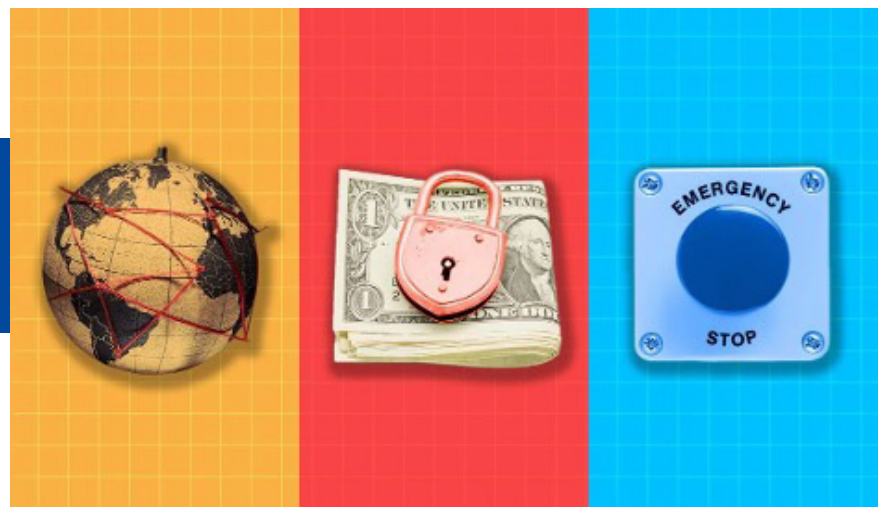
BE SAFE | BE INFORMED | BE AWARE

FIGHTING FRAUD with ENOA

Eastern Nebraska Office on Aging
(402) 444-6536 | Blair (402) 426-9614
enoa.org

3 Key Things to Know About Scams in 2025

By Ken Budd, AARP



Today's sophisticated fraud criminals are serious about stealing your money; you need to get serious about protecting yourself

Over a recent two-week period, Frank McKenna engaged with scammers six times — on purpose.

McKenna, chief innovation officer for Point Predictive, a San Diego-based fraud-prevention company, interacts with scammers to better understand how they work. Hiding his identity, he responds to criminals' emails and texts to analyze their sophisticated manipulations, then uses that information to hone prevention methods. (Do not do this at home: If you suspect a scammer is targeting you, cut off all communication immediately and follow these steps.)

That knowledge has never been more vital. Last year, consumers reported to the Federal Trade Commission (FTC) fraud losses of more than $12.5 billion. That's a 25 percent increase from the previous year. The actual losses are likely higher because fraud is a notoriously underreported crime. While only $10 billion was reported stolen through fraud to the FTC in 2023, for example, the agency's later analysis concluded that the real amount may have been as high as $158.3 billion.

Here are three things you need to know about fraud right now:

1. Scams are perpetrated by highly sophisticated international criminal organizations.

Scammers typically aren't two-bit lone criminals working out of their basements. McKenna estimates that roughly 80 percent of scams that target Americans come from mafia-style crime organizations based outside of the United States. "These are gangsters," he says, and they're ruthless: When the criminals realized he was probing their operations rather than succumbing to the scams, they sent him death threats.

Americans lost $3.5 billion from scams originating from Southeast Asia in 2023, according to data from the United States Institute of Peace. In countries such as Myanmar, Cambodia, and Laos, 40 percent of the economy is based on fraud.

Southeast Asia is not the only criminal hotspot. India is home to a large number of tech-support scams.

Romance scams often originate in West Africa. Nigeria, for example, is well-known for its "Yahoo Boys," who lure victims with catfishing techniques (creating false identities and attracting people through dating apps, messaging apps, and social media). But Southeast Asia is scam central, most notorious for frauds that use financial grooming, often known as pig butchering, as a technique: Criminals will spend time fostering relationships with their targets, building trust before proposing they invest in phony cryptocurrency schemes.

