Don't Fall for These Classic Scams

Even in an era when a sizable proportion of fraud has migrated online, most con artists ply their trade on the phone, via U.S. mail, and even door to door. Here are a few of the most enduring con games. If you encounter them, simply don't engage.

IRS Imposters

News accounts in October 2016 reported that a notorious fraud swindled victims out of up to $150,000 a day by convincing them they owed the IRS money. And while news reports in April of last year said that the alleged ringleader of the network of call centers was arrested in Mumbai, this type of con is still going strong.

In a recent version making the rounds, scammers target deaf and hard-of-hearing individuals who use a video relay service, a type of video telecommunication, instead of a regular telephone. Placing a video phone call, the scammers claim to be from the IRS, providing fake names and IRS identification badge numbers, and ask for personal information.

Another variation on the con targets recent immigrants and other non-native English speakers. Scammers call, addressing their victims in their native language, and may threaten them with arrest, deportation, or suspension of their driver’s license if they don’t supply the information demanded.

Less-polished fraudsters also engage in imposter scams. A telltale sign is the use of “scammer grammar” in email and on the phone, communications that contain spelling errors or subject-verb disagreements.

Home Repairs and Security Checks

Many con artists show up on doorsteps claiming to be contractors offering to inspect a roof or driveway, gratis. They then declare it in need of an overhaul, get victims to fork over an advance cash payment for “supplies,” and skip town.

Another variation on this theme: “Representatives” who have spotted a home-security sign in your yard will knock on your door, hand you a business card, and inform you that, while you might not have received an official letter, your security company was just acquired by their company, which is now upgrading clients’ systems. The scam that follows might involve crooks coming inside your home to dismantle your system and case your house for a future robbery, install shoddy or worthless equipment, and/or get you to sign a draconian contract.
Grandparents Scam

Many scoff at the very idea of ever falling for this long-running phone fraud—until they get a call from a “grandchild” or other loved one in desperate need of money to pay for medical treatment.

“Victims will tell us, ‘I knew everything about this scam, and yet when I picked up the phone and this person said she was my granddaughter and was in trouble, everything I had in my brain went out the window and my emotions took over,’ ” says Amy Nofziger, a fraud expert at AARP. She notes that “we still see about two or three victims of this scam a week” on the organization’s Fraud Network helpline.

Lotteries and Sweepstakes

According to one study, these bogus jackpots nabbed nearly 10 percent of the fraud victims surveyed. Typically, the con begins with a phone call congratulating you on winning a contest you probably don’t remember entering—an objection the scammers skillfully overrule. But before you can receive your winnings (a car, a vacation, a big check), you must first pay taxes, fees, or other expenses via a wire transfer or prepaid debit card. The “winner” sends off the money, but the jackpot never arrives.

Editor's Note: This article also appeared in the June 2018 issue of Consumer Reports magazine.