5 of the Biggest Scams to Watch for in 2025

By Ken Budd, AARP

“Hi Dr. Richard,” the text to Amy Nofziger began. “I was playing with my puppy today and noticed a lump on his belly.” The stranger requested an exam and included a photo of her puppy’s belly.

Like so many of us, Nofziger, director if AARP’s Fraud Network, gets loads of fake wrong number texts – a tactic scammers use to engage you – but the sophistication and imagination of this one surprised her (they’re often simply, “Do you want to meet for dinner? Or something more straightforward). “If I wasn’t aware that they’re using emotional manipulation, I would have said, ‘Sorry, you have the wrong number. I hope your puppy is okay,’” says Nofziger, a dog lover, as plenty of recipients of this text are likely to be.

Using a cute puppy picture is a new, more sophisticated twist on a common scam tactic – which experts like Nofziger predict will be a major trend in 2025.

“A lot of the scams that were tried and true in 2024 are going to be repurposed, especially with the advent of more effective AI,” says Michael Bruemmer, vice president of data breach resolution and consumer protection at Experian, a global credit verification and financial services firm. Impersonating scams are a good example, whether criminals are posing as celebrities, trusted companies, desperate relatives, or strangers with sick dogs. “Deep fakes, both audio and video, have gotten so good, and the language models have gotten so good, it’s hard to tell (what’s real),” Bruemmer says.

And older people are frequent targets of these crimes: Losses from scams reported by Americans over age 60 were up 11 percent last year over the year before, according to the FBI's Elder Fraud Report, with fraud criminals stealing more than $3.4 billion from older Americans in 2023.

Here are five common scams to watch out for in 2025.

Employment Scams

Every source contacted for this article – from the Better Business Bureau (BBB) to the Identity Theft Resource Center (ITRC) – reported a rise in employment scams, from phony ads on job sites, to fake recruitment pitches in your inbox.

In some cases, the goal is simply to gain your personal information. You're told you got the job, so you fill out paperwork that includes your Social Security number and your bank account information for direct deposit, notes Melanie McGovern, director of public relations and social media for the International Association of Better Business Bureaus, Inc.

More elaborate scams can involve bogus payments. Some scams, for example, ask would-be employees to pay for training or useless certifications. Others pay new staffers a bonus (with a check that will eventually bounce), then ask for money back due to "overpayment," the Federal Trade commission (FTC) reports. Scammers might also request money to cover shipment costs for job-related equipment.

How to stay safe: Remember that just because ads appear on reputable platforms such as LinkedIn and Indeed, it doesn't mean they're genuine.

"Those platforms do their best to police what's there, but they cannot catch everything," says Eva Velasquez, president and CEO of ITRC. "And the bad actors often use the name of a real hiring manager and make it look like they are involved in that company."

If you're contacted by a recruiter, visit the company's website and see if they're hiring for that particular position, if the person actually works there, and if it's a legitimate company. Also watch for jobs that promise you can work at home while making big money. During the application process, companies only need basic information – not your Social Security number or financial information. And if you're promised a job but required to pay money, it's a scam.

Cryptocurrency Scams

Cryptocurrency is hot, with the price of one Bitcoin reaching $100,000 for the first time in December 2024. That may be good for savvy investors, but the hype could lure novices into cryptocurrency scams – with huge potential losses. In 2023, the FBI's Internet Crime Complaint Center (IC3.gov) received nearly 9,000 cryptocurrency complaints from people age 50-59. Their total losses: more than $900 million. People 60 or older registered nearly 17,000 complaints and reported losses of $1.6 billion. (The numbers are probably far higher, because scams are notoriously underreported.)

Scammers use dating apps, messaging apps, social media and other communications to build relationships and trust with their targets, then share their "expertise" on investments, frequently promising large returns and little risk. In 2023, this "confidence-enabled cryptocurrency investment fraud" was the most prominent type of crypto scam, the Federal Bureau of Investigation (FBI) reports.

Criminals often show victims fake profit reports, which encourages them to invest more. But when investors try to withdraw funds, they're frequently charged outrageous fees. The bogus companies then typically vanish before investors receive their money.

How to Stay Safe: If you're interested in crypto but lack expertise, talk with a financial advisor. And watch for impostor sites that mimic actual companies. In California, one victim transferred over $127,000 to two crypto exchanges, one of which was Celestia.bet. The true network, however, is Celestia.org.

To confirm that a company is legit, make sure it's registered with the Commodities Futures Trading Commission (CFTC) and the National Futures Association. Also avoid companies with no physical address or customer service line, the CFTC suggests.

Also beware of requests to pay for something or address an urgent financial matter with crypto; they may ask you to use a crypto ATM. "Crypto is the payment method in a lot of different scams," Velasquez says, because it's hard to trace and payments usually can't be reversed.

