Can you trust your ears? AI voice scams rattle US

June 12 2023, by Anuj Chopra and Alex Pigman

US officials warn that fraudsters are using convincing AI voice cloning tools to dupe people.

The voice on the phone seemed frighteningly real—an American mother heard her daughter sobbing before a man took over and demanded a ransom. But the girl was an AI clone and the abduction was fake.

The biggest peril of Artificial Intelligence, experts say, is its ability to demolish the boundaries between reality and fiction, handing cybercriminals a cheap and effective technology to propagate disinformation.

In a new breed of scams that has rattled US authorities, fraudsters are using strikingly convincing AI voice cloning tools—widely available online—to steal from people by impersonating family members.

"Help me, mom, please help me," Jennifer DeStefano, an Arizona-based mother, heard a voice saying on the other end of the line.

DeStefano was "100 percent" convinced it was her 15-year-old daughter in deep distress while away on a skiing trip.

"It was never a question of who is this? It was completely her voice... it was the way she would have cried," DeStefano told a local television station in April.

"I never doubted for one second it was her."

The scammer who took over the call, which came from a number unfamiliar to DeStefano, demanded up to $1 million.

The AI-powered ruse was over within minutes when DeStefano established contact with her daughter. But the terrifying case, now under police investigation, underscored the potential for cybercriminals to misuse AI clones.

Grandparent scam

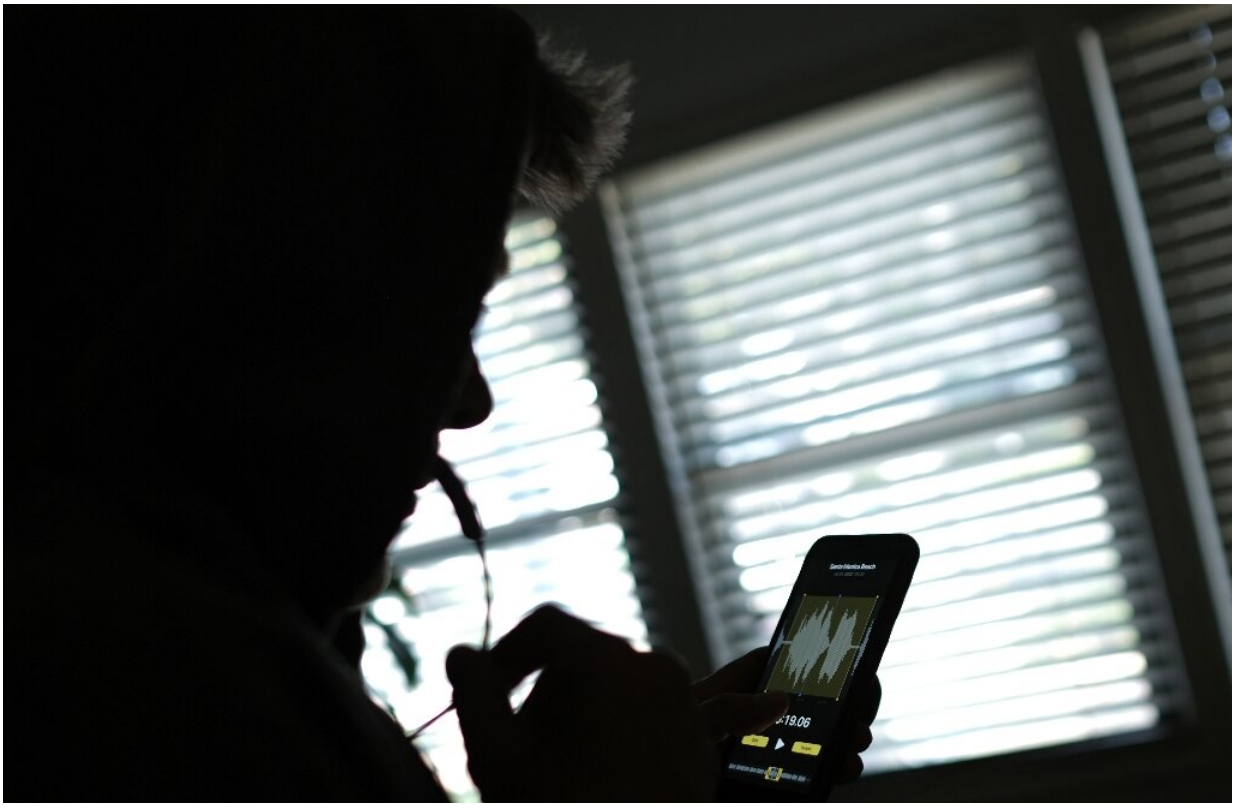
"AI voice cloning, now almost indistinguishable from human speech, allows threat actors like scammers to extract information and funds from

victims more effectively," Wasim Khaled, chief executive of Blackbird.AI, told AFP.

A simple internet search yields a wide array of apps, many available for free, to create AI voices with a small sample—sometimes only a few seconds—of a person's real voice that can be easily stolen from content posted online.

"With a small audio sample, an AI voice clone can be used to leave voicemails and voice texts. It can even be used as a live voice changer on phone calls," Khaled said.

"Scammers can employ different accents, genders, or even mimic the speech patterns of loved ones. [The technology] allows for the creation of convincing deep fakes."



The biggest danger of Artificial Intelligence is its ability to blur the boundaries between reality and fiction, tech experts say.

In a global survey of 7,000 people from nine countries, including the United States, one in four people said they had experienced an AI voice cloning scam or knew someone who had.

Seventy percent of the respondents said they were not confident they could "tell the difference between a cloned voice and the real thing," said the survey, published last month by the US-based McAfee Labs.

American officials have warned of a rise in what is popularly known as the "grandparent scam" -– where an imposter poses as a grandchild in urgent need of money in a distressful situation.

"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," the US Federal Trade Commission said in a warning in March.

"It sounds just like him. How could it be a scam? Voice cloning, that's how."

In the comments beneath the FTC's warning were multiple testimonies of elderly people who had been duped that way.

'Malicious'

That also mirrors the experience of Eddie, a 19-year-old in Chicago whose grandfather received a call from someone who sounded just like

him, claiming he needed money after a car accident.

The ruse, reported by McAfee Labs, was so convincing that his grandfather urgently started scrounging together money and even considered re-mortgaging his house, before the lie was discovered.

"Because it is now easy to generate highly realistic voice clones... nearly anyone with any online presence is vulnerable to an attack," Hany Farid, a professor at the UC Berkeley School of Information, told AFP.

"These scams are gaining traction and spreading."

Earlier this year, AI startup ElevenLabs admitted that its voice cloning tool could be misused for "malicious purposes" after users posted a deepfake audio purporting to be actor Emma Watson reading Adolf Hitler's biography "Mein Kampf."

"We're fast approaching the point where you can't trust the things that you see on the internet," Gal Tal-Hochberg, group chief technology officer at the venture capital firm Team8, told AFP.

"We are going to need new technology to know if the person you think you're talking to is actually the person you're talking to," he said.

Citation: Can you trust your ears? AI voice scams rattle US (2023, June 12) retrieved 8 May 2024 from https://techxplore.com/news/2023-06-ears-ai-voice-scams-rattle.html