

Headline: Four Do's and Don'ts to Protect Seniors Against Identity Theft

It has been a problem, and it's getting worse: Seniors are most likely to fall victim to identity theft.

People ages 50 and older accounted for nearly half—45 percent—of identity theft complaints, according to the Federal Trade Commission's [Consumer Sentinel Network Data Book](#). And that number has been increasing, from 38 percent in 2013 and 42 percent in 2014.

And it's the younger end of the older generations who are the most victimized: Those between the ages of 50-59 were victimized more than any other group last year, according to the FTC. About a quarter—24 percent—of all identity theft complaints came from 50- to 59-year-olds. That compares with 17 percent two years ago.

Experts say there are a number of reasons that older people are more susceptible.

First, seniors are more trusting of people, and more trusting online. A 2013 study by the IT security firm McAfee found [that 88 percent of Americans older than 50 are more likely to share personal information](#) online than their children or grandchildren. According to the study, an estimated 26 percent of older respondents have shared their home address and more than 50 percent have shared their email address online.

People in their retirement years also have other habits or circumstances that make them susceptible to identity theft. They use paper checks more often, which gives identity thieves a wealth of information that makes theft easier. They are more likely to have caretakers in their homes. And people over 50 also have more money than younger people—and identity thieves go where the money is.

There are steps that everyone can take to make them less vulnerable to identity theft. Here are some that older people should pay special attention to:

1. Don't give personal information in an unsolicited phone call. If the phone caller says that he or she is from your bank or a creditor, hang up and call the business at the number on its website to see whether the business needs information from you.
2. Don't click on a link in any email you get that says something like "your account is about to be canceled!" and supply any personal information. Legitimate businesses would not ask for personal information in such an unsecured manner.
3. Don't share personal information — even your birth date — on your Facebook page or through any other social media. Thieves can use that information in combination with other information to commit identity theft.
4. Do routinely check credit reports to see whether anything is amiss. Every year get your free credit report at annualcreditreport.com. Also consider enrolling in a monitoring program like IDT911's Fraudscout program.

If you suspect you're a victim of identity theft or wish to proactively manage your identity, check with your insurance company, financial institution, or employee benefits provider. Many companies offer identity services from IDT911 for low or no cost.