MILENIO

Milenio Diario
Sección: Portada
2024-07-02 03:17:39 806 cm$^2$ Página: 1, 4 1/3

**Inseguridad.** Plataforma de autenticación dice que el crimen internacional puede suplantar voz y rasgos faciales; localizan 19 cuerpos en La Concordia, Chiapas CRISTINA OCHOA, JORGE MARTÍNEZ Y JHONATAN GONZÁLEZ, CDMX Y TUXTLA GUTIÉRREZ, PAGS. 4 Y 15

# Inteligencia artificial potenció diez veces el robo de identidad

## Fraudes tecnológicos

Sumsub, plataforma de verificación, revela que el crimen internacional puede suplantar voz y rasgos faciales; México, el cuarto país con más registros de *deep fakes* en Latinoamérica

# Inteligencia artificial potenció diez veces el robo de identidad

**Reportaje**

CRISTINA OCHOA
CIUDAD DE MÉXICO

El auge de la inteligencia artificial a nivel mundial ha abierto un nuevo *modus operandi* de fraude que va en aumento en el país con el robo de identidad ya sea por voz o rasgos faciales.

La plataforma de autenticación de identidad Sumsub destaca que entre 2022 y 2023 se incrementó 10 veces el número de *deep fakes* (imágenes, video o audios imitando a una persona), principalmente en mercados como Bangladés, Hong Kong, Latvia, Tanzania y Pakistán, aunque Latinoamérica fue la única región en la que todos sus países tuvieron crecimientos en reportes por fraude.

México triplicó los casos de robo de identidad y se ubicó en la cuarta posición con mayores registros de *deep fakes* en la región, solo detrás de Brasil, Argentina y Colombia.

De acuerdo con el reporte más reciente en la materia del Consejo Ciudadano para la Seguridad, en 2023 las denuncias por robo de identidad crecieron 218 por ciento en relación con el año anterior.

Mientras que el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública reporta 50 mil 79 carpetas de investigación iniciadas por fraude entre enero y mayo de 2024, un repunte de 10.6 por ciento respecto al mismo periodo del año pasado.

*Vishing* es el término utilizado para referirse a la suplantación de identidad a través de la voz, un mecanismo empleado para realizar fraudes.

El Instituto Nacional de Ciberseguridad de España indica que a través de ingeniería por teléfono se puede suplantar la identidad de una empresa, organización o persona para obtener su información.

En México la Guardia Nacional recibe al día un promedio de 200 denuncias de ciberataques al número 088, de acuerdo con el segundo subinspector de la corporación, José Alberto Bárcenas.

Advirtió que los chats con inteligencia artificial son herramientas de aprendizaje y comunicación, por lo que emitió algunas recomendaciones para evitar ser víctima de los ciberdelincuentes que se roban datos personales de los usuarios.

"Es una herramienta que nos facilita la vida; sin embargo, cuando este chat nos hace preguntas, por ejemplo, sobre nuestro nombre, correo electrónico, familia o datos más sensibles, en ese momento es mejor detener la alimentación de información", indicó en entrevista.

"Aún no logra diferenciar la ciudadanía cuáles tienen que ver con inteligencia artificial o cuáles son los delitos que transcurren de forma común; sin embargo, continuamos investigando para tener muy identificado cuál es el *modus operandi* y que la población logre identificar estas amenazas", agregó.

Sumsub señala que las industrias más propensas al fraude son el comercio electrónico, servicios profesionales, salud, transporte y videojuegos.

Mientras que Santander explica que en el caso del sector bancario suelen hacerse llamadas en las que un supuesto técnico intenta resolver una incidencia en temas de seguridad y le solicita varios datos a la persona usuaria, que posteriormente son utilizados para vulnerar su cuenta bancaria.

Ni famosos como Bad Bunny se han salvado del robo de identidad mediante inteligencia artificial; en 2023 cientos de cancio-

nes con su voz comenzaron a acaparar las redes sociales.

Aunque el sonido era idéntico al tono del puertorriqueño, esas no eran grabaciones suyas; el caso desató el debate sobre los alcances de las herramientas tecnológicas y los problemas que esto puede generar.

Veridas, compañía del segmento de identidad humana y tecnología biométrica, señala que la utilización de estas herramientas puede incluir fraudes financieros.

"Este tipo de situaciones representa pérdidas económicas significativas para la empresas y los individuos, además de un impacto reputacional", sostuvo Fernando Casas, quien es director general de Veridas para México y Latinoamérica.

Esta práctica no es nueva; sin embargo, el uso de la inteligencia artificial ha permitido que los defraudadores incursionen en otros sectores y permiten incluso tener voces similares a las de conocidos u otros que pueden afectar a empresas y usuarios, para quienes la distinción es compleja.

"Esto va a continuar avanzando en la medida que lo hagan las herramientas y se requiere de la colaboración con instituciones gubernamentales y privadas, lo cual es fundamental para proteger a los usuarios; a simple oído del usuario común es muy difícil lograr identificar una voz generada con estas tecnologías", añadió el especialista.

