INSOUTH BANK Member FDIC

Member FDIC

THE INSIGHT

Quarterly Newsletter for the Seasoned Adult

1st Quarter 2026

How Scammers are Stealing Life Savings & How to Protect Yourself

According to the Federal Trade Commission, recent reports show a growing wave of scams aimed squarely at retirees' life savings. These scammers pretend to be from known and trusted government agencies and businesses. These scams use fake security alerts and other false alarms to prey on older adults' vigilance about protecting their money and identity to steal it from them. Some people have reported emptying out their bank accounts and even clearing out their 401Ks because of this scam.

From 2020 to 2024, the number of reports from older adults who lost $10,000 or more to these scams increased more than fourfold. These high-loss scams typically start with a (fake) story that gets your attention with one or a combination of these lies:

- **Lie #1**: Someone is using your accounts. This lie might start with someone pretending to be your bank, flagging so-called suspicious activity or pretending to be Amazon with a message about an unauthorized purchase.
- **Lie #2:** Your information is being used to commit crimes. This lie may come from a supposed government officer or agent, warning that your Social Security number is linked to a crime like drug smuggling, money laundering, or even child pornography.
- **Lie #3:** There's a security problem with your computer.   This lie often starts with a fake on-screen security alert that looks like it's from Microsoft or Apple with a number to call. If you call, they say your online accounts have been hacked.

These scammers say the only way out of the (fake) crisis is to follow their instructions – which will include sending money to the scammers. They may say this will keep your money safe, secure your identity, clear your name, or help catch the criminals. There may be layers of complexity to the story, but it's all a lie aimed at draining your accounts. Reports show that when people think they are fixing a problem rather than sending a stranger money, their losses are often limited only by their available funds.

Lots of scams are now carried out online, but these scams still depend on a phone call. Even when they don't start with a call, reports show the goal is to get you on the phone. A call is still the best way to dial up the fear and the urgency so it's harder for you to think clearly and check things out. Keeping you on the phone is also designed to keep you from talking to anyone who could help – a friend or family member in a calmer state of mind who might see through the lies.

Scammers pretend to be businesses and agencies, including banks, Microsoft, and the Social Security Administration. Often, they tag team you: maybe starting with a pop-up security alert impersonating Microsoft and then transferring you to someone pretending to be from the FTC for "help" with a fake identity theft problem.

The security of your accounts, along with the risk of identity theft, are real concerns that real companies might call you about. So how can you stay vigilant and steer clear of these scams?

- **Don't move money to "protect it."** Never transfer or send money to anyone, no matter who they say they are, in response to an unexpected call or message. Even if they say it's to "protect it."
- **Hang up and verify.** Hang up the phone and call the company or agency directly using a phone number or website you know is real. Don't trust what an unexpected caller says, and never use the phone number in a computer security pop-up or an unexpected text or email.
- **Block unwanted calls.** Stop many of these scammers before they reach you.

Safeguard yourself against scams with these tips:

- **Block unwanted calls and text messages.**
- **Don't give your personal or financial information in response to a request that you didn't expect.** Honest organizations won't call, email, or text to ask for your personal information, like your Social Security, bank account, or credit card numbers.
- **If you get an email or text message from a company you do business with and you think it's real, it's still best not to click on any links.** Instead, contact them using a website you know is trustworthy. Or look up their phone number. Don't call a number they gave you or the number from your caller ID.
- **Resist the pressure to act immediately.** Honest businesses will give you time to make a decision. Anyone who pressures you to pay or give them your personal information is a scammer.
- **Know how scammers tell you to pay.** Never pay someone who insists that you can only pay with cryptocurrency, a wire transfer service like Western Union or MoneyGram, a payment app, or a gift card. And never deposit a check and send money back to someone.

Information provided from https://consumer.ftc.gov/articles/how-avoid-scam & https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/08/false-alarm-real-scam-how-scammers-are-stealing-older-adults-life-savings

You're Never a Burden — We're Here to Help

If something doesn't feel right, please don't feel embarrassed or afraid to call us. Scams are becoming more common, and according to AARP.com, older adults reported losing nearly $4.9 billion to scams and fraud in 2024, with more than 147,000 complaints submitted by people aged 60 and older. These situations can happen to anyone. At INSOUTH Bank, our goal is to protect your personal information and your hard-earned money to the very best of our ability. We are always happy to listen, answer questions, and help you decide what steps — if any — should be taken. No concern is too small. If you receive a call, text, email, or request that worries you, please don't hesitate to contact your local INSOUTH branch. We are here to support you and help keep you safe.

If you or a loved one suspects scam or fraud, please **contact us immediately**.

Millington - (901) 872-4545
Atoka - (901) 837-9675
Covington - (901) 476-3330
Brownsville - (731) 772-1201
Memphis - (901) 747-5555
Jackson - (731) 574-2500

Holiday Hours Notice

Just a friendly reminder that INSOUTH Bank will be closed in observance of the following holidays. You can still access your accounts anytime through online and mobile banking.*

Presidents' Day: Monday, February 16th
Good Friday: Friday, April 3rd
Memorial Day: Monday, May 25th
Juneteenth: Friday, June 19th

*Message and data charges may apply with your cellular provider. Registration required. Online and Mobile Banking may be subject to additional terms and conditions and/or third party service provider fees. Registration and approval required for mobile deposit.