Um 'conselho' aos bancos que operam em Portugal: cuidado com as nossas vozes, "são um risco grande"

cnnportugal.iol.pt/inteligencia-artificial/fraudes/um-conselho-aos-bancos-que-operam-em-portugal-cuidado-com-as-nossas-vozes-sao-um-risco-grande/20250730/68820e00d34ef72ee448adda

CNN Portugal July 30, 2025

Usar a voz como forma de identificação dos clientes bancários é comum nos EUA e o CEO da OpenAI, criadora do ChatGPT, diz que "é de loucos continuar a fazer isso". Porque, explica Sam Altman, a inteligência artificial (IA) já é capaz de imitar a voz humana para contornar as verificações de segurança. Portanto: "é de loucos" usar a voz dos clientes porque aumenta loucamente o risco de fraude

Um banco que quer comprovar em Portugal a identidade de uma pessoa durante uma chamada telefónica recorre a métodos como as perguntas pessoais, “que estão associadas à identificação com alguma privacidade”. Há ainda a possibilidade, por exemplo, de códigos de SMS na interação entre bancos e clientes ou autenticações através das aplicações - ou seja, métodos que “obrigam a ter um controlo físico que está associado à pessoa”, explica o especialista em cibersegurança Bruno Castro, que é também CEO da VisionWare.

“O que temos visto é vários bancos a testar ainda o modelo de autenticação por voz, mas numa fase perfeitamente embrionária. Portanto, não está em produção”, diz Bruno Castro. A ser implementado em Portugal como método único ou principal de identificação e autenticação dos clientes, o método de impressão por voz teria um “risco elevado” associado. “Mesmo que o utilizem, não é o único fator que é pesado”, afirma o também especialista em cibersegurança Rui Shantilal.

O método de autenticação por voz consiste num pedido que é feito ao cliente para que este diga uma frase-chave com o intuito de provar a sua identidade para que consiga aceder à sua conta. Em Portugal o método de verificação por voz ainda não se aplica e os bancos recorrem a outros métodos.

“É um risco grande. Eu diria que isto não será a tendência da banca em aplicar este controlo como o único ou principal sequer”, sublinha Bruno Castro. O especialista acredita que, ao ser utilizado, este método, ou outros que requeiram o uso da voz ou imagem, serão associados a outro tipo de mecanismos de segurança e controlo de forma a “minimizar o risco que existe”.

O banco pode ainda socorrer-se de outros fatores de forma a proteger os seus clientes e tentar garantir a segurança dos mesmos durante uma chamada telefónica. “Pode pedir ao cliente para se autenticar dentro da aplicação bancária, pode pedir ao cliente um código secundário, pode enviar uma SMS para o cliente enquanto está em chamada”, enumera Rui Shantilal.

Outra situação: “O banco recebe uma chamada telefónica com a voz e com os dados de um cliente - que faz um pedido que parece inusitado. O banco pode adotar um procedimento complementar, no qual diz a quem ligou ‘ok, obrigado, registei o seu pedido’. Desliga e liga o banco para a pessoa. Ou seja, o atacante tinha, além de simular todo o exercício inicial, de intercetar esta chamada telefónica do banco”, diz Rui Shantilal.

Uma fraude "simples, rápida, barata"

Com o avanço da tecnologia, principalmente da IA, os riscos e ameaças aumentam e consequentemente as fraudes disparam. Quer os bancos, quer outras instituições devem estar aptos e qualificados para proteger os seus clientes e manter a devida segurança dos dados.

“Temos cada vez mais de nos socorrer de métodos de autenticação fortes para, no fundo, não sermos afetados por essa nova tendência de utilização da IA”, aconselha Rui Shantilal.

Além de ser possível replicar a voz, nos dias de hoje já é também possível a IA produzir vídeos manipulados de pessoas - técnica esta apelidada "deepfakes". “Já se começa a ver os atacantes a usarem isto em contexto de videochamada, por exemplo, no qual

entram em videochamadas e assumem a identidade de outra pessoa.” Trata-se de algo que, nas palavras de Rui Shantilal, “reforça ainda mais a necessidade de métodos de autenticação que sejam mais fiáveis”.

“O deepfake é uma ameaça, nomeadamente na voz... É uma ameaça grande. Eu consigo criar um deepfake de voz de forma simples, rápida e barata”, alerta Bruno Castro. Por outro lado, explica que “há vários mecanismos de fraude aplicados ao utilizador bancário que utilizam a IA”: phishing personalizado, deepfake ou sites clonados são alguns dos mecanismos utilizados que, com a ajuda da IA, levam a que o cliente seja enganado. Estes métodos, com a ajuda da IA, tornam-se “cada vez mais assertivos e a probabilidade de a vítima desconfiar é cada vez menor e, portanto, a taxa de sucesso da fraude é maior”.

Portanto: as fraudes “são cada vez mais bem feitas, personalizadas ao utilizador final e feitas de forma maciça”. Mas Bruno Castro não deixa de sublinhar isto: a banca está preparada para este avanço tecnológico e possíveis ameaças. “A banca sempre foi pioneira no tema da cibersegurança, por razões óbvias - guardam o nosso dinheiro e, portanto, são os garantes do dinheiro.” O especialista aponta ainda que a inovação e conservadorismo, característicos da banca no que diz respeito ao risco de questões tecnológicas, permite “implementar medidas de segurança que recebam a inovação a nível da IA mas em segurança”.