Fighting scams isn't simply about protecting your life savings, as essential as that is. It's about knowing that your stolen money is enriching inhumane criminal organizations. Southeast Asian fraud factories use human trafficking and deceit to ensnare and enslave workers who are often tortured for not meeting quotas.

"They've got about 400,000 people, they put them in scam compounds,

Continued on next page

and they have them work 20 hours a day," says McKenna, who calls it "the most brutal thing that's happened to humanity at this scale since World War II."

Another reason this knowledge is essential: Knowing your adversary's strength can lead to better defenses.

2. Protect your finances like you protect your health and property.

A sophisticated threat requires strong defenses, but many of us aren't taking proper steps. Amy Nofziger, director of victim support for the AARP Fraud Watch Network, gives an example from a recent talk on financial security. She asked her audience: How many of you lock your doors? How many of you have an alarm or live in a gated community? How many of you have a dog or even a gun? Nearly every hand was raised. Then, she asked, How many of you have a credit freeze on your credit report? Only two hands stayed up.

"You're probably more likely to be a victim of a fraud or a scam than you are to have your property burglarized," Nofziger says. "So why are we focusing on someone stealing our TV and not on someone stealing our retirement savings?"

You need to create barriers against scammers. Basic protections include:

- Managing your phone's settings so any unknown number goes to voicemail.
- On social media, adjusting privacy settings to the most restrictive levels.
- Freezing your credit and regularly checking your credit report.
- Asking your credit card company to send notifications for charges over a certain amount (or for any amount).

Find more tips here and at AARP's Fraud Resource Center.

3. Report scams to the authorities.

William Webster was an unlikely scam target. He is a former judge and former director of the FBI and the CIA. And yet in 2014, Webster, then age 90 (he's 101 now), was targeted in a Jamaica-based lottery scam (victims are told they've won money but need to pay a fee before receiving it). When Webster's wife, Lynda, repeatedly told the scammers to stop calling, one of them issued a chilling threat. She would die, he said, from a sniper's bullet.

"We were getting lots of scamming calls, and I would tell [William] to hang up, and when he didn't, I'd get on and say, 'Look, I'm his wife, I know what you want, and if you call back, I won't be so nice,' " recalls Lynda, who encouraged the FBI to film an elder fraud public service video with her husband in 2022. But one man did call back.

"He told me how nice the blood would look on the walls of our house," she says.

The Websters reported the scam to the FBI, which arrested the criminal in 2017. The man had targeted many older people; he had manipulated one 82-year-old woman into sending him $600,000.

Reporting scams isn't just about helping authorities nab criminals. It also helps reveal the size of the problem.

Crime-fighting resources depend in large part on victims' reporting. "If you live in a neighborhood and people start breaking into cars, you have to call the police and report it, because the police will patrol the neighborhood based upon the number of calls they're getting," McKenna says. The same applies to scams: "You have to report crimes to get protections."

But it's confusing to know where to report scams, with different agencies tracking them (FTC, Federal Communications Commission, Better Business Bureau), sometimes depending on the type of fraud.

AARP Fraud Watch Network experts recommend contacting your local police so you have an official record of the crime and the FBI's Internet Crime Complaint Center (IC3.gov). If you have questions, call the AARP Fraud Watch Network Helpline (877-908-3360).

Ken Budd has written for National Geographic Traveler, Travel+Leisure, The Washington Post Magazine and many more. He is the author of a memoir, The Voluntourist.

Phone Scams and Phishing Attacks

Phone Scams

CDC has become aware that members of the general public are receiving calls appearing to originate from CDC through caller ID, or they are receiving scammer voice mail messages saying the caller is from the Centers for Disease Control and Prevention (CDC). Some calls are requesting donations.

Downloadable apps and some free websites now make it simple for anyone to "spoof" a phone call and make it appear to come from any phone number. This is usually done by unscrupulous salespeople, in hopes that people are more likely to pick up the phone if the caller has a number similar to theirs.

