blog.knowbe4.com

CEO Fraud Attacks Now Use Deepfake Audio and AI to Mimic Executives Over the Phone

Stu Sjouwerman

3 minutos

While deepfake video gets most of the attention on social media, it’s deepfake audio that is quickly becoming the cybercriminal’s tools of choice for committing fraud.

Everything you’ve ever learned about phishing attacks and social engineering tells you that the bad guys work to find ways to establish the illusion of legitimacy – making their emails, webpages, and phone calls seem like they’re coming from real people.

We’ve seen a rise in CEO fraud, where the focus is usually a scam intent on convincing employees to fraudulently transfer money to a scammer’s bank account.

Then there's the CEO Gift Card scam, where a low-level employee is asked to purchase gift cards and send pictures of the card details to the scammer.

In both of these cases, a quick phone call to the person purporting to be asking for the money-related task, and you can verify that it's a scam.

But, what if you got a phone call from that person?

New reports of deepfake *audio* are springing up in larger numbers. Cybercriminals are using earnings calls, YouTube videos, TED talks, etc. of CEOs, training AI to speak just like them.

Adobe unveiled their VoCo product back in 2016 (which seems to have never made it to market), and a new startup Lyrebird AI says they can mimic your voice *with as little as 30 sentences*.

In both these cases, the result is a recording that sounds like you. But scammers are using AI to hold conversations with employees. It's only a matter of time until enough development is done to allow someone to simply talk in their own voice but be heard as the person they're attempting to mimic.

So, what's your defense against an attack like this?

There are two parts to a defense strategy:

- **Ensure users are security-minded** – any user with access to financials or banking details needs to undergo continual Security Awareness Training so they understand the need for and develop a security mindset while working. This same training also keeps users up-to-date on the latest types of attacks – including deepfake audio. So, when a request comes in from anyone in the company that even remotely seems odd, the red flags go up.

- **Have a process in place** – organizations should have a formal process in place on how requests for money transfers and the like are made. You should even have a process for how one-off immediate needs are to be met – make it something that isn’t just a phone call to someone with their finger on the “send money” button.