+44 345 094 0945
www.waterstons.com
Article

Voice Cloning – The Good, The Bad and The Ugly

Breadcrumb

1. Home /
2. Print /
3. Pdf /
4. Node /
5. Entity Print

Insight navigation

- Latest insights
- Latest news
- Articles
- Case studies

Download PDF

Aug 2023

Voice Cloning – The Good, The Bad and The Ugly

The rise in voice cloning is becoming an increasing threat to individuals, businesses and even governments. Scammers are starting to use the AI technology to commit crimes causing distressing situations for people all over the world.

Categories Cyber Resilience, Cyber Security Strategy

Aug 2023

Helen Hopwood-Curry

Information Security Consultant

Email

helen.hopwood-curry@waterstons.com

Voice cloning refers to the process of creating a computer-generated replica of someone's voice through the use of machine learning tools which mimic speech patterns, intonations and the vocal characteristics of people. Once the tool is trained it can often be indisguisable from the real thing, and can therefore be used for both good and bad. Worst of all, research from a recent McAfee report suggests it can take as little as three seconds of someone talking to make a clone of their voice.

The Good

Voice cloning technology can be beneficial for:

- Voice preservation
- Archiving the voice of individuals with degenerative conditions that may impact their speech, allowing them to communicate through speciality build machines.
- Speech Therapy
- Providing a model for individuals with speech issues to mimic or practice specific speech patterns, helping them improve their communication skills.
- Vocal assistant
- As well as speech therapy, it can be used as a vocal assistant, helping improve chatbots to make a more human experience, and interactions more intuitive and engaging.

The Bad

When new technology is released, there are always cases of misuse as some look at ways it can help aid criminal activities.

Identity theft

Identity theft is a real risk of voice cloning with people being deceived by voice impersonators leading to an increase in fraudulent activity, such as gaining access to personal accounts, making false statements, or social engineering distressing situations to trick people into making rash decisions. Some of the social engineering attacks include tricking family members, friends or colleagues into giving up information, such as passwords, or manipulating them into carrying out damaging activities such as sending them money to a specified account, exploiting the trust associated with the cloned voice.

Legal and ethical issues

Cloning someone's voice without their consent can infringe upon their privacy rights, and may violate laws related to fraud, impersonation or intellectual property.

The Ugly

Voice cloning has been used in instances of threat and harm against children, turbocharging fraud and scams by tricking parents into believing their children are in trouble.

In April 2023, it was reported that a scammer attempted to trick a mother into paying a $1 million ransom after cloning the voice of her 15-year-old daughter to pretend she had been kidnapped. It was reported that the scammer had used social media to develop the cunning scam, discovering that the teenager was away on a ski trip without her mother at the time of the 'kidnapping', therefore making it more believable.

A global concern of voice cloning is that impersonators may use the technology to mimic government officials and world leaders, which could lead to fraudsters successfully passing voice biometric systems to gain unlawful access to information, or in some instances may be used by state-sponsored attackers to spread misinformation, both of which could have devastating impacts.

How do we protect ourselves?

Voice cloning is constantly evolving, so it's vital to stay informed and adapt your security practices accordingly.

It is recommended that as voice cloning becomes more prevalent, individuals should be cautious with voice recordings, avoid sharing these with unfamiliar or untrusted sources. If you receive an urgent voice call or voice message from out of the blue, always question the source, consider confirming the information is correct before making any decisions or carrying out their request.

Stay vigilant and if the worst does happen – report it!

To find out more about how you can protect your business, and how interactive training can make your team even more vigilant to cyber threat, get in touch with cyber@waterstons.com