Unfortunately, current technology doesn't make it easy to block these spoofed calls, either on business or personal phones. A spoofed call does not mean that anyone's telephone has been hacked, so you can simply hang up.

These calls are a scam and are referred to as "government impersonation fraud," meaning criminals are impersonating government officials for nefarious purposes. Scammers are becoming more sophisticated and organized in their approach. They are technologically savvy and often target young people and the elderly.

To protect yourself from falling victim to these scams, be wary of answering phone calls from numbers you do not recognize. Federal agencies do not request donations from the general public. Do not give out your personal information, including banking information, Social Security number or other personally identifiable information over the phone or to individuals you do not know.

You can also report these calls to the Federal Communications Commission (FCC).

Phishing Attacks

Malicious cyber criminals are always attempting to leverage interest and activity in public health emergencies to launch themed phishing emails. These phishing emails contain links and downloads for malware that can allow them to take over healthcare IT systems and steal information.

It is critical to stay vigilant and follow good security practices to help reduce the likelihood of falling victim to phishing attacks.

- Don't open unsolicited email from people you don't know.
- Be wary of third-party sources.
- Hover your mouse over links to see where they lead.
- Do not click links in emails. If you think the address is correct, retype it in a browser window.
- Be wary of attachments in any email.
- Do not supply any personal information, especially passwords, to anyone via email.

Additional resources:

- Department of Homeland Security Cybersecurity & Infrastructure Security Agency (DHS CISA)
- Federal Trade Commission (FTC) COVID-19 scams
- Department of Justice (DOJ)

If you spot a scam, report it to the ***FTC*** @ ReportFraud.ftc.gov.

Scammy texts offering "refunds" for Amazon purchases

Scammers are pretending to be Amazon again. This time, they're sending texts claiming there's a problem with something you bought. They offer a refund if you click a link — but it's a scam. Here's how the scam works so you can avoid it.

You get an unexpected text that looks like it's from Amazon. It claims the company did a "routine quality inspection" and an item you recently bought doesn't meet Amazon's standards or has been recalled. The text offers you a full refund and says you don't need to return the item — as long as you click a link to request your money back. But there is no refund. Instead, it's a phishing scam to steal your money or personal information.

To avoid a scam like this:

- **Don't click links in unexpected texts** — and don't respond to them. If you think the message could be legit, contact the company using a phone number, email, or website you know is real — not the info from the text.
- **Check your Amazon account.** If you're worried, log in through the Amazon website or app — don't use the link in the text — to see if there's a problem with or recall on anything you've ordered.
- **Send unwanted texts to 7726 (SPAM)** or use your phone's "report junk" option. Once you've reported it, delete the message.

Learn more about how to get fewer spam texts. And if you spot a scam, tell the FTC at ***ReportFraud.ftc.gov.***

How to Keep a Loved One With Cognitive Decline Safe From Scams

By Christina Ianzito, AARP

Key steps to protect vulnerable family members' finances in an age of rampant fraud.

Jessica, an event planner in Massachusetts, was surprised to discover last December that her 74-year-old mother, Joyce, was deep into text conversations with someone Jessica had never heard of. "My heart was racing," she says, describing what she was thinking after seeing the Google chat exchanges on her mom's phone on that Christmas Day. "I had no idea what I was looking at."

She eventually learned that her mom had spent nearly a year communicating with people she thought were the country star Vince Gill and his associates and had sent them more than $400,000. Joyce had even told her friends she was moving to Nashville to be near Gill — her spouse. They called each other "husband" and "wife."

Before discovering the scam, Jessica (who asked us not to use her or mother's full names, for privacy reasons), 42, had already begun to worry about her mom's cognitive decline, which a doctor recently diagnosed.

