LITORALPRESS

Fecha: 20-09-2024
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo A
Tipo: Noticia general
Título: Las estafas telefónicas se vuelven más sofisticadas con la clonación de voz por IA

Pág. : 8
Cm2: 876,3

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Incluso se ofrecen servicios en el mercado negro:

Las estafas telefónicas se vuelven más sofisticadas con la clonación de voz por IA

Los ciberdelincuentes pueden usar videos y audios extraídos de las redes sociales para imitar la forma de hablar con herramientas tecnológicas. Así simulan un secuestro u otra emergencia para que se les deposite dinero o entreguen especies de valor.

ALEXIS IBARRA O.

EL MERCURIO

Aunque la voz suene familiar, hay que desconfiar de llamadas que piden hacer acciones urgentes y no le den tiempo de colgar y verificar su origen.

A Viviana le clonaron la voz y delincuentes la usaron para tratar de engañar a su familia. "Llamaron a mi papá haciéndose pasar por mí, con mi misma voz. Mi papá ni sospechó. Le decía que estaba secuestrada y que él debía sacar el dinero que tenía en el banco para depositarlo en una cuenta y así no me pasaría nada. La persona que se hacía pasar por mí trataba de hablar poco, llantos más que nada. Mi papá ya estaba en el banco cuando pidió que mejor le hablara en inglés —porque él es extranjero—, y la otra persona no pudo hablar y ahí mi papá se dio cuenta del engaño".

Las llamadas por teléfono han sido usadas hace años por los delincuentes para timar a personas, haciendo que entreguen dinero, especies valiosas o sus contraseñas. Este engaño clásico ha evolucionado, lo que podría considerarse una versión más tecnológica del "cuento del tío". Así, con herramientas de inteligencia artificial (IA), pueden imitar el tono de voz y el ritmo del habla de una persona para generar aún mayor confianza.

"Estas modalidades de estafas usan la IA, logrando casi a la perfección el timbre y forma de hablar de la víctima. A este método se le conoce como *deepfake-deepvoice* y se sabe de casos de fraudes asociados con llamadas a familiares, amigos, de jefes a empleados o suplantando a gerentes para solicitar en forma urgente dinero o alguna aprobación de transacción de dinero", dice Francisco Fernández, gerente general de Avantic Chile, empresa de seguridad informática.

Pero ¿cómo se logra clonar la voz de una persona? David López, vicepresidente de ventas para EE.UU. y Latinoamérica de la empresa de ciberseguridad Appgate, dice que "esto funciona con programas de IA y aprendizaje automático que pueden aprender y copiar los patrones de una persona a través de videos y archivos públicos. Luego, emplean su *software* para imitar la voz, con el objetivo de engañar o estafar a otros".

Los especialistas coinciden en que las fuentes para clonar la voz son extraídas por los ciberdelincuentes principalmente de archivos públicos, disponibles en redes sociales. "Una vez recabados los datos, pueden generar la simulación y los criminales pueden elegir las palabras que dirá la simulación", explica Fabiana Ramírez, investigadora de seguridad informática de ESET Latinoamérica.

Ramírez agrega que no se necesita que la muestra sea muy grande para poder hacer una clonación. Mientras que Fernández dice que incluso se pueden emplear audios de WhatsApp o sacarse de una llamada previa. Así, el delincuente podría llamar a la víctima con cualquier excusa —una promoción o una encuesta, por ejemplo— para grabar su voz.

Varias compañías de seguridad informática han alertado de este engaño. "Los avances en la IA generativa han propiciado la creación de contenido multimedia falso, cada vez más realista. Mientras más videos y audios con nuestra voz estén disponibles, más puede la red generativa entrenarse y generar una grabación convincente", dice Fabio Assolini, director de Análisis e Investigación de Kaspersky para América Latina.

Distorsionar llamadas

Ramírez cuenta que a nivel global se ha visto un aumento de este tipo de estafas desde 2022, "con la aparición de algoritmos de IA generativa accesible para cualquiera". El principal *modus operandi*, añade, es utilizar la voz clonada para hacer creer que la víctima de suplantación fue secuestrada. "También se han conocido casos de suplantación de voces de empresarios que solicitan, por ejemplo, transferencias a empleados de menor rango".

