SCAM AND FRAUD PREVENTION

How to Avoid an Online Scam: 5 Ways to Protect Yourself

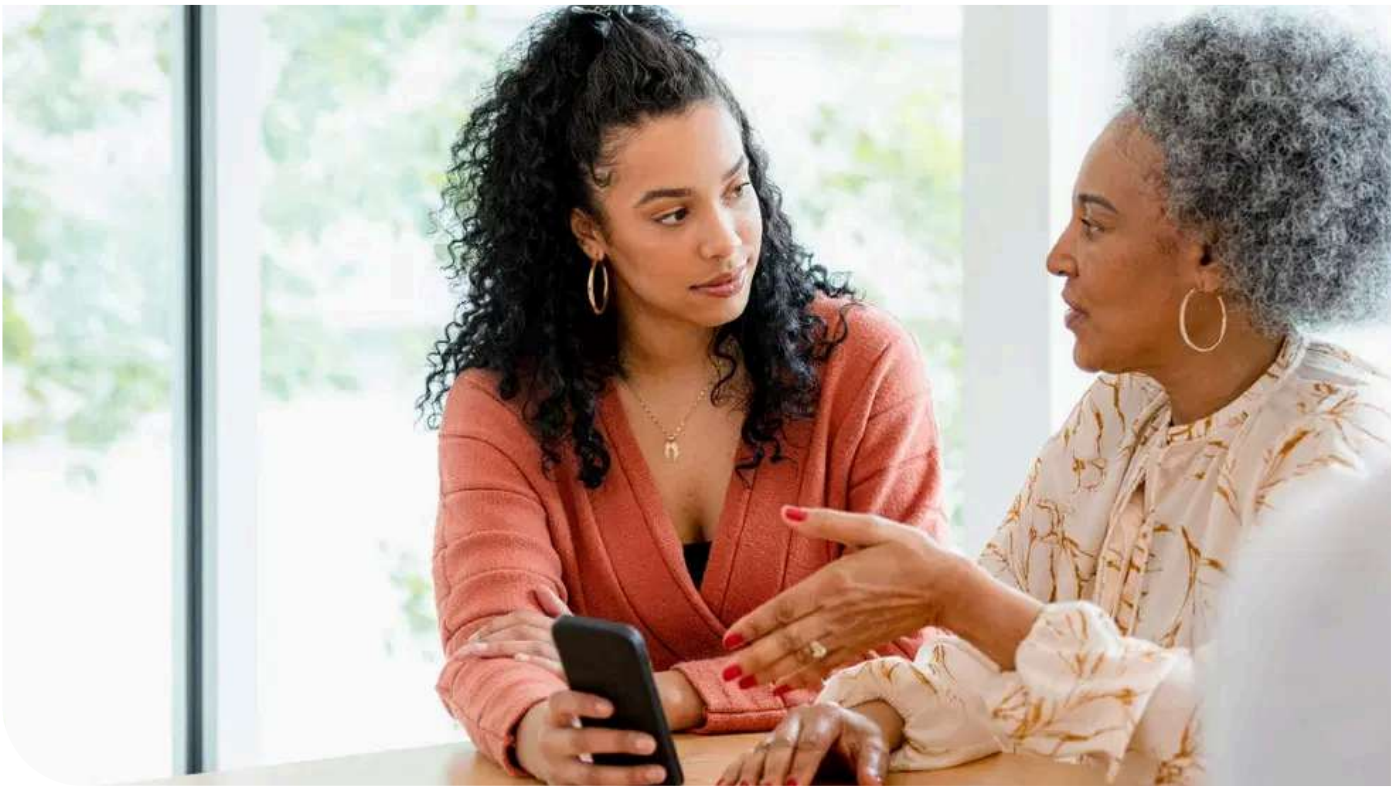
Jul 17, 2024 7 min read

KEY TAKEAWAYS

Scammers are getting more sophisticated and skilled at targeting older adults. A scam can happen to you—even if you don't think you're at risk.

