

It's not just phishing emails, now we have to worry about fake calls, too

March 3 2020, by Jefferson Graham, Usa Today



Credit: CC0 Public Domain

When your boss calls and tells you to wire \$100,000 to a supplier, be on your toes. It could be a fake call.

As if "phishing" phony emails weren't enough, on the rise now are "deep fake" audios that can be cloned with near perfection to sound almost

perfect, and are easy to create for hackers.

"It's on the rise, and something to watch out for," says Vijay Balasubramaniyan, the CEO of Pindrop, a company that offers biometric authentication for enterprise.

Balasubramaniyan demonstrated during a security conference how easy it is to take audio from the internet and use machine learning to create recorded phrases into sentences that the human probably never said.

"All you need is five minutes of audio, and you can create fake audio," said Balasubramaniyan.

For instance, he showed a database of voices, typed "This morning American forces gave North Korea the bloody nose they deserve," and connected it to President Donald Trump's name in the list. A few seconds later, he clicked play, and it sounded eerily real.

He also presented an example of Facebook CEO Mark Zuckerberg supposedly responding to the \$5 billion 2019 fine of the social network for violating privacy by him supposedly saying, "The FTC thinks a \$5-billion fine is going to stop us from violating people's privacy? Suckers."

Recently, House Speaker Nancy Pelosi's voice was altered in a social media clip, but that wasn't an example of fake audio, Balasubramaniyan said, just slowing down audio to make it appear that her voice was slurred.

More costly are examples of fake phone calls, where fraudsters were able to fake the phone number of real contacts and make calls that resulted in employees sending off lots of money.

He cited the example of a United Kingdom energy firm in 2019 that got hacked by deep fake audio, in a call that demanded transfer of what came to \$243,000 to a supplier. Per the Wall Street Journal, the exec was directed to pay it within the hour.

So what to do?

Balasubramanian says if you were to get that kind of call purportedly from a "boss," be skeptical and ask to call back right away to confirm authenticity.

Place the call, and if the real boss answers, "you know it's real."

Beyond being on your toes, companies need to employ multiple security measures for also keeping up with deep fake artificial intelligence generated phone calls, he adds, software to detect authentic versus fake calls.

"This is a threat that's waiting to happen," he says. "It's a very small number now, but it's very real."

(c)2020 U.S. Today

Visit U.S. Today at www.usatoday.com

Citation: It's not just phishing emails, now we have to worry about fake calls, too (2020, March 3) retrieved 25 April 2024 from <https://techxplore.com/news/2020-03-phishing-emails-fake.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.