The Threat of Voice Cloning

cyber security artificial intelligence

Summary: Artificial intelligence is taking voice recognition capabilities to new levels, creating multiple applications for financial institutions — both added conveniences for customers and enhanced security. Before embracing AI-backed voice software, however, financial institutions should be aware of the security risks they can create.

Within the first four days of its launch, "The Tinder Swindler," a documentary about how Shimon Hayut used a popular dating app to con women out of roughly $10MM, racked up just shy of 46MM hours in global viewing and rocketed to Netflix's top 10 lists in 92 different countries. Hayut, an Israeli man, used the alias Simon Leviev to pretend to be the wealthy CEO of diamond producer LLD Diamonds, and developed in-person relationships with multiple women he met on Tinder. He established enough trust with each of his marks that when he claimed he had been the victim of an attack that compromised and temporarily locked up his assets, each of them willingly loaned him massive amounts of money.

Unlike single people looking for love online, financial institutions have implemented countless mechanisms to verify that the individuals it deals with are in fact who they claim to be. As it turns out, however, voice recognition, one of the biometric methods that many institutions employ to verify a person's identity, could actually enhance their chances of becoming victims of fraud.

Ease of Use

As consumers seek ever-more-convenient and seamless banking experiences, many financial institutions have begun employing biometrics to make it easier for customers to access their finances and execute transactions. Multiple large banks, including Wells Fargo, Capital One, Lloyds Bank, and Chase, among others, already employ voice verification as a way of confirming customers' identities. The hope is that voice recognition provides a customer experience that removes the need for pin codes or customer service representatives to do business.

Voice banking capabilities also make it easier for handicapped people or individuals who have difficulty navigating mobile phones or computers to access banking services. Given the speed at which customers are embracing voice-based banking, its expected value is $3.7B by 2031.

"Sounding" the Alarm

Though voice recognition is appealing to financial institutions and customers alike, it may not be as secure as organizations previously believed. As artificial intelligence (AI) continues to evolve and lead to new uses, fraudsters have jumped on voice cloning apps to create almost indecipherable replicas of individual voices.

The quality of voice cloning has improved so much that fraudsters are using it to impersonate their victims' acquaintances to convince people to reveal sensitive information, or even transfer money. All criminals need to replicate someone's voice is a recording of them speaking for just a few seconds — a particular threat for high-profile individuals, whose voice recordings are widely available online.

From posing as family members needing money sent to resolve emergency situations to impersonating senior colleagues and instructing employees to wire payments to clients, there are countless instances where people have been conned through voice cloning. The technology is now so good that it has even fooled the biometric voice recognition features of some major financial institutions.

The Dangers of Voice Cloning

A recent article in the Wall Street Journal discussed how voice cloning was used to convince the CEO of an unnamed energy firm in the UK that his German boss wanted him to transfer €220K to the account of a Hungarian supplier. In such cases, fraudsters employ additional measures such as spoofing software that allows them to mask their true identity and location by mimicking legitimate numbers. Not surprisingly, scams involving voice cloning software are rapidly becoming a favorite of fraudsters. These scams resulted in losses of $2.6B in 2022, and voice cloning was the most frequently reported type of fraud. It generated the second-biggest losses for victims, according to the Federal Trade Commission.

Joseph Cox, a British journalist for Vice, recently wrote about how he was able to use voice cloning software to bypass the security measures of Lloyds Bank in England. Using a synthetic clone of his own voice, coupled with his date of birth — information that scammers have gotten creative at accessing through everything from phishing efforts and hacking databases or tricking people into revealing it through entertaining quizzes and memes on social media — Cox was able to get a replica of his voice verified by Lloyds' voice recognition software. He was then able to access his account information, including recent transactions and balance details.

Protecting Employees and Customers

As financial institutions embrace AI-backed voice technologies, both for security measures and customer convenience, it is important to be aware of the risks that exist. Given how readily available voice cloning software is (the program used by Cox to bypass Lloyds Bank's security was free online), financial institutions should make sure that they are using multifactor authentication and self-testing any weaknesses within their own offerings.

It is equally important to educate customers about voice cloning risks, particularly small business customers where employees may be more susceptible to being fooled by believable impersonations of a boss. Educating customers about the ease of impersonating loved ones, particularly elderly customers, has never been more important. Make sure your organization is constantly drumming it into people that voices and phone numbers can be easily replicated, and that if they ever receive such a call, they should hang up and dial their loved one or friend directly to verify it is them that they are speaking with.

AI-backed voice technologies are useful tools for security and for customer convenience, but awareness and education are key to ensure that your employees and your customers are cognizant of the risks and know how to protect themselves.

NEW PODCAST EPISODE: CRYPTO & BLOCKCHAIN

Learn the ins and outs of cryptocurrency, blockchain technology, and other digital assets from the experts at FS Vector. Plus, get insights on the most recent regulatory guidelines and other ways to leverage these technologies at your institution. Listen now.

ECONOMY & RATES

Rates As Of: 06/12/2023 06:43AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	5.37	-0.15	0.95
6M	5.39	-0.07	0.63
1Y	5.14	-0.01	0.44
2Y	4.58	0.18	0.15
5Y	3.91	0.16	-0.09
10Y	3.75	0.10	-0.13
30Y	3.89	0.02	-0.08

FF Market	FF Disc	IORB
5.08	5.25	5.15

SOFR	Prime	OBFR
5.05	8.25	5.06