Understanding the psychological tricks scammers use to manipulate consumers can help you beat them at their own game.

If you think you've been scammed, report it to a reputable agency. Your story can help them build a case against scammers and take action.



We'd all like to believe we could spot an online scam a mile away. But the truth is that con artists and cybercriminals are getting craftier and more sophisticated by the day. It's their full-time "job" to deceive, exploit, and swindle consumers.

It happened to Alice Lin. As reported by KCAL News, the 80-year-old widow received an unexpected message from a man on the app WeChat. A good friendship seemed to blossom, and her new friend persuaded her to download a cryptocurrency trading app. In the end, Lin lost more than $700,000 after emptying her retirement and savings accounts to invest in what appeared to be a promising financial opportunity.

Online scams can happen to anyone—even those who consider themselves too smart to get duped. According to the FBI FBI Internet Crime Complaint Center (IC3), $3.4 billion in total fraud losses were reported by people over age 60 in 2023, up 11% from 2022. The most shocking number? The average loss per scam victim: Nearly $34,000.[1]

"The retirement security of Americans across the board is at risk," said Christine Kieffer, Senior Director of the FINRA Investor Education Foundation, during a panel at Age + Action 2024. "And we have international crime syndicates behind a lot of the scams that are growing. This is a problem that needs everybody's attention."

Why are scammers so successful in finding victims? One reason is they know how to use human psychology their advantage.

What tricks do scammers use to target older adults?

Thieves use several psychological tactics to gain a victim's confidence and manipulate them into doing what the thief wants. Knowing the techniques scammers use—and how to combat them—can help you beat them at their own game.

How are psychological tricks used in payment scams that target seniors? Below are the top five.

1. Targeting those who are socially isolated

Many older adults live alone. This social isolation can lead to loneliness, which makes some people more eager to interact with a friendly voice on the other end of the phone (or email or text message). Scammers are skilled at using "grooming" tactics to exploit the person they're targeting. This involves creating a deep sense of trust, uncovering that person's vulnerabilities, and using this information to manipulate them for their own personal gain.

What's more, scammers know older adults in solo households are less likely to talk a situation through with another person who may realize something is off.

> **How to protect yourself:** If you're unsure about the person you're talking to or what you're being told, ask a friend or family member for advice before taking any further steps. Sending a quick screenshot of a text, or simply walking through the scenario with someone you trust, can often help you see things more clearly.

2. Posing as an authority figure

Most people, especially those of older generations, were taught to respect authority. That's why many payment scams are carried out by thieves impersonating people and organizations you would normally trust without question—such as a government agency (e.g., the IRS), charities, debt collection agencies, your utility company, or even your financial institution. In what's referred to as an imposter scam, the caller explains that a bill is overdue. They try to trigger feelings of fear and anxity by threatening harsh consequences if you do not immediately pay what you "owe."

> **How to protect yourself:** The first step you should take is confirm whether a company or agency trying to reach you is legitimate. This can be done by hanging up and contacting them using phone numbers or email addresses listed on their official website. If there is a problem you need to address, they will be able to help. Other tips for avoiding this type of payment scam include:

- **Do not rely on caller ID**, since it can be spoofed to look like a familiar organization (e.g., the SSA or your bank) is calling you.

- **Do not grant remote access** (the ability to control your computer or device from another location) to anyone unless the request comes from a verified source. Most tech support brands will not reach out to you unsolicited or request personal information.

- **Do not give out sensitive information** such as bank account details or your Social Security number over the phone—unless you initiated the contact.

"You should be very leery of any emails, calls, or text messages that claim to be coming from their financial institution, government agencies, or other legitimate companies you do business with," said Soo-Lynn Getz, Director of Fraud Prevention at Zelle®. "These kinds of institutions rarely use informal ways to communicate important information that requires immediate action or implies serious consequences. When in doubt, pause, ask questions, and locate the officially listed number of your financial institution, government agency, or other legitimate institution from their websites—not links that are provided by the potential scammer. Hang up or disconnect with the chat session and call a trusted number before sending any funds."

