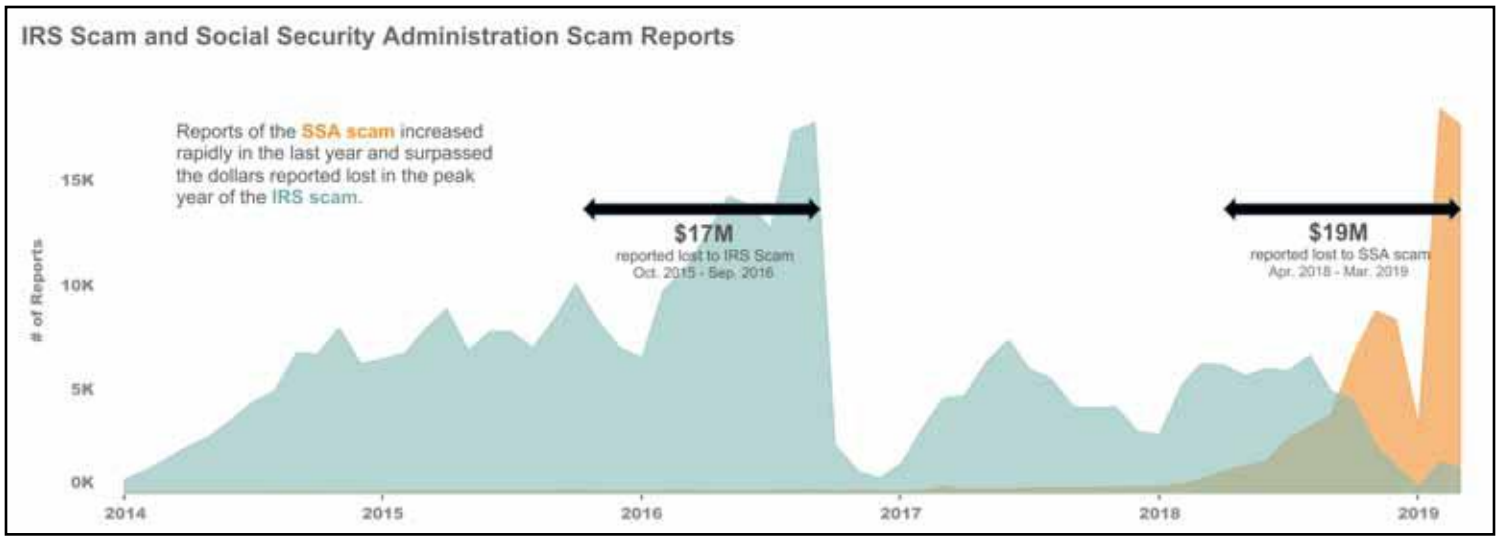
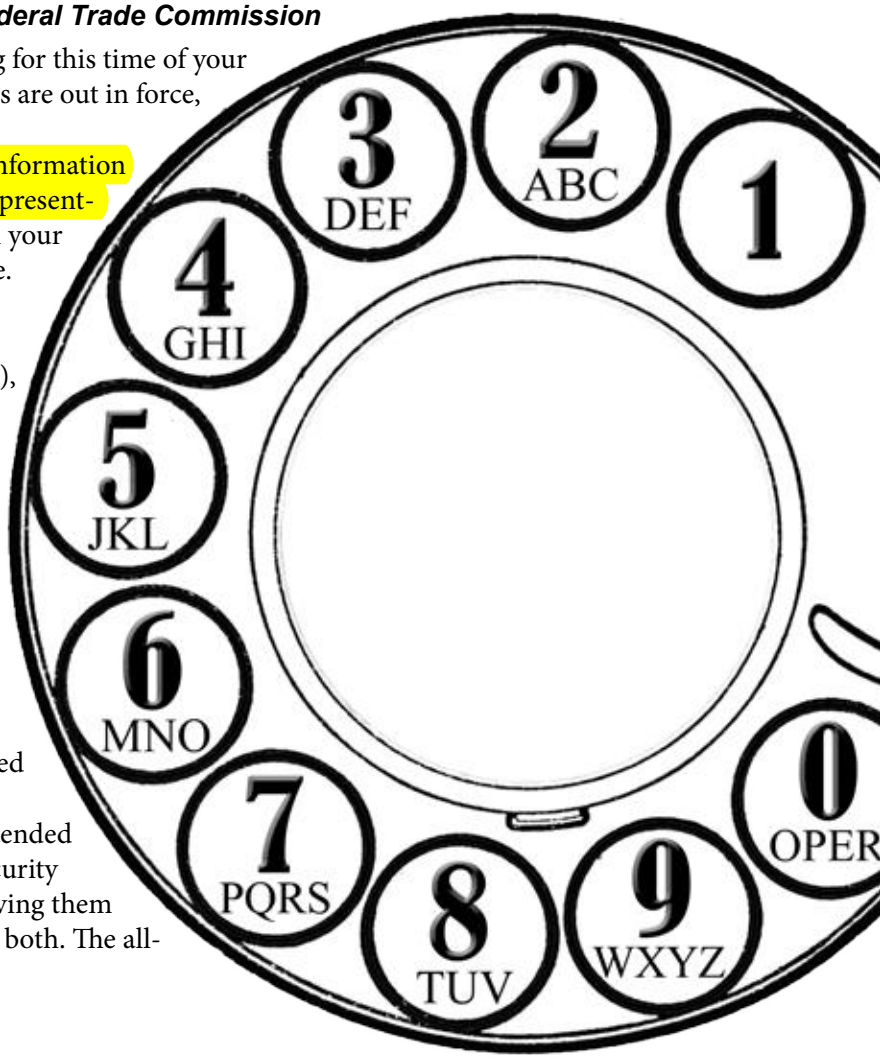


