Is voice banking the Achilles heel of consumer security?

For those wary of digital banking, a phone call to the bank provides a comforting human touch. It's often the go-method for account alterations or large money transfers. But as the spectre of banking fraud looms large and increasingly sophisticated, the safety of voice banking is under scrutiny. Could an AI-generated voice convincin mimic a consumer and pilfer their funds?

Gur Geva, founder of iiDENTIFii

Impersonation is a favoured tactic amongst fraudsters. Armed with personal details or an AI-generated voice, they can infiltrate consumer bank accounts with alarming ease. The Southern African Fraud Prevention Service (SAFPS) reports a 264% increase in impersonation attacks in the first five months of 2022 compared to the same period in 2021.

Gur Geva, founder of iiDENTIFii, sheds light on the worrying trend. "The technology to impersonate an individual has become cheaper, easier to use, and more accessible. It's simpler than ever for a criminal to assume one aspect of a person's identity," he warns.

FINTECH

#WEF24: Startups to test their AI models on European Commission supercomputers

Katja Hamilton 24 Jan 2024

As the incidents of banking fraud multiply, it's time to question: is voice banking a safe option for consumers?

How voice impersonation works

Voice recognition systems in banking rely on a person saying something aloud, such as a unique catchphrase or passwo This is vulnerable to exploitation because synthetic AI-generated voice technology has evolved to such an extent that it is indistinguishable from real voices.

According to MIT and Google, generative AI voice cloning tools only need a minute of voice data–which is often scraped from social media–to create a result that is almost indistinguishable from the original.

The potential of this technology is vast. Microsoft, for example, has recently piloted an AI tool that, with a short sample of a person's voice, can generate audio in a wide range of different languages. While this has not been released for public us illustrates how much voice as a medium can be manipulated.

The appeal of voice recognition in banking

Voice recognition has a multitude of benefits. It is accessible to a diverse range of consumers, who only need a phone lin to perform banking tasks. Voice recognition programs can often pick up a voiceprint much faster than a person can type, which streamlines and reduces friction in the banking process for consumers without needing to enter complex passwords

“Historically, voice biometrics has been seen as an intimate and infallible part of a person’s identity. For that reason, many businesses and financial institutions used it as a part of their identity verification toolbox,” says Geva.

Audio recognition technology has been an attractive security solution for financial services companies across the globe, v voice-based accounting enabling customers to deliver account instructions via verbal commands.

> *“Voice biometrics offers real-time authentication, which replaces the need for security questions or even PINs.”*

One of the UK’s biggest banks, for example, integrated Siri to facilitate mobile banking payments without the need to open log into the banking app. An Abu Dhabi based bank introduces a biometric voice and voice-based authentication platform e-commerce which uses biometric sensors built into a standard smartphone.

“As voice-cloning becomes a viable threat, financial institutions need to be aware of the possibility of widespread fraud in voice-based interfaces. For example, a scammer could clone a consumer’s voice and transact on their behalf,” says Geva

Do our banks need to do away with voice authentication altogether?

Not necessarily. Thankfully, banks do not rely on a single form of authentication when performing a transaction. As the thr of cyber fraud grows, a rising number of local banks are investing in innovative, multi-layered biometric authentication protocols.

“Our experience in mitigating fraud and our research into rising AI-enabled cybercrime trends has led us to believe that voice authentication can be made safer if it is bolstered by additional remote digital verification methods," adds Geva.

> *“We recommend to banking clients that they adopt multimodel identity verification, especially for sensitive transactions”*

Voice biometrics in banking still serves several customers, particularly those who may need access to smartphone apps o in-person banking. While fraud risks abound, voice cloning is less of a threat to the public as it is difficult to roll out at scal as criminals would need to have access to substantial personal information for each target.

AI voice cloning technology may be cheaper and more accurate, but, if banks employ up-to-date, enterprise-grade biome authentication processes, they will be better protected.

“While identity theft is growing in scale and sophistication, the tools we have at our disposal to prevent fraud are intelligent scalable and up to the challenge," concludes Geva.

Face biometrics remains the strongest form of biometrics, as the face can be matched against a government issued, trust ID document, whereas a voice cannot.