AI scam calls imitating familiar voices are a growing problem—here's how they work

July 13 2023, by Oliver Buckley

Credit: AI-generated image (disclaimer)

Scam calls using AI to mimic voices of people you might know are being used to exploit unsuspecting members of the public. These calls use what's known as generative AI, which refers to systems capable of creating text, images or any other media such as video, based on prompts from a user.

Deepfakes have gained notoriety over the last few years with a number of high-profile incidents, such as actress Emma Watson's likeness being used in a series of suggestive adverts that appeared on Facebook and Instagram.

There was also the widely shared—and debunked—video from 2022 in which Ukrainian president Volodymyr Zelensky appeared to tell Ukranians to "lay down arms".

Now, the technology to create an audio deepfake, a realistic copy of a person's voice, is becoming increasingly common. To create a realistic copy of someone's voice you need data to train the algorithm. This means having lots of audio recordings of your intended target's voice. The more examples of the person's voice that you can feed into the algorithms, the better and more convincing the eventual copy will be.

Many of us already share details of our daily lives on the internet. This means the audio data required to create a realistic copy of a voice could be readily available on social media. But what happens once a copy is out there? What is the worst that can happen? A deepfake algorithm could enable anyone in possession of the data to make "you" say whatever they want. In practice, this can be as simple as writing out some text and getting the computer to say it out loud in what sounds like your voice.

Major challenges

This capability risks increasing the prevalence of audio misinformation and disinformation. It can be used to try to influence international or national public opinion, as seen with the "videos" of Zelensky.

But the ubiquity and availability of these technologies poses significant challenges at a local level too—particularly in the growing trend of "AI scam calls". Many people will have received a scam or phishing call that

tells us, for example, that our computer has been compromised and we must immediately log in, potentially giving the caller access to our data.

It is often very easy to spot that this is a hoax, especially when the caller is making requests that someone from a legitimate organization would not. However, now imagine that the voice on the other end of the phone is not just a stranger, but sounds exactly like a friend or loved one. This injects a whole new level of complexity, and panic, for the unlucky recipient.

A recent story reported by CNN highlights an incident where a mother received a call from an unknown number. When she answered the phone, it was her daughter. The daughter had allegedly been kidnapped and was phoning her mother to pass on a ransom demand.

In fact, the girl was safe and sound. The scammers had made a deepfake of her voice. This is not an isolated incident, with variations of the scam including a supposed car accident, where the victim calls their family for money to help them out after a crash.

Old trick using new tech

This is not a new scam in itself, the term "virtual kidnapping scam" has been around for several years. It can take many forms but a common approach is to trick victims into paying a ransom to free a loved one they believe is being threatened.

The scammer tries to establish unquestioning compliance, in order to get the victim to pay a quick ransom before the deception is discovered. However, the dawn of powerful and available AI technologies has upped the ante significantly—and made things more personal. It is one thing to hang up on an anonymous caller, but it takes real confidence in your judgment to hang up on a call from someone sounding just like your

child or partner.

There is software that can used to identify deepfakes, and will create a visual representation of the audio called a spectrogram. When you are listening to the call it might seem impossible to tell it apart from the real person, but voices can be distinguished when spectrograms are analyzed side-by-side. At least one group has offered detection software for download, though such solutions may still require some technical knowledge to use.

Most people will not be able to generate spectrograms so what can you do when you are not certain what you are hearing is the real thing? As with any other form of media you might come across: be skeptical.

If you receive a call from a loved one out of the blue and they ask you for money or make requests that seem out of character, call them back or send them a text to confirm you really are talking to them.

As the capabilities of AI expand, the lines between reality and fiction will increasingly blur. And it is not likely that we will be able to put the technology back in the box. This means that people will need to become more cautious.

Provided by The Conversation

Citation: AI scam calls imitating familiar voices are a growing problem—here's how they work