Protecting Yourself from Senior Fraud

What Every Retiree Needs to Know

Financial fraud targeting seniors costs Americans over $3 billion every year — and that number only reflects reported cases. This guide gives you the knowledge to recognize threats before they reach you, and the steps to take if they do.

Why Seniors Are Targeted — And How Often It Happens

Financial fraud targeting seniors costs Americans over $3 billion every year according to the FBI — and that number only reflects reported cases. Most incidents go unreported because victims feel embarrassed, confused about what happened, or unsure who to tell.

The reason seniors are disproportionately targeted is straightforward: they tend to have accumulated savings, receive regular income from Social Security or pensions, and may be less familiar with the tactics fraudsters use today. Scammers also count on the fact that many seniors live alone, making it easier to manipulate without interference from family members.

Understanding how these scams work is your single most effective defense. You cannot be defrauded by a scheme you recognize.

What's Changed — And Why It's Harder Than Ever to Spot

Fraud targeting seniors isn't new. But the tools scammers use today are. Artificial intelligence can now clone a family member's voice from just a few seconds of audio found online. Scammers can make a phone call appear to come from your bank, your doctor's office, or even the Social Security Administration. Fake websites look identical to legitimate ones. Emails arrive with perfect grammar and official-looking logos.

This means your instincts matter more than ever. If something feels off — trust that feeling. Ask yourself one simple question: *Why is this person contacting me when I never contacted them?* Legitimate institutions rarely initiate unexpected contact demanding immediate action. Scammers always do.

The Most Common Scams Targeting Seniors Right Now

1. Government Impersonation Scams

Someone calls claiming to be from the Social Security Administration, IRS, or Medicare. They tell you there's a problem with your account, that your benefits are being suspended, or that you owe back taxes. They create urgency and demand immediate payment — often by gift card, wire transfer, or cryptocurrency. The reality: government agencies do not call you unexpectedly demanding immediate payment. If you receive a call like this, hang up and call the agency directly using the number on their official website.

2. The Grandparent Scam — Now Powered by AI

You receive a call from someone who sounds exactly like your grandchild or child. They tell you they're in trouble — arrested, in an accident, stranded abroad — and beg you not to tell anyone else in the family. They need money immediately. What you're hearing may not be your loved one at all. Using artificial intelligence, scammers can clone a person's voice from as little as a few seconds of audio gathered from social media videos or voicemail greetings. If you receive a call like this, hang up immediately and call your family member directly on their known number. Establish a family code word that only real family members would know.

3. Medicare and Health Insurance Fraud

Someone contacts you offering free medical equipment, tests, or services in exchange for your Medicare number. Once they have it they bill Medicare for services never rendered, and your coverage can be compromised as a result. Guard your Medicare number the same way you guard your Social Security number — it is just as valuable to a fraudster.

4. Romance Scams

These are among the most financially devastating scams affecting seniors. A stranger makes contact online — through social media, email, or a dating platform — and invests weeks or months building a relationship. They are warm, attentive, and convincing. Eventually a financial crisis emerges and they ask for help. They will never meet you in person. They do not exist as presented. The FBI reports that seniors lose more money to romance scams than any other age group.

5. Tech Support Scams

A popup appears on your computer warning that your device has been compromised. A phone number is displayed. When you call, a convincing technician walks you through giving them remote access to your computer — and your financial accounts. Microsoft, Apple, and legitimate tech companies do not send unsolicited popups asking you to call them.

6. Lottery and Prize Scams

You're told you've won a prize, sweepstakes, or lottery — but must pay fees, taxes, or processing charges to collect your winnings. No legitimate prize requires you to pay money to receive money. If you have to pay to collect a prize, it isn't a prize.

7. Utility and Service Shutoff Scams

Someone calls claiming your electricity, water, or gas will be shut off within hours unless you pay immediately by an untraceable method. Legitimate utility companies send written notices well in advance and offer multiple payment options. Hang up and call your utility company directly using the number on your bill.