The crime and its repercussions

The scam began in the fall of 2022, after Joyce, a longtime Gill fan, posted a cheerful message on his Instagram page — "hope you come to Boston!" She then was inundated with "multiple people reaching out to pretend that they were him, his daughter or his manager," who'd ask her to talk to them on private chat platforms like Telegram, according to Jessica. (Scammers inundate many stars' social media accounts; I posted a simple "love this!" on one of Gill's Facebook posts and received multiple entreaties to chat privately from bogus Gill fan accounts.)

Jessica, Joyce's only child, has spent the months since trying to sort through the wreckage that is now her mother's finances. She's convinced that Joyce was more vulnerable to these scammers because of her cognitive issues, which may have clouded her judgment and made her more likely to respond to some wild requests. At one point "Gill" told Joyce that he needed money because he was getting a divorce from his wife, Amy Grant, who had frozen his bank accounts.

Jessica and a social worker staged an intervention. She says, "I took the checkbooks, the credit cards, everything, and I said, 'Here's an allowance for now.'" She's been trying to track all the money lost on a detailed spreadsheet, including a series of loans Joyce took out to pay the scammers. She's also wrestling with the tax implications and other fallout from the crime. "Even now, months later, I'm still finding [losses], so it's kind of a moving target," she says.

Cognitive impairment and fraud

Someone certainly doesn't need to have dementia to become a scam victim. "It's important to understand that this can and does happen regardless of cognitive impairment," notes Kathy Stokes, AARP's director of fraud prevention programs. "These fraud criminals have a playbook. And the playbook works against

Continued on next page

anybody, regardless of age, education, any other demographic characteristic."

That said, "absolutely," one of the first signs of cognitive decline is a change in financial behavior, notes Sarah Lock, AARP's senior vice president for policy and brain health. "You may notice that the person who's been meticulous in their financial affairs suddenly becomes less so."

An analysis of more than 81,000 Medicare beneficiaries' health data found that people who were later diagnosed with dementia were more likely to experience drops in their credit scores and miss bill payments than those who weren't. Problems started as early as six years before the diagnosis, according to the 2020 Johns Hopkins University study,

And a 2016 study published in the Journal of Alzheimer's Disease found that older adults with mild cognitive impairment are more susceptible to scams, particularly when they displayed slower processing speed and lower short-term memory. Co-author Duke Han, Ph.D. a professor of psychology and family medicine at University of Southern California, explains in an email that if an older adult is cognitively slower, they "may have difficulty keeping track in a high time-pressure situation." With memory issues, they "may be more easily led to misremember events or facts. These cognitive difficulties can reflect brain changes that make it more difficult for an older adult to discern a scam from a legitimate situation."

Ian Bednowitz, 46, general manager for identity and privacy at Gen Digital, maker of Norton and LifeLock identity theft protection, among other products, also saw his late mother become a fraud victim when she had cognitive decline. In 2015 her paid caregiver stole her personal information, including her Social Security number as well as balance transfer checks from her mail. The caregiver wrote the checks to herself, which meant she took out a fraudulent loan for thousands of dollars against his mother's credit card limit. The unusual charges led him to check her credit report and "my heart just sank, because there were all kinds of loans and credit cards and things in her name that she had nothing to do with, with high balances on them. It was tens of thousands of dollars." (Authorities did eventually catch the criminal, whom he says was part of a crime syndicate that preyed on vulnerable older people.)

Bednowitz says he wishes he'd been aware of the different steps he could have taken that may have helped prevent the crime.

Where to begin

If you're concerned, it's crucial to "start to talk about money, start to talk about scams," says Darius Kingsley, head of consumer banking practices at Chase. "That sounds obvious, but a lot of older Americans — that's a generational thing — don't want to talk about money. So you've got to explain the threat [of scams] and tell them you want to help keep them safe. You're not trying to be intrusive. You're not trying to be condescending." (See below for the scam-prevention basics that you can emphasize.)

Some older adults who are accustomed to independence may resist their adult child becoming involved in their financial affairs. "My mom was very stubborn," says Bednowitz. "She hated me taking care of anything for her." But if he approached her carefully — suggesting he pay her bills without having control of her account, for example — "she was OK being helped. I think it has to feel like help and not control."

