Beware: 8 Red-Hot Frauds

En español

In their never-ending pursuit of your money and identity, criminals are constantly coming up with new cons. Here's a closer look at eight relatively new types of scams that are becoming more common, along with expert advice on avoiding them. Check out the list of today's hottest emerging frauds.

1. Google Voice Scam

Let's say you've posted a notice online — an item for sale, for example, or a plea to find a lost pet — and included your phone number. In this scam the crook will call you, feign interest, but say they want to verify first that you aren't a scammer. They tell you that you are about to get a verification code from Google Voice (their virtual phone and text service) sent to you, and ask you to read it back. What's really going on: They are setting up a Google Voice account in your name. "They can go on to perpetrate scams and pretend to be you, hiding their footprint from law enforcement," says Eva Velasquez, CEO of the Identity Theft Resource Center.

How to stay safe: "Never share verification codes with anyone," Velasquez says. If you have fallen for this scam, you'll find steps to reclaim your account at the Google Voice Help Center.

2. Rental Assistance Cons

As eviction bans in cities and states expire, renters should be on the lookout for rental assistance scams, says Deborah Royster, assistant director at the Consumer Financial Protection Bureau. Over 583,000 older adults were behind on their rent in mid-2021, opening the door for scammers to impersonate government or nonprofit employees and to request personal info and money up front for applications.

How to stay safe: Apply only to legit rental assistance programs run by government or nonprofit groups, Royster says. Find programs in your area at www.consumerfinance.gov

3. Fake-Job Frauds

Scammers harvest contact info and personal details from résumés posted on legit job websites like Indeed, Monster and CareerBuilder. Then, pretending to be recruiters, they call, email, text or reach out on social media with high-salary or work-at-home job offers. Sometimes the goal is to get additional info about you; other times it's to persuade you to send money for bogus home-office setups or fake fees.

How to stay safe: Use a separate email address just for job hunting, and set up a free Google Voice phone number that rings on your phone but keeps your real number private, says Alex Hamerstone, advisory solutions director for the information security company TrustedSec. If you get a sudden job offer, independently call the company's human resources department to verify it is real, suggests Sandra Guile, spokeswoman for the International Association of Better Business Bureaus.

4. Fake Amazon Employees

One-third of business-impostor fraud complaints involve scammers claiming they're from Amazon, the Federal Trade Commission (FTC) reports. Older adults are four times more likely to lose money and get hit harder — losing a median of $1,500, versus $814 for younger adults — in such scams. "Amazon is the biggest, best-known company in the [online sales] space," Hamerstone says. So the impersonator scams "feel real" to people.

How to stay safe: Ignore calls, text messages, emails and social media messages about suspicious account activity, raffles or unauthorized purchases. If you think you may have a real account problem, contact Amazon customer support at 888-280-4331.

5. Cryptocurrency ATM Payments

Those ATMs cropping up in convenience stores, gas stations and big retailers are scammers' newest payment method. Pretending to be government officials, utility agents or sweepstakes representatives, they direct you to pay a purported fee, bill or handling charge by sending cryptocurrency bought at these ATMs to an untraceable digital wallet. "It's irreversible. There's no way to get your money back,"

says Lisa Cialino, an attorney with the New Jersey State Commission of Investigation.

How to stay safe: According to the FTC, “nobody from the government, law enforcement, a utility company or prize promoter will ever tell you to pay them with cryptocurrency. If someone does, it’s a scam, every time.”

6. Local Tax Impostors

Scammers are impersonating state, county and municipal law enforcement and tax collection agencies to get you to share sensitive personal information or send money to “settle your tax debt.” They may call, email or mail letters threatening to revoke your driver’s license or passport. Some pretend to offer state tax relief.

How to stay safe: Ignore any such calls and emails. Real tax agencies, from the IRS to your town tax collector, do business by mail and won’t ask you for passwords or bank account or credit card info. They also won’t threaten to call the police or ask you to pay with gift cards, peer-to-peer (P2P) payment apps or cryptocurrency.

7. ‘Favor for a Friend’ Gift Cards

You receive an email from a friend asking for a quick favor. She’s having trouble with a credit card or store account and, annoyingly, can’t buy a gift card she needs for a birthday present. Will you buy the card and call her with the numbers on the back? She’ll pay you back. But this favor’s really a fraud, as it’s almost always an impostor sending the request, the Better Business Bureau (BBB) warns. If you do as told, you’ll never see the money again because gift cards don’t have the protections that debit and credit cards have.

How to stay safe: Call or text your friend to confirm the person really needs the favor. Target, Google Play, Apple, eBay and Walmart were the top cards used by scammers in 2021. “Always double check before sending someone money,” the BBB advises.

8. P2P Payment Requests

Scammers are increasingly demanding payment via money-transfer apps like Venmo, Zelle and Cash App. It’s so convenient — you pay in seconds from your phone or computer. But these payments usually cannot be canceled.

How to stay safe: Only use P2P apps to send money to friends and family. And turn on the security-lock feature that requires entering a passcode to make a payment.

More on Scams and Fraud

AARP's Fraud Watch Network can help you spot and avoid scams. Sign up for free Watchdog Alerts, review our scam-tracking map, or call our toll-free fraud helpline at 877-908-3360 if you or a loved one suspect you've been a victim.

---------- Written by Sari Harrar, AARP, April 11, 2022

AARP was founded in 1958 and has over 38 million members. It is a nonprofit, nonpartisan organization for people over the age of 50. AARP is well-known for its advocacy efforts, providing its members with important information, products and services that enhance quality of life as they age. They also promote community service and keep members and the public informed on issues relating to the over 50 age group.

Article Source
AARP
Source URL
https://www.aarp.org
Last Reviewed
Monday, July 15, 2024