3. Impersonating a trusted organization

Imposter scams don't always involve government organizations. For instance, in a business imposter scam , criminals pose as well-known companies and take advantage of consumers' trust in that brand. While these kinds of phishing schemes can be conducted in the name of any company, Amazon is the most common business impersonated by scammers.

> **How to protect yourself**: As with other imposter scams, it's important to practice healthy skepticism. Look out for red flags like poor grammar and spelling and strange-looking links shortened with bit.ly or a similar service.

Any requests for payment via cryptocurrency, online payment apps, prepaid debit cards, or gift cards are suspicious, since these are telltale signs of a scam.

If you think a communication you receive may be valid, verify the information by checking with official trusted sources (e.g., calling a phone number found on a company's website or brochure). Never send money or personal information to someone whose identity you are not able to verify.

4. Creating a sense of urgency or scarcity

Scammers will often try to rush you into making decisions or providing information. To do this, they create a sense of urgency around the situation so that you're more likely to act impulsively. They may say an offer is good for a limited time only, a product is about to run out, or that you must make a payment immediately to prevent negative consequences. Their goal is to put the squeeze on—so you don't have time to think carefully about what they're asking of you.

How to protect yourself: Don't be afraid to slow down and ask questions. Give yourself enough time to think through the situation logically, which will prevent you from making snap decisions. It's also important to harness your inner skeptic. If a product you want is being offered at a suspiciously low price, ask to see it in person and get a service contract to protect yourself (if applicable). Bottom line: if something seems too good to be true, it probably is.

When you do buy products online, make sure you only use a payment option that offers reimbursement for authorized payments (such as most major credit cards). Using a form of direct payment, such as a payment app, is essentially the same as sending cash. You may not be able to receive a refund.

5. Tapping into the desire to help others

If you're like most people, you want to help someone who is in trouble. This is especially true when that "someone" is a person you care about, such as a grandchild or romantic interest. Certain scams, such as the grandparent scam and romance (or sweetheart) scam, capitalize on this tendency.

With the grandparent scam, for example, someone calls you pretending to be your grandchild and claiming they're in dire straits. They need money to get out of jail (or pay urgent medical bills), and they're pleading with you to help.

> **How to protect yourself:** In any scenario where you're being asked for money or personal information, take a moment and ask, "Why?" If you've been contacted out of the blue, you want to first verify the call is coming from the person the caller is claiming to be. Hang up and call back from your saved phone number of the contact, or email from a saved address to avoid typos.
>
> If you do send money to someone you know, make 100% certain you're sending it to the right person—especially if you use a payment app, which does not allow cancellation. Double-check that you have their correct information before you make the transaction. Above all, don't send money you're uncomfortable losing or outright cannot afford to lose. It's important to remember that someone who truly cares about you would not put you in the position of putting your finances at risk.

The strategies above can help you spot scams early on. But what if it's too late? What if you've already fallen for a fraudster's trickery?

Report scammers to protect yourself—and others

"If you realize you have been scammed, you should contact your financial institution to report the details of what happened," Getz explains. "You can also report the scam details to government agencies like the FBI or FTC, because the U.S. government's focus on identifying and holding these scammers accountable is growing."

I also highly recommend sharing the story with friends and family; this will help them cement the red flags in their memory and ensure their loved ones can recognize them, too," Getz continued.

Where do you report a scam?

Try these reputable resources that allow you to make a report online:

- BBB Scam Tracker (Better Business Bureau®)
- FBI Internet Crime Complaint Center (IC3)
- Federal Trade Commission (FTC)

Source

1. Federal Bureau of Investigation Internet Crimes Complaint Center. Elder Fraud Report 2023. Found on the internet at https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3ElderFraudReport.pdf

Top 5 Financial Scams Targeting Older Adults

Financial scams targeting older adults can be devastating, leaving you in a vulnerable position and without time to recoup your losses. Learn how to identify and stop the top 10 financial scams.

Explore More →