HARTFORDFUNDS

Our benchmark is the investor.®

The Data Doesn't Lie —Raise Your Phone Scam Awareness

By Laurie M. Orlov

It's pretty easy to be scammed. My husband and I (both 50+ tech veterans) were targets of identity theft a few years ago. How did we know? We got a letter from the IRS saying they were reviewing our request for a tax refund. At first, we were concerned because it looked official. But we knew it was a scam because when we received the letter, we hadn't filed our taxes.

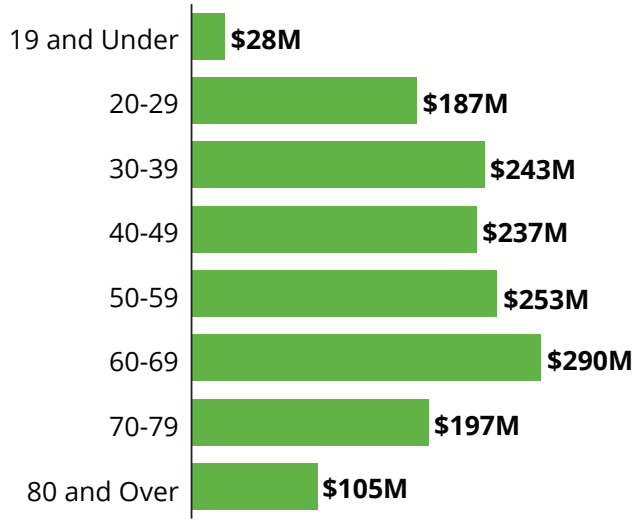
Unfortunately, many people don't discover scams until it's too late. In terms of scams, phone scams are the worst: They resulted in $20 billion in losses in 2020, $9 billion more than in 2019.[1] And the scam problem is probably bigger than it seems since only one in 44 scams is ever reported.[2] Financial losses from scams in total are worse for aging adults (see Figure 1).

What We'll Cover

- Why phone scams are so effective
- Three top phone scams
- Tips to help protect you from phone scams

Figure 1 Aging Adults Lost the Most

Reported frauds and losses by age in 2020



Source: Federal Trade Commission, 2020

First: Why Phone Scams Are So Effective

Phone scammers are extremely crafty, learning their techniques through rigorous training programs. Successful scammers target and prey on individuals who are viewed as more likely to fall for a scam and capitalize on their vulnerability.[3]

- **It's a comparatively good-paying job for young people in large foreign countries**
  Professional scammers go through extensive training and they're provided scripts that are known to be effective. For example, they may say they owe you a refund for computer software you purchased that's been discontinued. Next, they may suggest giving them remote access to uninstall the software. Then, they may ask their victims to log in to their bank account to receive the refund. Once they get remote access to a bank account, the scammer may steal funds or lock the victim's computer until they send money.
- **Caller ID spoofing makes the call appear to be local**
  Caller ID spoofing is the process of changing the Caller ID to any number other than the actual calling number. The number may look as though it's coming from a government agency, business, or even someone in your neighborhood in an attempt to trick you into answering the call. Caller ID makes scammers seem more believable when they claim they're from an organization known to you, like a church or a local business, making it more likely that you'll pick up.
- **Callers prey on lonely, aging adults**
  In the US, 27% of aging adults live alone,[4] and they're the most likely to be targeted for scams.[5] One reason being that lonely people are more likely to answer the phone and are willing to talk to someone. Additionally, one study used MRI tests to compare brain characteristics of people who were scammed against those who resisted. They found that age-related brain changes can make some aging adults more susceptible to scams.[6] Further, aging adults can be attractive to scammers because they're more likely to have substantial savings, own a home, and have good credit.[7]

Second: What are the Three Top Phone Scams

To protect yourself against future phone scams, it's important to understand them. Here are three of the most effective approaches used against aging adults.

- **Government impostor**
  The last organization we want to get a call from is a government agency. A government impersonator might even give you their "employee ID number" to sound official. They might even have information about you, like your name or home address.