People reported the IRS scam (blue) in huge numbers for many years, but the new SSA scam (orange) is trending in the same direction – with a vengeance. People filed over 76,000 reports about Social Security imposters in the past 12 months, with reported losses of $19 million. Compare that to the $17 million in reported losses to the IRS scam in its peak year. About 36,000 reports and $6.7 million in reported losses are from the past two months alone.

One Scurvy Scam

Retirees, elderly susceptible targets of newest nationwide telephone impersonation ruse

From Social Security Administration & Federal Trade Commission



Retirees, you've spent your entire careers preparing for this time of your lives. But be advised, the unscrupulous phone pirates are out in force, and they want the hard-earned fruits of your labors.

Some schemers try to gain access to the personal information on your computer by claiming to be tech-support representatives from Apple or Microsoft, while others play on your generosity for a (seemingly) worthy, charitable cause.

However, one scam in particular is effective with retirees and the elderly.

According to the Federal Trade Commission (FTC), reports concerning Social Security fraud are rising, replacing reports about IRS imposters on its complaint list. Last year, Social Security Administration (SSA) swindles cost consumers $19 million. The biggest year for the IRS scam was 2016, which cost consumers $17 million.

According to an SSA release, just 3.4 percent of people who report the scam say they lost money. Most people are worried because they believe a scammer has their SSN. But when people do lose money, they lose a lot; the average individual reported loss last year was $1,500.

In this scam, callers use robocalls to reach their intended victims, and by pretending to be from the Social Security Administration (SSA), attempt to trick them into giving them their money, their Social Security number (SSN), or both. The all-

WHEN SCAMMERS COME CALLIN'

► ALWAYS be cautious and avoid providing sensitive information such as your Social Security number or bank account information.
► Your Social Security number IS NOT about to be suspended. You DON'T HAVE TO verify your number to anyone --- and your bank accounts ARE NOT about to be seized.
► The SSA will NEVER threaten you or your benefits.
► The SSA WILL NOT tell you to wire money, send cash, or put money on gift cards. Anyone who tells you to do those things is a scammer -- EVERY TIME.
► DO NOT trust caller ID. Scammers can make it look like the call is originating from anywhere – even a real SSA phone number.
► NEVER give any part of your Social Security, bank account or credit card number to anyone who contacts you.
► Real SSA staff do call people who have ongoing business with the agency, but they'll NEVER threaten you, or ask you to send money.
► Get the caller's information, hang up, and contact the official phone number of the business or agency the caller claims to represent.

HELP ON THE WEB:

♦ If you believe a scammer has your Social Security number, visit www.identitytheft.gov/Assistant?ssa=true to learn what you can do.
♦ To report other government imposter scams, go www.FTC.gov/complaint.
♦ To make a report to the Office of the Inspector General (OIG) Fraud Hotline, call (800) 269-0271, or go online at www.oig.ssa.gov/report.

SCAM from Page 4

too-common tactic will have the caller tell you that your SSN is suspended and you need to give the caller the number to reactivate it.

Another method is to tell you that their SSN has been involved in suspicious activity or a crime, and your bank account is in trouble. However, you can protect yourself by withdrawing money from your bank, putting a specified amount on a gift card — or some other "storage" or "safekeeping" method — and giving the caller the code or PIN number on the back to access the funds. The caller will attempt to pressure you by saying that if you don't act fast; your account will be seized or frozen.

Gift cards are the most common method of separating you from your money, but there are others. People have reported withdrawing money and fed cash into Bitcoin ATMs. No matter the method, the result is the same. The scammer gets fast cash and stays anonymous while the money you thought you were keeping safe has vanished.

It can get confusing. The scammers have developed methods such as "ID spoofing," which bypasses caller ID protections, making it seem as if the call is actually originating from a government agency. Being on the no-call list is no safeguard either, as many people no longer trust that the caller is actually the name appearing on the ID. While SSA employees do occasionally contact people — generally those who have ongoing business with the agency — by telephone, they will never threaten a person or promise a Social Security benefit approval, or increase, in exchange for information. In those cases, the call is fraudulent and people should not engage with the caller.

If you receive such a call, remember — the real SSA will never randomly call or tell you to put money on a gift card, visit a Bitcoin ATM, or wire them money. If the caller ID shows a number that looks like it belongs to the SSA, don't trust the number. If concerned, call the SSA at (800) 772-1213.