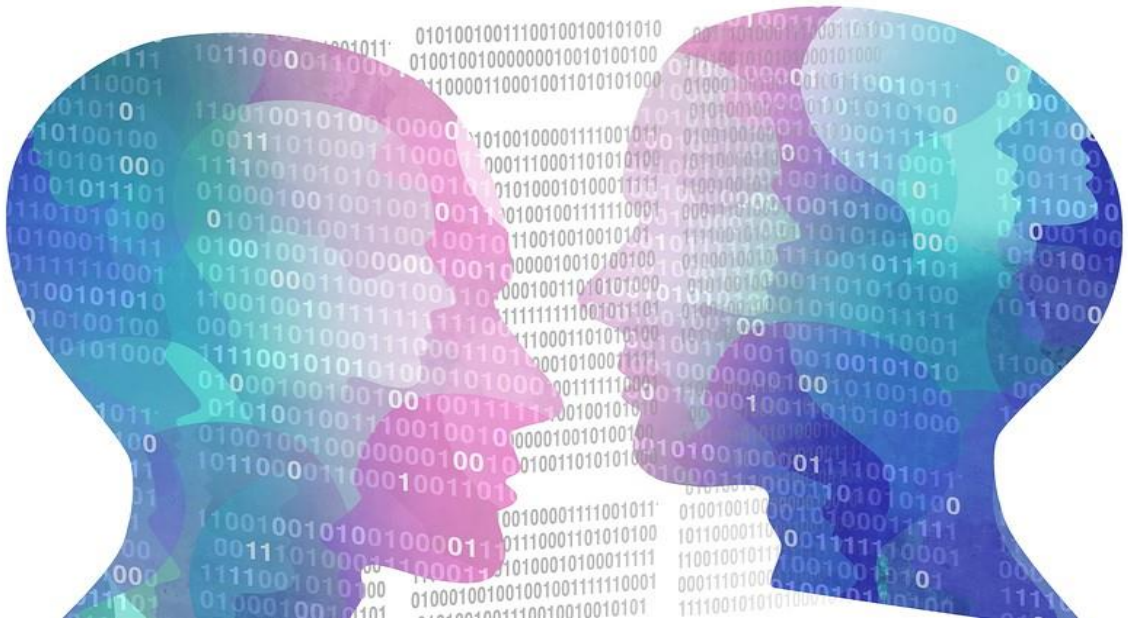
Voice Cloning Elevates Security Threats to the Next Level



Last year, scammers convinced a director at a British company to send them $240,000. Using voice cloning, they impersonated a senior executive at the company, instructing the director to wire the sum to a secret account. Recognizing his boss's voice, he complied, only becoming suspicious when the thieves called a second time.

While this may represent one of the first artificial intelligence (AI) heists on record, it will hardly be the last. Consider the possibilities. If bad actors use voice cloning technology to steal money from businesses, they can easily sabotage political elections or impersonate family members.

Dangers of Increasingly Sophisticated Voice Cloning

Voice cloning presents an example of just one type of "deepfake." The term comes from "deep learning," a type of machine learning that roughly mimics the human brain. While the technology has existed in some form for at least a couple of decades, advancements have made it easily accessible and difficult to detect.

For instance, using just a few seconds of audio, cloning software can create a believable voice impersonation. With more extensive audio samples, often publicly available through social media and news, users can create a fake almost impossible to detect. The counterfeit voice convincingly mimics speech patterns, accent and voice inflections.