Incluso hay técnicas más sofisticadas como el *audio-jacking*: "El ciberatacante puede manipular silenciosamente una llamada de audio, sin que los participantes se den cuenta. En lugar de utilizar la IA generativa para crear una voz falsa, se intercepta una conversación en vivo y se reemplazan palabras específicas según el contexto, esas palabras podrían estar relacionadas con información financiera, médica o, incluso, podrían ordenar a un analista que venda o compre acciones y muchas otras cosas", explica Juan Carlos Zevallos, gerente de IBM Security Software para Latinoamérica. Por ejemplo, en una llamada real de un jefe, esta se intercepta y se le pide al empleado entregar ciertos equipos o información confidencial.

El equipo de IBM Security X-Force, explica Zevallos, interceptó y distorsionó una llamada en vivo con éxito para probar la factibilidad de hacer este tipo de engaños.

Héctor Rodríguez, comisario de la Brigada Investigadora del Cibercrimen, dice que no están investigando "casos que tengan que ver con fraude en que se utilice la voz clonada de una persona para engañarla". Aun así, reconoce que en policías de otros países se han registrado casos y que se han generado instructivos para prevenirlos.

"Es una derivación de los clásicos engaños, pero es más sofisticado, en que se usurpa la identidad de la persona para hacer el 'cuento del tío' más creíble. Normalmente buscan la transferencia de dinero, pero también datos como claves o información importante", añade.

Desde Kaspersky señalan que este fraude ha ido en aumento en el mundo; "en los últimos meses, la alteración de contenidos con IA ha dado un salto apuntando a la falsificación de voz", dice Assolini.

Y añade: "En Kaspersky hemos detectado el crecimiento del mercado negro de los *deepfakes* y *deepvoice*, donde el costo del contenido puede oscilar entre US$ 300 a US$ 20 mil por minuto, dependiendo de su calidad y complejidad".

El consejo de los especialistas es estar alertas a llamados sospechosos. "Los cibercriminales utilizan tres elementos para captar la atención para estafar: urgencia, emoción y dinero", concluye López.

Sugerencias para prevenir el engaño

"Dado que con muestras de nuestras voces se puede hacer la clonación, es recomendable evitar compartir en forma pública audios o grabaciones de voces", explica Fabiana Ramírez.

Al enfrentarse a la llamada dudosa, "se debe prestar atención a la calidad de esta. Sospechar si hay un tono monótono y que suene antinatural. También, si el audio es incomprensible o tiene ruidos extraños de fondo", recomienda Fabio Assolini.

El comisario Rodríguez sugiere tomarse un tiempo para analizar una llamada, aunque el interlocutor exprese urgencia. "Los delincuentes buscan que la víctima no tenga la oportunidad de cortar para llamar a otras personas y cerciorarse de que lo que se dice es verdad", añade.

Entre muchas formas de evitar ser engañado el comisario dice que es bueno establecer una palabra clave entre familiares que pueda confirmar que son ellos los que llaman. Y a nivel de empresa, "establecer protocolos de seguridad para retirar equipos, recibir órdenes de hacer depósitos, entre otras cosas".

Otra medida es no entregar contraseñas, códigos ni otra información importante, aunque la voz suene familiar. En esos casos, es mejor llamar de vuelta o hacer una comprobación de identidad.

Según Rodríguez, otra recomendación práctica es instalar en el teléfono aplicaciones que identifican llamadas. "Usan una base de datos colaborativa, creada por los mismos usuarios, y que identifican cuando las llamadas son *spam* o engaños telefónicos".

También se sugiere evitar llamadas de números desconocidos en los que se le haga hablar largamente, por ejemplo, para responder una encuesta sin una acreditación adecuada.

Finalmente, se recomienda denunciar el fraude para que así pueda ser investigado y evitar que otras personas sean víctimas en el futuro.