Proliferan deepfakes de voz de famosos, con Facebook e Instagram como canales favoritos

Por: Cronica viva. 20/02/2024

Plataformas y redes sociales como **Facebook** e **Instagram** se han llenado en los últimos meses de los denominados '**deepfakes**' de voz de personas famosas, que respaldan sorteos y concursos fraudulentos, juegos de azar y oportunidades de inversión para intentar engañar a los internautas.

Los 'deepfakes' de voz se generan a través de herramientas de **Inteligencia Artificial** (IA) para crear copias sintéticas de la voz de otro individuo. Esto es posible porque dicha tecnología emplea técnicas de aprendizaje profundo para replicar el habla de una persona con un audio realista y convincente, debido a sus similitudes con la voz humana.

Frente a las voces sintéticas generadas íntegramente por un ordenador que utiliza sistemas de conversión de texto a voz, la clonación de voces usa la voz real de otro individuo para producir una interpretación realista del original.

Crear un 'deepfake' es relativamente sencillo, ya que solo necesario recopilar muestras de la voz humana que se quiere clonar, ya sea a través del audio de un vídeo o mediante una grabación física de alguien hablando.

Una vez se ha recogido esa muestra, el 'software' de clonación de voz la analiza para identificar las características de la voz, como el tono, el ritmo o el volumen, entre otras características vocales. Todos estos datos se utilizan para entrenar un modelo de aprendizaje automático.

Este proceso implica introducir los datos de voz en un algoritmo que sea capaz de aprender a imitar la voz original. Admite, además, la adición de más datos complementarios a este modelo y el ajuste de diferentes parámetros para refinar el 'deepfake'.

Taylor Swift vende derechos del filme 'The Eras Tour' en más de 75 millones de dólares

https://www.cronicaviva.com.pe/taylor-swift-vende-derechos-del-filme-the-eras-tour-en-mas-de-75-millones-de-dolares/embed/#?secret=idOpIdR2FI#?secret=sEEAA9jZoO

Si bien la clonación de voz tiene muchos usos legítimos, como la creación de asistentes de voz personalizados para el sector de la salud o para la educación, ya que se puede utilizar para ayudar a personas con problemas del habla, esta tecnología se usa también para actividades fraudulentas.

Entre algunas de las más dañinas se encuentran el ciberacoso, el chantaje o la creación de 'deepfakes' para manipular, engañar o dañar financieramente a otros usuarios, tal y como explica Bitdefender en su blog.

Las plataformas y redes sociales se han convertido en el canal de difusión de buena parte de estas estafas, debido a que millones de personas las utilizan a diario y cualquier campaña maliciosa puede tener un gran alcance.

Esto es algo que preocupa especialmente a sus usuarios, ya que más del 57 por ciento asegura sentirse intranquilo por su exposición ante esta tendencia creciente, como se desprende de un reciente sondeo realizado por los responsables de las soluciones de 'software' Voicebot y Pindrop.

La compañía de ciberseguridad ha hecho un análisis de este fenómeno y se ha centrado principalmente en los 'deepfakes' de voz que circulan por Facebook, plataforma desarrollada por Meta, aunque no es la única en la que proliferan estos ataques, ya que Instagram, Audience Network y Messenger se encuentran entre las principales plataformas distribuidoras de estas estafas.

En primer lugar, la firma ha determinado que la mayor parte del contenido fraudulento descubierto empleó generadores de voz de IA para clonar las voces de personajes famosos, como Elon Musk, Oprah Winfrey, Mr. Beast, Kylie Jenner, Vin Diesel, Jennifer Aniston o Tiger Woods.

Los ciberdelincuentes usaron la imagen de estas personas para promover diferentes engaños mediante vídeos publicitarios con una duración inferior a 30 segundos. En ellos, se ofertaban regalos de productos de alto coste, como el último modelo de iPhone, MacBooks, aspiradoras de Dyson e, incluso, asientos de coche para bebés de la marca Chicco, por un precio simbólico.

La compañía de ciberseguridad también ha indicado que se utilizaron los ‘deepfakes’ para promover inversiones y participaciones en juegos de azar, y que estas estafas llegaron a las víctimas a través de anuncios fraudulentos de la red social.

> Tik Tok: Universal Music retira su música tras no alcanzar acuerdo con la plataforma
>
> https://www.cronicaviva.com.pe/tik-tok-universal-music-retira-su-musica-tras-no-alcanzar-acuerdo-con-la-plataforma/embed/#?secret=LTfmsA1C89#?secret=F6SYQIFk7L

Para sumar víctimas, los estafadores llevaron a cabo el método tradicional de engaño, consistente en prometer un premio a los cien, mil o 10.000 primeros participantes o bien el retorno de estas inversiones multiplicado por cinco.

Una vez las víctimas hacen clic sobre el enlace falso, se las redirigía a una página web fraudulenta en la que se promociona el sorteo y donde se encumera una cantidad limitada de dispositivos y productos restantes.

Tras completar una encuesta falsa, en la que se preguntaba a los usuarios si eran mayores de edad, entre otras cuestiones, se presentaba un formulario que el usuario debía cumplimentar, introduciendo sus datos personales -nombre completo, correo electrónico, número de teléfono, etc.- y bancarios para pagar el producto a una cantidad generalmente mayor a la inicialmente indicada.

FÁCILES DE IDENTIFICAR

Bitdefender ha aclarado que, de acuerdo al análisis que ha realizado de los ‘deepfakes de voz en Facebook, los grupos demográficos más afectados por esta clase de fraudes de voz son los que tienen edades entre los 18 y los 65 años.

Con ello, ha reconocido que, a pesar de que se trata de un método cada vez más sofisticado, la mayoría de los vídeos y suplantaciones de voz analizadas para este estudio “están mal ejecutados” e incluyen indicios “muy visibles y anomalías visuales” que permiten determinar que se trata de una estafa.

Entre algunas de estas evidencias, ha mencionado la más habitual, que son los movimientos de labios que no coinciden con lo que se está diciendo o las imágenes distorsionadas, entre otros ejemplos.

CÓMO PROTEGERSE DE ESTAS ESTAFAS

Según los cálculos de la firma de ciberseguridad, las estafas ‘deepfake’ de voz se dirigieron al menos a un millón de usuarios estadounidenses y europeos, en países como España, Rumanía, Francia, Austria, Bélgica, Portugal, Polonia, Suecia, Holanda, Chipre y Dinamarca. De hecho, un solo anuncio llegó a 100.000 usuarios.

Taylor Switf: bloquean búsquedas por difusión de imágenes manipuladas

https://www.cronicaviva.com.pe/taylor-switf-bloquean-busquedas-por-difusion-de-imagenes-manipuladas/embed/#?secret=tAv0QLY1RQ#?secret=8Ru1oYP1uI

Para evitar esta clase de estafas, Bitdefender ha comentado que siempre se debe verificar la calidad y la consistencia de la voz, debido a que las voces clonadas suelen tener tonos inusuales, ser estáticas o presentar inconsistencias en los patrones del habla.

También se debe escuchar atentamente el sonido del vídeo, para detectar si hay ruidos de fondo inusuales, así como verificar que se trata de una oferta legítima contactando directamente con la persona u organización que la promociona.

Y señalan que hay que desconfiar de aquellos anuncios y vídeos que prometen recompensas poco creíbles y, sobre todo, de formularios de contacto en páginas web desconocidas que soliciten datos personales y financieros.

Europa Press- Foto internet-medios

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ

Fotografía: Cronica viva

Fecha de creación
2024/02/20