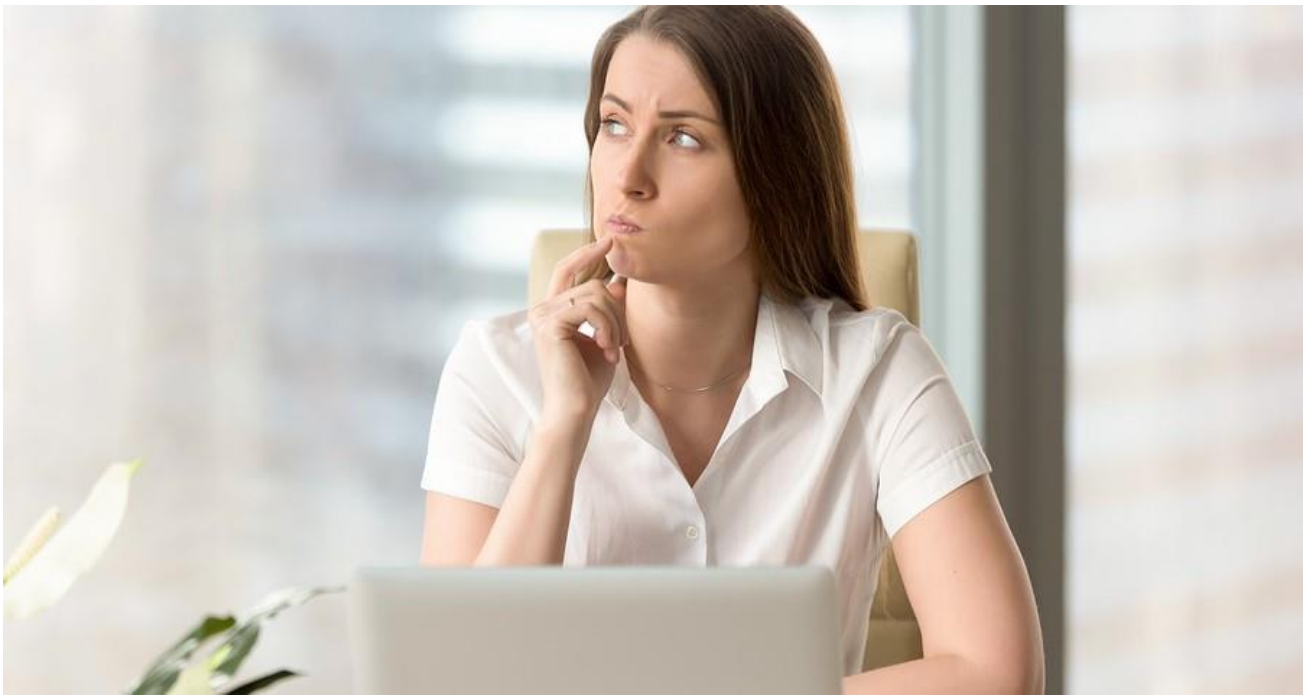
The technology does have positive applications. For instance, patients diagnosed with Lou Gehrig's disease can clone their voice in the early stages. Then, using text to speech technology, they can "speak" with their own voice in later stages. However, the inherent dangers and ethical implications of voice cloning require a greater public awareness.

Tips to Avoid Being Scammed

Security experts have long warned of the dangers of spear-fishing and business email compromise. With the emergence of deepfakes, employees must now take care when dealing with audio and video messages, as well.

Unfortunately, a high quality fake voice or video can prove impossible for humans to detect. Consequently, individuals and businesses should take basic steps to protect against scams.

- Develop appropriate policies – For transactions involving money or sensitive information, business policies should require multiple forms of verification. A voicemail or email should never prove sufficient on its own.
- Increase awareness – Make employees aware of AI capabilities, that bad actors can not only spoof emails and phone numbers but also voices and video.
- Ask questions – If you receive a phone call with a sensitive request, even from someone you normally trust, experts suggest asking questions. Even with sophisticated cloning, the answers may come after a longer than usual pause. Also, the old method of asking the caller something only they would know may still prove useful.
- Watch what you put on social media – The more audio samples publicly available, the easier it will prove for criminals to clone a person's voice.
- Keep up with emerging cyber security technology – Industry leaders have taken notice of the growing deepfake threat and have begun developing technology to detect fakes. AI and even blockchain may provide methods to confirm authenticity of video and audio files.



Protect Against Emerging Threats

As technology grows more sophisticated, businesses need to evolve their security measures to match the threat. This will involve a multi-prong approach, including training, policy development and employing emerging cyber security technologies.

The security experts at eMazzanti keep abreast of threats and security tools as they evolve. We can guide you through the process of understanding your security needs and implementing a strategy to address them.