August 2025

Consumer Protection Data Spotlight
FTC reporting back to you

False alarm, real scam: how scammers are stealing older adults' life savings

Reports to the FTC 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. And, in an ironic twist, recent scams use fake security alerts and other false alarms to prey on older adults' vigilance about *protecting* their money and identity to steal from them.[1] Some people 60+ have reported emptying their bank accounts and even clearing out their 401ks.

While younger people report losing money to these imposters too, reports of losses in the tens and hundreds of thousands of dollars are much more likely to be filed by older adults,[2] and those numbers have soared. From 2020 to 2024, the number of reports from older adults who lost $10,000 or more to these scams increased more than fourfold.[3] When older adults reported losing more than $100,000, the trend was even more striking: during the same period, the number of reports increased nearly sevenfold, and the combined reported losses went up eightfold.

These high-loss scams typically start with a (fake) story that gets your attention with one or a combination of these lies:

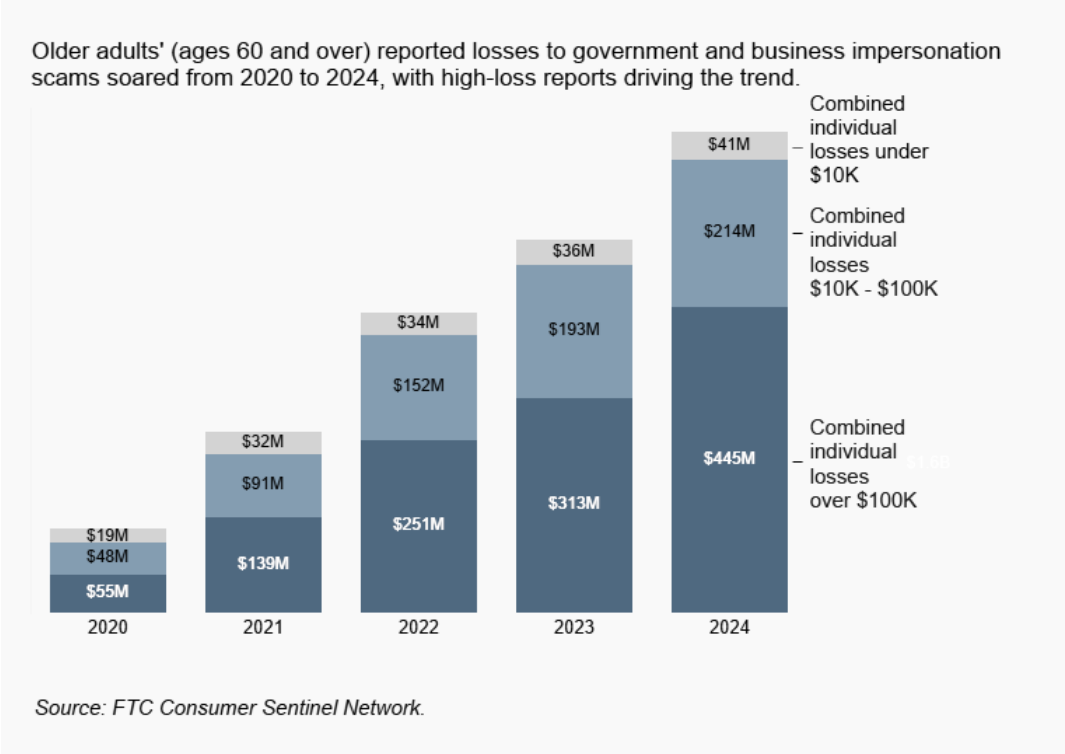
- **Lie #1: Someone is using your accounts.** This lie might start with someone pretending to be your bank, flagging so-called suspicious activity, or pretending to be Amazon with a message about an unauthorized purchase;
- **Lie #2: Your information is being used to commit crimes.** This lie may come 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; or
- **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.[4] 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.

In another layer of irony, these scammers often pretend to be the FTC, the nation's consumer protection agency, sometimes impersonating real staff. Reports show these scammers have told people to transfer money out of their accounts, deposit cash into Bitcoin ATMS, and even hand off stacks of cash or gold to couriers[5] – all things the real FTC will *never* do. Scammers also pretend to be other 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.** Learn about your call blocking options to stop many of these scammers *before* they reach you.

Learn more about imposter scams. To spot and avoid scams – and learn how to recover money if you paid a scammer – visit ftc.gov/scams. Report scams to the FTC at ReportFraud.ftc.gov.

The FTC uses reports from the public to investigate and stop fraud, for consumer education and outreach, and for analyses like this. File your fraud report at ReportFraud.ftc.gov. To explore Sentinel data, visit FTC.gov/exploredata.

1 A 2023 Gallup poll asked Americans how much they worry about various types of crime. The results showed people most often worried about being a victim of identity theft. Being tricked by a scammer into sending money or providing access to a financial account was the second highest concern. See Gallup.com, Scams: Relatively Common and Anxiety-Inducing for Americans (November 2023).

2 In 2024, losses to business imposter and government imposter scams of $10,000 and over were more than twice as likely to be reported by older adults, with losses over $100,000 three times as likely to be reported by older adults. This comparison of older and younger consumers' reporting rates is normalized based on the population size of each age group using the Census Bureau's 2019-2023 American Community Survey 5-Year Estimates. This excludes reports that did not include consumer age information.

3 The total number of business imposter and government imposter reports filed by older adults with a loss of $10K or more are as follows: 1,790 (2020), 3,516 (2021), 5,559 (2022), 7,091 (2023), 8,269 (2024).

4 In 2024, 41% of older adults who reported losing $10K or more to a business or government imposter scam indicated a phone call was the initial contact method, 15% indicated the scam started with an online ad or pop-up, and 13% said it started with an email. Reports indicating online ad or pop-up as the contact method typically described pop-up security alerts impersonating Microsoft or Apple with a number to call.

5 In 2024, 33% of older adults who reported losing $10K or more to a business or government imposter scam indicated cryptocurrency was the method of payment, followed by bank transfer (20%), and cash (16%). Most reports that identified cryptocurrency as the payment method mentioned Bitcoin ATMs in the report narrative. Although gold is not a payment method consumers can select, in about 5% of reports with losses of $10K or more (and about 21% of reports with losses over $100K) gold was written in as the payment method and/or mentioned in the complaint narrative. Note that when losses exceeded $100,000, bank transfer was the most frequently reported method at 32% of reports.