  Why this works
  If we think a government official is calling, it's natural to think we might have done something wrong. Did I forget to send or sign a required form? Scammers often say they work for the Social Security Administration, the IRS, or Medicare. They'll give you a compelling reason why you need to send money or give them personal information immediately.
- **Grandparent scam**
  The victim gets a call from someone posing as his or her grandchild. This person explains, in a frantic-sounding voice that he or she is in trouble and needs money (e.g., there's been an accident, arrest, or a robbery). To add to the urgency, the caller might claim to be hospitalized or stuck in a foreign country. They may even throw in a few family particulars, gleaned from the actual grandchild's social media activity to make the impersonation even more convincing.

  Why this works
  The impostor offers just enough detail about where and how the emergency happened to make it seem plausible and perhaps turns the phone over to another scammer who pretends to be a doctor, police officer, or lawyer to back up the story. The scammer impersonating a "grandchild" implores the target to wire money immediately, adding an anxious plea: "Don't tell Mom and Dad!"
- **Robocall phone scam**
  These computer-generated calls are first trying to verify that you are a real person. This may entail just recording your "Yes" answer to "Can you hear me?" for further use, possibly to authorize bogus charges. They may leave a voicemail about an Amazon purchase made on your account, asking to call back to clear up a problem. If you answer the phone and there is a long pause, that could be because the call is being switched to a call center of trained phone scammers—that is a good time to hang up.

Why this works
If you get a voicemail about a problem with your Amazon purchase, we might be relieved someone found the problem. If you call back, a scammer will seem willing and able to help solve the problem. While they may seem friendly and helpful, they'll be trying to gather personal information to swindle their victims' money.

Third, Tips to Help Protect You from Phone Scams

Train yourself to avoid answering calls from unknown numbers. If it's important and relevant to you, such as a call back from someone that you telephoned, the caller will leave a message. If you do pick up the phone, use suggestions from this list:

1. If a caller asks who you are, or if this is [your name], ask them to identify themselves and their company first, and where they're calling from. If you don't recognize them, ask for a phone number you can use to call them back. (In many cases, you won't get one—a red flag.) You can also google the company "calling" you then call them to confirm their legitimacy.
2. Be cautious about caller ID numbers that seem legitimate. You may not be able to tell right away if an incoming call is using Caller ID spoofing. Beware: Caller ID showing a "local" number does not necessarily mean it's a local caller.
3. If you answer the phone and the caller, or a recording, asks you to hit a button to stop getting the calls, hang up. Scammers often use this trick to identify potential targets.
4. Don't respond to any questions asked by a robocall that tries to verify your name. For example, "Is this Robert?" answered with "Yes." They may record your response and use it to authorize purchases.
5. Set a password for your voicemail. If a hacker gets your phone number, they may be able to gain access to your voicemail if it's not password protected.
6. Talk to your phone company about available call-blocking tools and check into apps that block unwanted calls on your phone.

7. Realize that it's highly unlikely that a government organization would ever contact you by phone. If you get a call from someone posing as a government official, hang up. If needed, they'll contact you by mail.

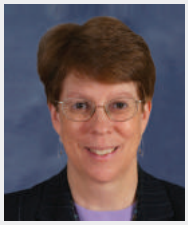
We Felt Vulnerable

After receiving our IRS refund scam letter, my husband and I were both angry and anxious about other vulnerabilities in our financial management that we may have missed. We didn't lose any money, but it was a wake-up call. Had we filed our tax return sooner, we may have become victims of that scam. Since then, we're less trusting of letters like that and calls from unknown callers.

Next step

Don't answer calls from unknown callers. If it's a legitimate caller, they'll leave a message. Explore settings on your mobile phones and try turning on the "Silence Unknown Callers" feature.

[1] Protecting Older Consumers, Federal Trade Commission, 10/18/20
[2] 5 Ways to Stop Senior Citizen Scams, Consumer Reports, 6/15/19
[3] Scam Glossary, Federal Communications Commission, 2/11/21
[4] Older people are more likely to live alone in the U.S. than elsewhere in the world, Pew Research Center, 3/10/20
[5] People who live alone among the likely to be scammed, Cadillac News, 10/17/19
[6] Financial Exploitation Is Associated With Structural and Functional Brain Differences in Healthy
[7] Older Adults, The Journals of Gerontology, 5/2/17. Most recent data available.
Elder Fraud, FBI, 2021



Laurie Orlov is a tech industry veteran, writer, speaker, and founder of Aging in Place Technology Watch. She conducts market research, follows trends, and writes reports about technologies and services that enable boomers and seniors to remain longer in their home of choice.