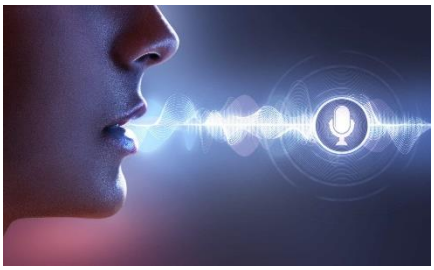
Ataques de clonación de voz con Inteligencia Artificial. (IA)

Ejemplo de un engaño en una llamada.



María, una maestra retirada disfrutaba una mañana tranquila en su casa. Un día, mientras disfrutaba de su café matutino, recibió una llamada desesperada de su nieto Pedro que estaba en la universidad. Su voz estaba llena de pánico mientras explicaba que había tenido un accidente automovilístico y necesitaba dinero urgentemente para pagar los daños y evitar problemas legales. Si no recibía el dinero de inmediato, podría terminar en la cárcel. La voz al otro lado era inconfundiblemente la de Pedro, el corazón de María se aceleraba de preocupación. Sin preguntar, corrió a su banco y transfirió dinero a la cuenta que Pedro le proporcionó. No fue hasta más tarde ese día que María llamó a la madre de Pedro para saber cómo estaba Pedro. Fue cuando María se enteró de que había sido estafada. La llamada había sido un truco cruel de un ciberdelincuente que había utilizado la tecnología de clonación de voz con Inteligencia Artificial (IA) para imitar la voz de Pedro, aprovechándose del amor y la preocupación de María por su nieto.

¿Qué es la clonación de Voz?

La clonación de voz es cuando alguien usa herramientas de Inteligencia Artificial (IA) para recrear la voz de una persona, incluir sus patrones de voz, entonaciones y ritmos de habla, creando una réplica casi perfecta. Un ataque de clonación de voz comienza cuando un ciberdelincuente recopila muestras de audio de la voz del objetivo.

Medidas de seguridad

Estas muestras se pueden recolectar de varias fuentes, como videos en YouTube o publicaciones personales en TikTok. Después de entrenar el audio grabado, la IA genera un nuevo audio que suena como el objetivo. Esta voz generada se puede utilizar de varias maneras, desde llamadas telefónicas hasta mensajes de voz, lo que la convierte en una potente herramienta para el engaño.

Al crear ataques de clonación de voz, los ciberdelincuentes suelen investigar primero. La mayor parte de la información que necesitan está disponible públicamente en los sitios de redes sociales. Estudian a sus víctimas para incluir tanto la voz de la persona a la que van a replicar como la víctima a la que van a llamar. Los ciberdelincuentes no solo aprenden a quién conocen y en quién confían sus víctimas, sino también vínculos emocionales que pueden más efectivos. Al realizar estas llamadas telefónicas, los atacantes cibernéticos a menudo modifican su identificador de llamadas por lo que cuando las víctimas miran sus teléfonos, la llamada telefónica parece provenir de un número en el que la víctima confía. El identificador de llamadas se puede falsificar fácilmente y no es una buena manera de validar o autenticar a las personas que lo llaman.

Como protegerse.

El primer paso para protegerse es ser consciente de que la clonación de voz con herramientas de Inteligencia Artificial ahora es posible y cada vez más fácil de hacer para los ciberdelincuentes. Estas son algunas medidas que puede tomar para protegerse:

Privacidad: Tenga en cuenta y limite la información que comparte con otras personas y restrinja quién puede acceder a sus grabaciones en las redes sociales como YouTube u otras redes.

Ser escéptico siempre: Esté atento a los indicadores comunes de que algo anda mal. Cada vez que alguien te llama con un tremendo sentido de urgencia o te presiona para que actúes de inmediato, lo más probable es que se trate de una estafa. Cuanto mayor sea el sentido de urgencia, como exigir dinero de inmediato, más probable es que alguien esté tratando de apresurarlo para que cometa un error. Otros indicadores comunes incluyen algo que es demasiado bueno para ser verdad (no, no ganaste la lotería) o cuando recibes una llamada inesperada que parece simplemente extraña.

Verificar: Si no está seguro de sí una llamada telefónica es legítima, cuelgue y vuelva a llamar a la persona a un número de teléfono de confianza. Por ejemplo, si recibes una llamada telefónica de un alto ejecutivo o compañero de trabajo de tu empresa, devuélvele la llamada a un número de teléfono de confianza que sepas que es realmente suyo. Si recibe una llamada telefónica extraña de un miembro de la familia, intente devolverle la llamada (tal vez incluso usar una videollamada) o llame a otro miembro de la familia que lo conozca bien.

Código de acceso (frase) o contraseñas familiares: Utilice una frase o contraseña secreta o un código de acceso que solo tú y tu familia conozcan. De esa manera, si recibe una llamada telefónica extraña que parece ser de un miembro de la familia, puede validar si es él solo si conoce su código de acceso secreto o frase familiar.

El contenido de este comunicado se proporciona únicamente con fines informativos y no constituye ni se interpretará como una recomendación, capacitación, instrucción u obligación, ni su contenido se tomará como base para cualquier decisión tomada por el destinatario. En cualquier caso, las decisiones tomadas al respecto serán solo suyas, no se basarán en la información proporcionada por MUFG, por lo que MUFG se deslinda de cualquier responsabilidad hacia usted con respecto a la caracterización o identificación de términos, condiciones y asuntos o riesgos legales u otros que puedan surgir en relación con cualquier herramienta, medida o estrategia implementada en materia de ciberseguridad u otros. La intención del mismo es proporcionar alertas sobre los diferentes riesgos que surgen diariamente y que pueden afectar a cualquier persona o institución.