Enjoy Your Retirement.

Your retirement savings have been an important part of your retirement plan. But what will you do with those savings when you no longer need them?

Many people decide to donate retirement accounts to charity, while leaving other less tax-burdened assets to loved ones.

You retain control over the funds you need during your lifetime—and leave a gift to help low-income seniors tomorrow. It's as easy as signing your name to a beneficiary designation form.

Call 1-888-709-5558 to receive your free copy of: *Gifts by Beneficiary Designation*

AARP Foundation®
For a future without senior poverty.

AI GIVES SCAMMERS A SCARY NEW TOOL

BY **CHRIS MORRIS**

Artificial intelligence has opened a new door for scammers, making it easy to replicate almost anyone's voice from a brief audio sample. That has made frauds such as the grandparent scam—built around a fake phone call supposedly from a grandchild—frighteningly effective, experts say.

All crooks need is a short sample of a person's voice, which can often be found on social media posts. From there, they run it through sophisticated but readily available (and cheap) software to create a digital duplicate, which they can program to say whatever words they want to use.

"The state-of-the-art AI can generate realistic images and voices, and is used as a tool of impersonation in scams targeting older Americans," says Siwei Lyu, a professor of computer science at the University at Buffalo, State University of New York, and an expert in digital media forensics. "The scammers rely on the familiarity of the voices."

Last year, consumers lost $2.6 billion to this sort of fraud, up from $2.4 billion in 2021.

The boom in AI scams is likely just beginning, says AARP anti-fraud expert Mark Fetterhoff. "It may be possible scammers are using AI to clone voices as part of romance scams, celebrity impostor scams and tech support scams," he says.

Lyu runs a project called DART (Deception Awareness and Resilience Training), which helps older Americans recognize scams via a mobile game. He warns that if the scammers fool you, there's often no way to get the money back. If you receive a call seemingly from someone close to you asking for money, there are steps the Federal Trade Commission suggests you take to protect yourself:

- **Slow things down.** These calls typically move fast. If someone you know seems to be calling you for money unexpectedly, tell them you'll call back. Then find the number from a trusted source.
- **Resist pressure.** If the caller stresses the urgency of their need, that's almost always a fraud signal. No legit organization demands money within hours. Don't be goaded or guilted into sending money until you've verified what's going on.
- **Listen for red flags.** If the caller says it's important to keep things secret, that's a strong indicator you're being scammed.

The bad news: More sophisticated scams are ahead. "The next round of robot calls will be made from scripts created from [AI chatbots], converted to a person's voice," Lyu warns. Technology "could also be used to create video calls with the grandkid's face." ■

__Chris Morris__ writes about technology for Fortune, Fast Company *and other news organizations.*

Have questions related to scams? *Call the AARP Fraud Watch Network Helpline toll-free at* ***877-908-3360.*** *For the latest fraud news and advice, go to* **aarp.org/fraudwatchnetwork.**

ASK THE FRAUD TEAM

My older sister lives alone and had some workers knock on her door claiming her roof needed fixing. She paid cash up front for the first half of the job. The crew never showed up again. Was she targeted for this scam?
This is a common fraud that recurs every year with warm weather. She may need to have a reputable contractor look at the roof to ensure no damage was done. Have her report this situation to local law enforcement. She is likely not the only victim in the area.

My daughter found Taylor Swift tickets for a great price on social media. They asked her to pay by Venmo, and then they would transfer the tickets. Should she?
Many criminals will post "too good to be true" offers for concert tickets online and ask to be paid by a peer-to-peer payment app such as Venmo, Cash App or Zelle. Those payments are virtually untraceable, and actually getting what you paid for is a long shot. For greater peace of mind when looking for event tickets, use an authorized ticket reseller that takes credit cards.

NIC RAPP