Celebrity Imposter Scams

The AARP Fraud Watch Network receives dozens of reports of celebrity imposter scams every month. Some involve phony product endorsements, such as the fake video of Kelly Clarkston or the *Shark Tank* judges promoting weight-loss gummies. But what most concerns Nofziger are scams where people believe they've entered a romance or friendship with a celebrity.

“These are the ones we see the most,” she says. The scammer hits the victim when they are emotionally vulnerable, she explains – when they might be feeling unworthy, lonely, or bored, or grieving the loss of a loved one. The supposed celebrity needs money, whether launching a new charity or putting money down on the house where you both will live.

How to stay safe: No legitimate celebrity will ever ask for money or personal information online. Most celebrities don’t manage their own social media accounts, so if you truly believe that you’re communicating with a star, go to the celebrity’s website and contact their management team to confirm, says Nofziger.

Before buying a product based on a celebrity recommendation, conduct an online search of the person and product, with words like “scam” or “fake,” the FTC suggests. When you see a celebrity promoting a product or making a political statement on a t-shirt, hat, flag – any surface with text – be suspicious. Those surfaces can be a canvas for false messages; it’s become easy to alter photos.

The FTC is trying to fight these bogus endorsements. In August 2024, the agency announced a new rule that prohibits “fake or false consumer reviews, consumer testimonials, and celebrity testimonials” and allows it “to seek civil penalties against knowing violators.”

Tech Support Scams

Consumers age 60 and older are five times more likely than their younger counterparts to lose money to tech support scams, which cost older Americans more than $175 million in 2023, the FTC reported to Congress in October 2024.

The fraud frequently starts with a pop-up message – often with a logo from companies like Microsoft or Apple – saying your computer has a virus. You click a link or call a supposed support number, and they request remote access to your computer. The criminals can now access all of the information on your machine and also install malware.

The scammers may also try to sell you useless software, maintenance or warranty programs. In March 2024, the FTC reached a $26 million settlement with two tech-support companies who used fake Microsoft pop-ups to lure consumers into buying software. Or they may install malware to harvest login credentials to your online accounts, including financial accounts.

How to Stay Safe: Legitimate tech companies won't call, email, or text you about problems with your computer, and their pop-ups will never ask you to make a call or click a link.

If a tech support person calls you unexpectedly, it's almost surely a scam, the FTC states. Hang up, even if the number looks real. Never click on a pop-up, never give remote access to someone who calls you out of the blue, and never share your password. If the pop-up won't go away, restart your computer, suggests scam expert Steve Weisman, founder of Spamicide.com. If you do share your password, change it immediately, he adds. And if you give someone remote access to your computer, update your security software and run a scan, or have a trusted person or big box store scan it for you.

Card-Declined Scams

The BBB's Scam Tracker has received many recent reports from consumers whose credit cards are declined while making an online purchase. Typically, they try using a different card, but that one fails, too. And yet despite the card-declined notices, the charges have actually occurred for each transaction – and often for more than they thought. After her card was denied, one victim tried it a second time, and received the same card-declined message. Then her credit card company alerted her that it had declined a $2,500 charge – even though she hadn't made a $2,500 charge while struggling with her transaction, she reported to the BBB.

"This is the scam I'm most concerned about," says McGovern. "We've seen a noticeable increase in card-declined problems."

The fraud typically occurs when people visit fraudulent sites or click on fraudulent links. In September 2024, the American Automobile Association (AAA) warned its members about emails and texts (which appear to come from AAA customer service) offering a free AAA car emergency kit if people took a survey. The catch: You had to pay for shipping. So people entered their credit card information and then received the card-decline message. One victim told AAA he found several fraudulent charges on his two credit cards.

How to Stay Safe: Always use a credit card rather than a debit card, because credit cards offer stronger fraud protections. If you're unfamiliar with a company, research it before making a purchase. And make sure a website is genuine. Scammers often build lookalike sites, the BBB notes, so scrutinize the URL (sometimes a letter or two might be different).

Perhaps most importantly, if you receive an unsolicited offer, ignore it. “Don’t click on any links or answer any calls,” Bruemmer says. “Those same rules apply to shopping scams, charity scams, job scams – if you didn’t ask for it, don’t touch it.”

Report Scams

If you spot or have been victim of a scam, file a police report. Also report scams to the FBI’s Internet Crime Complaint Center. The more information authorities have, the better they can identify patterns, link cases and ultimately catch the criminals. You can also report scams to the AARP Fraud Watch Network Helpline, 877-908-3360. It’s a free resource, with trained fraud specialists who can provide support and guidance on what to do next and how to avoid scams in the future.