En este tenor, actualmente empresas de servicios bancarios trabajan en estrategias de procesos de identificación para el caso de clientes pensionados, donde se requiere la autenticación de los usuarios y en la que han implementado tecnología que ayude a diferenciar y evitar el fraude.

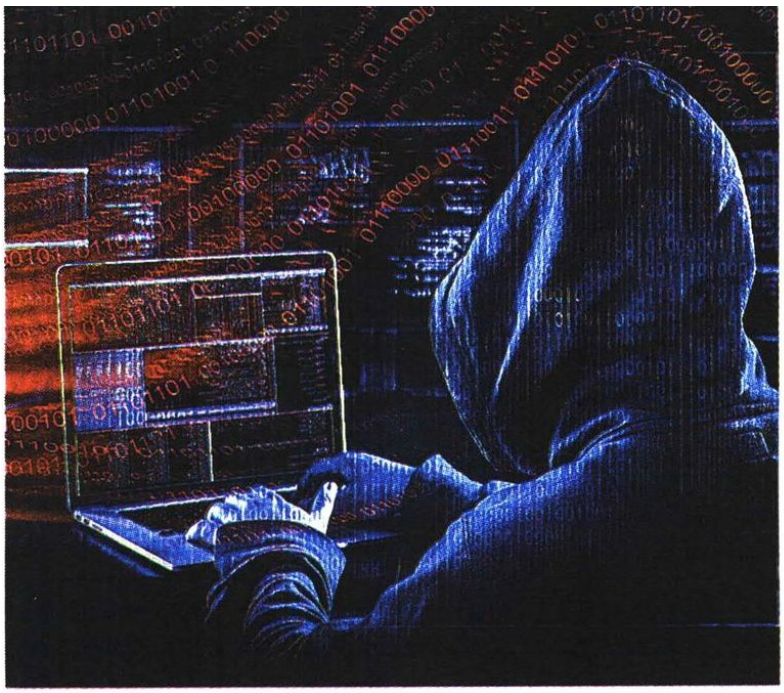
Veridas sostiene que a medida que otras industrias se digitalicen, sectores como el de la banca, hospitales y el *retail* implementarán mecanismos que ataquen este tipo de incidentes.

Por su parte, el subinspector Bárcenas agregó que los famosos *chatbots* son actualmente uno de los medios de consulta más empleados por los jóvenes dentro de la inteligencia artificial y aunque ésta se alimenta de los datos de las búsquedas, su uso en México no está regulado, lo que facilita a los criminales emplearla de forma ilegal.

"Es muy importante destacar que la Guardia investiga de forma cotidiana las tecnologías emergentes y de este modo podemos identificar cuáles son sus riesgos y amenazas".

**Con información de:** Jorge Martínez

## La GN recibe al día un promedio de 200 denuncias por ciberataques, de acuerdo con el subinspector José Bárcenas



SHUTTERSTOCK

# Suplantación al alza

México experimentó un aumento en este delito entre 2021 y 2023, periodo en el que los casos se triplicaron

● % de los ataques cibernéticos

**0.48**
2021

**1.27**
2023

**4**
**lugar**
México ocupa ese sitio entre los países de AL con más casos de *deep fakes*

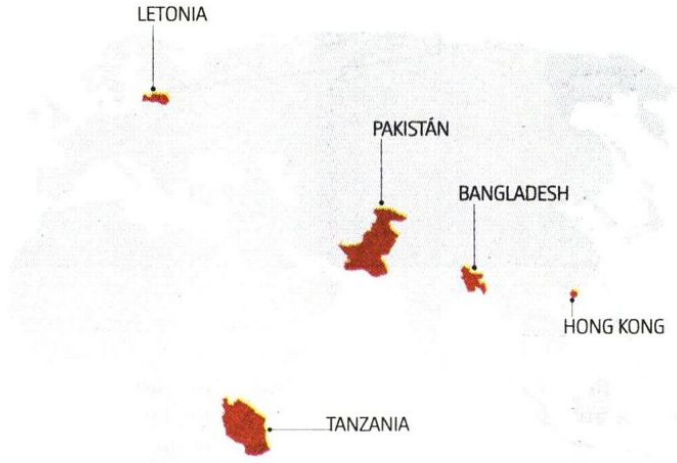
**10**
**veces**
Aumento en el número de *deep fakes* detectado en todo el mundo entre 2022 y 2023

**Latinoamérica**
Región donde todos los países tuvieron incrementos en reportes de fraude

## MÁS VULNERABLES

Electrónica | Servicios profesionales | Salud | Transporte | Videojuegos

## PAÍSES MÁS INDEFENSOS




· FUENTE: Consejo Ciudadano · INFORMACIÓN: Cristina Ochoa · GRÁFICO: Juan Carlos Fleicer