AI voice cloning scam warning issued by bank

Posting voice recordings online could potentially lead to scam attempts being made against family members and friends, a bank is warning.

Voice cloning scams, where fraudsters can imitate a person’s voice by using videos uploaded on social media, could catch many people out, Starling Bank found.

Nearly half (46%) of people do not know this type of scam even exists, according to a survey for the bank.

The bank said AI (artificial intelligence) enables criminals use voice cloning technology to replicate a person’s voice from just a few seconds of audio, which can easily be captured from a video someone has uploaded online or to social media.

Scammers can then identify that person’s family members and use the cloned voice to stage a phone call, voice message or voicemail to them, asking for money that is needed urgently.

People regularly post content online which has recordings of their voice, without ever imagining it's making them more vulnerable to fraudsters

Lisa Grahame, Starling Bank

In the survey, one in 12 (8%) people said they would send whatever money was requested, even if they thought the call seemed strange.

The survey also indicated that nearly three in 10 (28%) people believe they have potentially been targeted by an AI voice cloning scam in the past year, according to the Mortar Research study among more than 3,000 people across the UK in August.

Starling Bank suggested that some people could consider agreeing a "safe phrase" with close friends and family members to help them verify the caller is genuine.

However, there could be a chance that safe words are compromised. The Take Five to Stop Fraud campaign urges people to pause and take time to think if it could be a scam.

People with doubts could call a trusted friend or family member to "sense check" a request or they could call 159 to speak directly to their bank.

Many banks can be reached this way, including Bank of Scotland, Barclays, Co-operative Bank, First Direct, Halifax, HSBC, Lloyds, Metro Bank, Monzo, Nationwide Building Society, NatWest, Royal Bank of Scotland, Santander, Starling Bank, Tide, TSB and Ulster Bank.

If someone believes they may have been scammed, they should contact their bank or payment provider immediately, as well as the police.

Lisa Grahame, chief information security officer at Starling Bank, said: “People regularly post content online which has recordings of their voice, without ever imagining it’s making them more vulnerable to fraudsters.

“Scammers only need three seconds of audio to clone your voice, but it would only take a few minutes with your family and friends to create a safe phrase to thwart them. So it’s more important than ever for people to be aware of these types of scams being perpetuated by fraudsters, and how to protect themselves and their loved ones from falling victim.”

She added: “Simply having a safe phrase in place with trusted friends and family – which you never share digitally – is a quick and easy way to ensure you can verify who is on the other end of the phone.”

Lord Sir David Hanson, Minister of State at the Home Office with Responsibility for Fraud, said: “AI presents incredible opportunities for industry, society and governments, but we must stay alert to the dangers, including AI-enabled fraud.

“As part of our commitment to working with industry and other partners, we are delighted to support initiatives such as this through the Stop! Think Fraud campaign and provide the public with practical advice about how to stay protected from this appalling crime.”

Actor James Nesbitt, who is taking part in Starling Bank’s campaign said: “I have children myself, and the thought of them being scammed in this way is really scary. I’ll definitely be setting up a safe phrase with my own family and friends.”