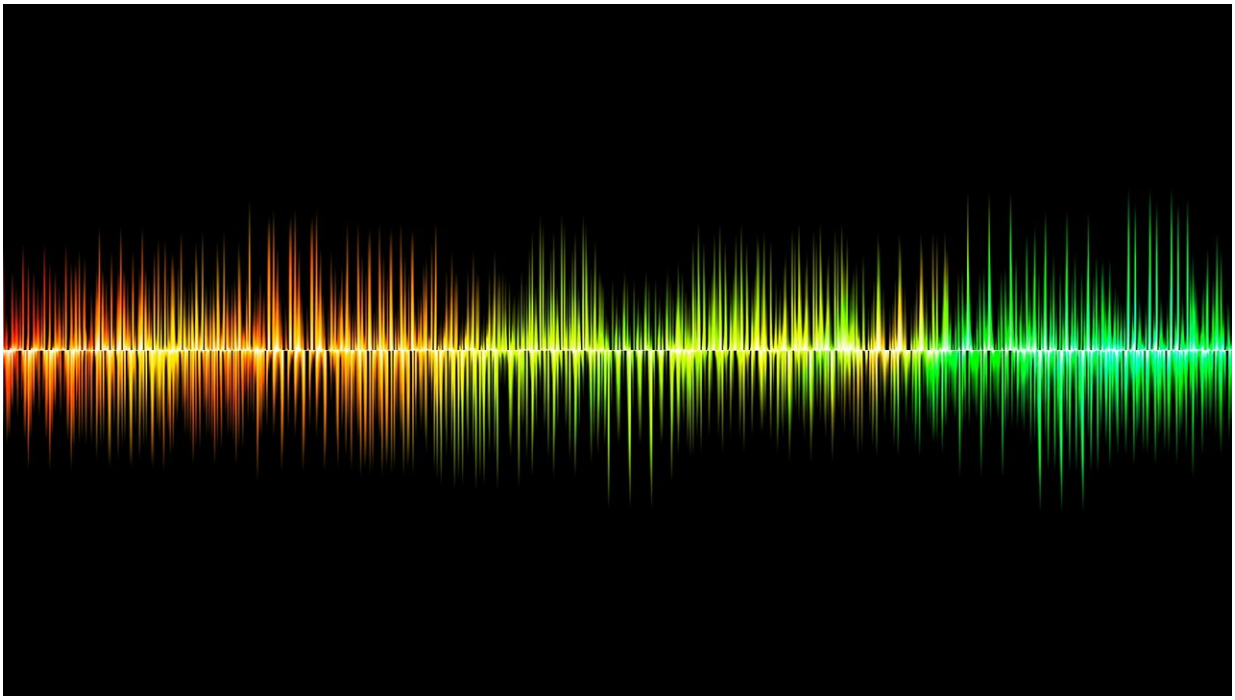
Voice deepfakes are calling—here's what they are and how to avoid getting scammed

March 20 2023, by Matthew Wright and Christopher Schwartz



Credit: Pixabay/CC0 Public Domain

You have just returned home after a long day at work and are about to sit down for dinner when suddenly your phone starts buzzing. On the other end is a loved one, perhaps a parent, a child or a childhood friend, begging you to send them money immediately.

You ask them questions, attempting to understand. There is something

off about their answers, which are either vague or out of character, and sometimes there is a peculiar delay, almost as though they were thinking a little too slowly. Yet, you are certain that it is definitely your loved one speaking: That is their voice you hear, and the caller ID is showing their number. Chalking up the strangeness to their panic, you dutifully send the money to the bank account they provide you.

The next day, you call them back to make sure everything is all right. Your loved one has no idea what you are talking about. That is because they never called you—you have been tricked by technology: a voice deepfake. Thousands of people were scammed this way in 2022.

As computer security researchers, we see that ongoing advancements in deep-learning algorithms, audio editing and engineering, and synthetic voice generation have meant that it is increasingly possible to convincingly simulate a person's voice.

Even worse, chatbots like ChatGPT are starting to generate realistic scripts with adaptive real-time responses. By combining these technologies with voice generation, a deepfake goes from being a static recording to a live, lifelike avatar that can convincingly have a phone conversation.

Cloning a voice

Crafting a compelling high-quality deepfake, whether video or audio, is not the easiest thing to do. It requires a wealth of artistic and technical skills, powerful hardware and a fairly hefty sample of the target voice.

There are a growing number of services offering to produce moderate-to high-quality voice clones for a fee, and some voice deepfake tools need a sample of only a minute long, or even just a few seconds, to produce a voice clone that could be convincing enough to fool someone.

However, to convince a loved one—for example, to use in an impersonation scam—it would likely take a significantly larger sample.

Protecting against scams and disinformation

With all that said, we at the DeFake Project of the Rochester Institute of Technology, the University of Mississippi and Michigan State University, and other researchers are working hard to be able to detect video and audio deepfakes and limit the harm they cause. There are also straightforward and everyday actions that you can take to protect yourself.

For starters, voice phishing, or "vishing," scams like the one described above are the most likely voice deepfakes you might encounter in everyday life, both at work and at home. In 2019, an energy firm was scammed out of US$243,000 when criminals simulated the voice of its parent company's boss to order an employee to transfer funds to a supplier. In 2022, people were swindled out of an estimated $11 million by simulated voices, including of close, personal connections.

What can you do?

Be mindful of unexpected calls, even from people you know well. This is not to say you need to schedule every call, but it helps to at least email or text message ahead. Also, do not rely on caller ID, since that can be faked, too. For example, if you receive a call from someone claiming to represent your bank, hang up and call the bank directly to confirm the call's legitimacy. Be sure to use the number you have written down, saved in your contacts list or that you can find on Google.

Additionally, be careful with your personal identifying information, like your Social Security number, home address, birth date, phone number, middle name and even the names of your children and pets. Scammers

can use this information to impersonate you to banks, realtors and others, enriching themselves while bankrupting you or destroying your credit.

Here is another piece of advice: know yourself. Specifically, know your intellectual and emotional biases and vulnerabilities. This is good life advice in general, but it is key to protect yourself from being manipulated. Scammers typically seek to suss out and then prey on your financial anxieties, your political attachments or other inclinations, whatever those may be.

This alertness is also a decent defense against disinformation using voice deepfakes. Deepfakes can be used to take advantage of your confirmation bias, or what you are inclined to believe about someone.

If you hear an important person, whether from your community or the government, saying something that either seems very uncharacteristic for them or confirms your worst suspicions of them, you would be wise to be wary.

Provided by The Conversation

Citation: Voice deepfakes are calling—here's what they are and how to avoid getting scammed (2023, March 20) retrieved 17 April 2024 from https://techxplore.com/news/2023-03-voice-deepfakes-callinghere-scammed.html