No-Talk Phone Scams

Dialing deceivers don’t need you to say anything to rip you off

by Sid Kirchheimer, AARP Bulletin Comments: 106
Most telephone scammers rely on talk, getting you to pick up the phone so they can give their impersonations of IRS agents, noble fundraisers, tech-support saviors or grandkids in need. But with a new breed of telephone fraudsters, sometimes you don’t even need to say "Hello" to get ripped off. Here’s how some of these crooks may target you.

Call Center Fraud

There are scam artists who spend hours calling the customer service centers of banks, insurance companies and other institutions, posing as people like you, to try to access accounts. These crimes have more than doubled in the past year. “That’s because reps only ask a couple of simple authentication questions — maybe your mother’s maiden name or your Social Security number — before you can transfer money or do whatever,” explains Ken Shuman of Pindrop, a company that provides antifraud services to call centers.

Scammers start by assembling information on you, stolen in data breaches, purchased on the “dark web” or gleaned with a simple Google search. Then, working from boiler rooms (often overseas), they spend all day phoning different call centers to determine if you have accounts with those companies. With your data in hand, they can often answer the authentication questions that call centers ask.

ATM PINs are especially prized — and vulnerable, adds Shuman. He notes that there are only 10,000 possible combinations for a four-digit PIN. Unless a bank’s system blocks calls after several tries — and some don’t — there are scammers who call back 150 times a day, trying different PINs until they get it right. Then they immediately log in as you, change your PIN and take over your account.

Smartphone Swindles

An ever-growing segment of the 20 billion text messages sent each day are attempts at defrauding people through “smishing” (a word that combines the SMS technology that sends text messages and phishing, a ploy to coax confidential information out of you). Typically, a scam texter will fake a problem with one of your financial accounts and ask you for data. Or they might pitch low-cost mortgages or credit cards, or promise free gift cards. If you respond by texting back confidential personal information, your identity may be stolen. Millions of these smishing texts can be launched simultaneously.

Your best defense is to be stingy with your phone number. Scam texts may result if you provide it to contests, say, or businesses. Mobile apps can also be to blame. When you install them, the fine print in the user agreement may grant permission to the app’s developer to use or sell your phone number and sometimes even the numbers of your contacts. In one recently popular scheme, scammers get your contacts from mobile apps, then text you posing as people you know to seek money or ID-theft-worthy information, says Jonathan Sasse, marketing executive at First Orion, a digital security firm that provides the mobile app PrivacyStar.
One more important tip: Never follow a text’s instructions to push a designated key to opt out of future messages. Instead, forward the questionable text to short code 7726, so cellphone carriers can block that sender. You can further bolster defenses against mobile scams — which have quadrupled in the past two years — with call-blocking apps such as Hiya, Truecaller, NoMoRobo and PrivacyStar.

**Curiosity Cons**

Knowing that you are likely to ignore unrecognized or private numbers on caller ID, today’s crooks use software that allows them to display fake numbers that are hard to resist. Here are some variations.

- **The neighbor ploy** Your area code and prefix are displayed, so the call appears to be from a neighbor or nearby business. “Fewer people are comfortable blocking local numbers, increasing scammers’ success rates,” notes Jonathan Nelson of Hiya. And the fake number makes it hard for law enforcement to track.
- **The “Hey, there’s a call from my own phone number” scam** It’s hard to resist answering a call from your own number, which scammers can simulate. And they are able to get around any call blocking that you’ve set up.
- **The one-ring rip-off** Criminals sometimes program auto-dialers to make repeated calls to you, each disconnecting after just one ring. They know this might spur you into calling back the displayed number to complain. There’s double trouble if you call area codes such as 268, 664 and 876. These are for Caribbean countries and other places that have high per-minute phone charges. One scam involves getting you to call one of those numbers, then getting you to hold through transfers that rack up your bill until a scammer gets on the line and starts a fraudulent pitch.

**Also of Interest**

- **AVOID SCAMS**: [Fraud Watch Network helps avoid scams and fraud](https://www.fraudwatchnetwork.org)