forbes.com

Fraudsters Cloned Company Director’s Voice In $35 Million Bank Heist, Police Find

Thomas Brewster

5-6 minutos

Deep fake voice heist scores crooks $35 million. Cybercriminals cloned the voice of a company director in the U.A.E. to steal as much as $35 million in a huge and complex heist.

getty

AI voice cloning is used in a huge heist being investigated by Dubai investigators, amidst warnings about cybercriminal use of the new technology.

In early 2020, a bank manager in the Hong Kong received a call from a man whose voice he recognized—a director at a company with whom he’d spoken before. The director had good news: His company was about to make an acquisition, so he needed the bank to authorize some transfers to the tune of $35 million. A lawyer named Martin

Zelner had been hired to coordinate the procedures and the bank manager could see in his inbox emails from the director and Zelner, confirming what money needed to move where. The bank manager, believing everything appeared legitimate, began making the transfers.

What he didn't know was that he'd been duped as part of an elaborate swindle, one in which fraudsters had used "deep voice" technology to clone the director's speech, according to a court document unearthed by *Forbes* in which the U.A.E. has sought American investigators' help in tracing $400,000 of stolen funds that went into U.S.-based accounts held by Centennial Bank. The U.A.E., which is investigating the heist as it affected entities within the country, believes it was an elaborate scheme, involving at least 17 individuals, which sent the pilfered money to bank accounts across the globe.

Little more detail was given in the document, with none of the victims' names provided. The Dubai Public Prosecution Office, which is leading the investigation, hadn't responded to requests for comment at the time of publication. Martin Zelner, a U.S.-based lawyer, had also been contacted for comment, but had not responded at the time of publication.

It's only the second known case of fraudsters allegedly using voice-shaping tools to carry out a heist, but appears to have been far more successful than the first, in which fraudsters used the tech to impersonate a CEO of a U.K.-based energy firm in an attempt to steal $240,000 in 2019,

according to the *Wall Street Journal*.

The U.A.E. case shows how devastating such high-tech swindles can be and lands amidst warnings about the use of AI to create so-called deep fake images and voices in cybercrime.

"Audio and visual deep fakes represent the fascinating development of 21st century technology yet they are also potentially incredibly dangerous posing a huge threat to data, money and businesses," says Jake Moore, a former police officer with the Dorset Police Department in the U.K. and now a cybersecurity expert at security company ESET. "We are currently on the cusp of malicious actors shifting expertise and resources into using the latest technology to manipulate people who are innocently unaware of the realms of deep fake technology and even their existence.

"Manipulating audio, which is easier to orchestrate than making deep fake videos, is only going to increase in volume and without the education and awareness of this new type of attack vector, along with better authentication methods, more businesses are likely to fall victim to very convincing conversations."

Once a technology confined to the realm of fictional capers like *Mission: Impossible*, voice cloning is now widely available. Various tech startups are working on increasingly sophisticated AI voice technologies, from London's Aflorithmic to Ukraine's Respeecher and Canada's Resemble.AI. The technology caused a stir in

recent months with the revelation that the late Anthony Bourdain had his voice synthesized for a documentary on his life. Meanwhile, recognizing the potential for malicious use of the AI, a handful of companies, such as $900 million-valued security firm Pindrop, now claim they can detect synthesized voices and thereby prevent frauds.

If recordings of you speaking are available online, whether on social media, YouTube or on an employer's website, there may well be a secret battle going on for control of your voice without you knowing.

UPDATE: *After publication, the U.A.E. Ministry of Foreign Affairs & International Cooperation contacted Forbes to note that the affected bank was in Hong Kong, not within the U.A.E., though the Dubai investigators were leading the probe. The article was updated on October 22 2022 to reflect that.*

In a statement, HE Hamid Al Zaabi, director general of the U.A.E. Executive Office of Anti-Money Laundering and Counter Terrorism Financing, added: "Even with incidents happening outside the U.A.E., we will work closely with law enforcement partners around the world to identify and detect those individuals who knowingly engage in deceptive practices such as imposter fraud. The U.A.E. will then pursue to the fullest extent of the law these individuals, ensuring they are held accountable and brought to justice quickly."

Follow me on Twitter. Check out my website. Send me a secure tip.