Warning Signs That Apply to Every Scam

No matter what form a scam takes, the tactics behind it are remarkably consistent. Fraudsters rely on a short list of psychological triggers because they work. Learning to recognize them is more valuable than memorizing every individual scam type.

- **Urgency and pressure.** You are told you must act immediately — within hours or even minutes. Legitimate institutions give you time to think, verify, and consult with family. The moment someone tells you there is no time to think, slow down.
- **Secrecy.** You are told not to tell anyone — not your spouse, your children, your bank. Scammers isolate victims deliberately because they know a second opinion would end the fraud immediately.
- **Unusual payment methods.** You are asked to pay by gift card, wire transfer, cryptocurrency, or by mailing cash. These methods are untraceable and irreversible. No government agency or legitimate business will ask you to pay this way. Ever.
- **Unsolicited contact.** The contact came to you — you did not initiate it. Ask yourself: why is this person contacting me? Legitimate organizations rarely initiate unexpected contact demanding immediate action.
- **Threats and fear.** You are told you will be arrested, your benefits cut off, or your account closed if you don't act. Fear shuts down rational thinking — which is exactly the intent.
- **Requests for personal information.** You are asked for your Social Security number, Medicare number, bank account details, or passwords. No legitimate organization needs to ask for information they should already have.
- **Something just feels wrong.** Trust that feeling. Your instincts are a valid and important defense.

A Simple Rule to Remember: If a contact is unexpected, creates urgency, demands secrecy, or asks for money or personal information — stop. Hang up, close the window, or walk away. Then independently verify by contacting the organization directly using a number you look up yourself, never one provided by the caller.

If You Think You've Been Targeted — What to Do Right Now

If you are currently on a call that feels wrong, hang up. You do not owe anyone an explanation. No legitimate caller will be offended by you saying you need to verify the information before proceeding.

If you haven't sent money or shared information yet:

- Hang up or disengage immediately
- Do not call back any number the caller provided
- Look up the organization's official number independently and call to verify
- Tell a trusted family member or friend what happened

If you have already sent money:

- Act immediately — time matters, especially with wire transfers
- Contact your bank or credit card company and report it as fraud
- If you paid by gift card, call the gift card issuer directly
- If cryptocurrency was involved, contact the exchange — though recovery is unlikely
- If you shared your Social Security number, contact the SSA at 1-800-772-1213
- If you shared Medicare information, call 1-800-MEDICARE

If you shared personal or financial information:

- Place a fraud alert or credit freeze with Equifax, Experian, and TransUnion
- Monitor your accounts closely for unauthorized activity
- Change passwords on any accounts that may be compromised

Report it — even if you feel embarrassed:

- Federal Trade Commission: reportfraud.ftc.gov
- FBI Internet Crime Complaint Center: ic3.gov
- Your state's attorney general office
- Local law enforcement

A Note on Embarrassment

Most fraud victims feel ashamed. The truth is these scams are professionally engineered to work on intelligent, careful people. The voice clone of your grandchild is indistinguishable from the real thing. The urgency is designed to override rational thinking. Being targeted is not a reflection of your intelligence — it is a reflection of how sophisticated these operations have become.

You Don't Have to Face This Alone

Knowing a scam exists and knowing exactly what to say and do when you're in the middle of one are two very different things. Most people freeze. The urgency is real, the emotion is real, and in the moment it's hard to remember what steps to take.

That's why we put together the **Senior Fraud Response Kit** — a companion guide with word-for-word call scripts, email and letter templates, a step-by-step action plan by scam type, and a documentation checklist. Everything you need to respond quickly and effectively when it matters most.

Available at **seniorlifeguides.org**

This guide is provided for educational purposes. Senior Life Guides is not a law firm and this content does not constitute legal advice. If you believe you are the victim of fraud, contact local law enforcement and appropriate financial institutions immediately.