How intrusive you need to be will depend on your parent's level of cognitive decline. In an ideal world, they would have designated someone they trust — maybe their child — to serve as their financial advocate under a power of attorney before they become unable to make financial decisions. For that to happen, though, "the parent has to really trust you as the individual," says Bednowitz, who notes the sad fact that when elder theft is perpetrated by someone the victim knows, it's most often a family member.

More ways to protect a loved one with (or without) cognitive decline from fraud

"We hear from our customers all the time where [they] were on the road to being scammed, and they caught it within the family," says Kingsley. "Very often that's because the adult child has been proactive."

Continued on next page

Secure all personal documents in the home. To avoid fraud perpetrated through stolen documents, as Bednowitz's mom experienced, make sure sensitive information — tax returns, passports, bank statements — is out of sight, whether it's in a physical safe or only accessible online. Bednowitz says he began redirecting his mother's mail to a paid service that scans and digitizes it for him to view online, "so it would come out of the hands of the caregivers." (She had access to it as well.)

Set up "unusual activity" alerts on your loved one's financial accounts. Different banks have different kinds of available account-activity alerts, which allow the account holder to receive texts, emails, or mobile push notifications for large withdrawals and/or other activity. It's a good idea to sign up for all available alerts, which you can do by logging into the account online or through the bank's app.

Ask if you can receive copies of their bank statements. Lock says that when her father was experiencing cognitive decline, she arranged to have a second set of financial statements sent to her, "so I could watch the patterns of your accounts to see if anything unusual was happening."

Consider using a service that can identify potential fraud. You can help your loved one subscribe to services like Aura, Identity Guard, and Lifelock by Norton that alert you to potential identity theft, such as someone applying for a credit card or loan in your name. AARP members can receive a discount on some Norton identity theft protection products.

Ask to be your loved one's trusted contact. You can be added as a "trusted contact" at their financial firm (they may have already added you when they opened the account). You won't be able to access the money, but it allows the financial institution to alert you if they notice suspicious activity.

Help them freeze their credit report. A freeze prevents anyone from opening a credit account in their name; they can quickly unfreeze it if they do need someone to access it — to get a loan approved, for instance.

Set up robocall blocking and SMS blocking. Scammers often try to reach potential victims through illegal robocalls (some robocalls are legal, but only if they are for informational or noncommercial purposes). Your phone service provider may offer free robocall-blocking tools. The website of CTIA, a Washington-based trade association that represents the U.S. wireless industry, has lists of apps for Android and Apple devices that block robocalls and spam texts.

Share scam-prevention basics. Tell your loved one about these keys to avoiding fraud — rules that everyone should keep in mind.

1. Be very wary of all unsolicited communications. Don't answer calls or texts from unknown numbers. "I tell my own parents, 'Be inherently suspicious of phone calls or random texts,'" says Kingsley. "You've got to train them to get their guard up — don't assume that if someone is contacting them it's legit."

2. Keep your personal/sensitive information private. If someone wants your bank account details or Social Security number, think twice. Make sure your social media accounts are private, and don't accept friend requests from people you don't know.

3. Talk to someone you trust if something seems off. It's important for people to have a go-to person who can be a sounding board — whether it's you or a friend or neighbor, says Kingsley. He suggests telling a loved one, "Before you panic, before you give out personal information or bank account details, talk to me about it or talk to your trusted circle, and say, 'Hey, does this seem right? Does it seem legit?'" And if the person who contacted you says not to talk to anyone about your interaction? That's a huge red flag that you're dealing with a scammer and should tell someone

Christina Ianzito covers scams and fraud, and is the books editor for aarp.org and AARP The Magazine. Also a longtime travel writer and editor, she received a 2020 Lowell Thomas Award for travel writing from the Society of American Travel Writers Foundation