MONEYWATCH

Cybercriminals are using AI voice cloning tools to dupe victims

BY MEGAN CERULLO
MARCH 21, 2023 / 7:02 PM / MONEYWATCH

If you answer a phone call from an unknown number, let the caller speak first. Whoever is on the other end of the line could be recording snippets of your voice – and later using it to impersonate you in a very convincing manner.

That's according to the Federal Trade Commission, which is warning consumers to beware of scam artists who are secretly recording people's voices in order to later pose as them and ask victims' relatives for money.

The FTC described such a scenario amid the rise of AI-powered tools like ChatGPT and Microsoft's Vall-E, a tool the software company demonstrated in January that converts text to speech. Vall-E is not yet available to the public, but other companies, like Resemble AI and ElevenLabs, make similar tools that are. Using a short sample of anyone's voice, this technology can accurately convert written sentences into convincing sounding audio.

"You get a call. There's a panicked voice on the line. It's your grandson. He says he's in deep trouble – he wrecked the car and landed in jail. But you can help by sending money. You take a deep breath and think. You've heard about grandparent scams. But darn, it sounds just like him," FTC consumer education specialist Alvaro Puig wrote on the agency's site.

All you need is 3 seconds

Criminals employing widely available "voice cloning" tools to dupe victims into thinking loved ones are in trouble and need cash fast, experts say. All it

requires is a short clip of someone's voice, which is sometimes available on the internet – or if it isn't, can be collected by recording a spam call – plus a voice-cloning app such as ElevenLabs' AI speech software, VoiceLab.

"If you made a TikTok video with your voice on it, that's enough," Hany Farid, a digital forensics professor at the University of California at Berkeley, told CBS MoneyWatch. Even a voice mailbox recording would suffice, for example.

He's not surprised such scams are proliferating. "This is part of a continuum. We started with the spam calls, then email phishing scams, then text message phishing scams. So this is the natural evolution of these scams," Farid said.

"Don't trust the voice"

What this means in practice, according to the FTC, is that you can no longer trust voices that sound identical to those of your friends and family members.

"Don't trust the voice," the FTC warns. "Call the person who supposedly contacted you and verify the story. Use a phone number you know is theirs. If you can't reach your loved one, try to get in touch with them through another family member or their friends."

Vall-E maker Microsoft alluded to this problem, including a disclaimer in a paper demonstrating the technology that "it may carry potential risks in misuse of the model, such as spoofing voice identification or impersonating a specific speaker." The paper noted that if the tool is rolled out to the general public, it "should include a protocol to ensure that the speaker approves the use of their voice."

In January, ElevenLabs tweeted, "We also see an increasing number of voice cloning misuse cases."

For this reason, the company said that identity verification is essential to weed out malicious content and that the tech will only be available for a fee.

How to protect yourself

With bad actors using voice cloning software to mimic voices and commit crimes, it's important to be vigilant. First, if you answer a call from an unknown number, let the caller speak first. If you say as much as "Hello? Who is this?" they could use that audio sample to impersonate you.

Farid said he no longer answers his phone unless he's expecting a call. And when he receives calls from supposed family members, like his wife, that seem "off," he asks her for a code word that they've agreed upon.

"Now we even mispronounce it, too, if we suspect someone else knows it," he told CBS MoneyWatch. "It's like a password you don't share with anybody. It's a pretty easy way to circumvent this, as long as you have wherewithal to ask and not panic."

It's a low-tech way to combat a high-tech issue. The FTC also warns consumers not to trust incoming calls from unknown parties and advises people to verify calls claiming to be from friends or family members in another way – such as by calling the person on a known number or reaching out to mutual friends.

Additionally, when someone asks for payment via money wire, gift card or in cryptocurrency, those can also be red flags.

Scammers ask you to pay or send money in ways that make it hard to get your

money back," the FTC said.

Cybersecurity

Could you get "carhacked"? The growing risk of keyless vehicle thefts

Cyberattack impacts U.S. federal agencies, NATO allies

Tech fears you shouldn't worry about

Card-skimming scams target new victims

More ›

First published on March 21, 2023 / 3:02 PM

In: **Federal Trade Commission** **Artificial Intelligence**