

ESTAFADORES CLONAN VOCES MEDIANTE INTELIGENCIA ARTIFICIAL PARA COMETER FRAUDES BANCARIOS

Por: R3D. 11/10/2023

El uso de herramientas de inteligencia artificial para imitar la voz de personas reales ha derivado en una nueva estafa de última generación: fraudes bancarios mediante *deepfakes* de voz, [según informa *The New York Times*](#).

El problema es muy nuevo y aún no se tienen datos de qué tan frecuente es, pero un vocero de Pindrop ?empresa que supervisa el tráfico de audio para muchos de los bancos más importantes de Estados Unidos? afirmó que este año habían detectado un aumento de su prevalencia y de la sofisticación de los intentos de fraude con voz por parte de los estafadores.

La gran velocidad con la que se mueve el desarrollo tecnológico en el mundo, aunado a los bajos costes de los programas de inteligencia artificial generativa y la amplia disponibilidad de grabaciones de voces de personas en Internet, están creando las condiciones perfectas para que los estafadores usen herramientas de IA para hacer fraudes usando voces generadas tecnológicamente.

Así, figuras públicas que tienen discursos o entrevistas que se pueden ver en diversos espacios en internet, incluidas redes sociales como Tiktok o Instagram, suelen volverse presas fáciles de los estafadores, quienes gracias a la disponibilidad de cuentas bancarias en mercados clandestinos, pueden hacer un emparejamiento entre datos bancarios y voces para cometer sus fraudes.

Hasta ahora, las voces falsas creadas mediante inteligencia artificial solo representan “un puñado” de las miles de llamadas de estafadores que suelen recibir los bancos, según Vijay Balasubramaniyan, fundador de Pindrop, y estos ataques recién empezaron a producirse desde el año pasado. La mayoría se han hecho en centros de atención telefónica de tarjetas de crédito, donde hay representantes humanos para atender a los clientes que tienen cuentas o servicios financieros con el banco.

Algunas de las herramientas de inteligencia artificial generativa, como VALL-E de Microsoft, podría crear una imitación de voz casi perfecta a partir de una muestra de audio de solo tres segundos, algo que se puede conseguir con cualquier video publicado en redes sociales.

El auge de las herramientas impulsadas por inteligencia artificial [representa un gran reto](#) para la educación, la seguridad digital y la desinformación. Sin embargo, pese a la sofisticación de este tipo de fraudes, vale la pena recordar que la mayoría se derivan de una amenaza básica a la privacidad que ha existido durante décadas: [la filtración de datos que revela la información personal de los clientes bancarios](#).

[LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ](#)

Fotografía: R3D. (CC-BY) Gibrán Aquino

Fecha de creación

2023/10/11