# IKUSI PROTECCIÓN TELEFÓNICA

mexico@ikusi.com · www.ikusi.com

## Los Retos

Cada día se vuelve más retador blindarse ante fraudes y proteger nuestra identidad personal y profesional, debido a que las personas y su información son el principal objetivo de actores maliciosos. Ya sea que posean datos personales o de la empresa, las personas siempre están expuestas a recibir llamadas y mensajes fraudulentos que ponen en riesgo su identidad, su dinero, y el acceso a información sensible.

Los criminales saben que **en el smartphone tenemos la información que da acceso a nuestra vida personal, económica y laboral**, por eso se mantienen actualizados en utilizar herramientas que les ayuden a lograr su objetivo, robar.

Por lo tanto, es ampliamente recomendable que las empresas brinden herramientas a sus empleados y a sus clientes para ayudarlos a evitar caer en fraudes y engaños que comprometan la reputación de la empresa, la continuidad de las operaciones y la información sensible que da acceso a los activos más importantes.

La manera más ágil y práctica para lograrlo, es convertir al teléfono en un arma contra estos riesgos. Una herramienta que funcione automáticamente, y que esté siempre vigilante para bloquear y neutralizar llamadas y mensajes de riesgo.

## Las principales amenazas a la seguridad telefónica

- **Vishing** es la práctica que busca engañar a las personas en una llamada telefónica, para así obtener datos de cuentas de acceso.
- **Smishing** es la práctica que invita a las personas a la acción a través de un mensaje de texto con contenido falso.
- **Extorsión telefónica** es la práctica de realizar llamadas o enviar mensajes de texto con alto contenido de violencia pasiva o agresiva, para obligar a la víctima a realizar una acción urgente y de alto impacto.
- **Estafa telefónica** se establece confianza con la víctima manteniendo un tono persuasivo, para invitarlo a la acción de transferir dinero.
- **Fraude guiado** aquí los estafadores guían a la víctima a través de un proceso para que el criminal logre su intención maliciosa.
- **Spam** son todas las llamadas no deseadas, ni solicitadas.
- **Deepfakes** se utilizan tecnologías de inteligencia artificial para crear videos, audios o imágenes falsificadas que parecen reales para engañar a la víctima.

## Casos relevantes de estas amenazas

### Caso 1. Ataque de vishing en firma financiera

A principios del año 2022, una de las principales firmas globales de servicios financieros informó que ciberdelincuentes accedieron a varias cuentas utilizando ataques de ingeniería social.

Utilizando **phishing basado en voz, o "vishing"**, los atacantes se hicieron pasar por la firma financiera llamando a los clientes, donde los alentaron a revelar información personal y financiera sensible, incluidos datos bancarios o credenciales de inicio de sesión. Los ataques de fraude, que en su mayoría ocurrieron en febrero, resultaron en que los estafadores transfirieran electrónicamente dinero a sus propias cuentas bancarias iniciando pagos mediante el servicio de pago Zelle.

*"Desafortunadamente, la estafa que afectó a algunos clientes de Morgan Stanley Wealth Management no es nueva"*, dijo Gary McAlum, analista senior de TAG Cyber. Señaló que esto no fue tanto por una violación de los sistemas de TI de Morgan Stanley sino que **fue una estafa dirigida a clientes individuales**, utilizando técnicas de ingeniería social para eludir los controles de autenticación normales.

*"Muchos otros clientes bancarios han sido víctimas de este tipo de estafa en el pasado"*, dijo McAlum. Lo que hace que esta técnica de fraude sea particularmente efectiva es la suplantación de un empleado del banco, que típicamente se presenta como un analista de fraude.

Según el informe *"Using Voice Biometrics and Phone Printing to Secure Telephony and Authenticate Callers"* de **Gartner** hasta el 30% de las tomas de control de cuentas financieras se trasladan a los canales de centros de llamadas y en línea. Los estafadores cometen delitos mediante la ingeniería social de los agentes de los centros de llamadas, que generalmente emplean métodos débiles para autenticar a los llamantes.

## Caso 2. Deepfake el "presidente" pide la rendición de soldados.

Algunos casos de deepfake vistos parecen inofensivos por tener intereses en entretener a usuarios en redes sociales, sin embargo, existen casos como el deepfake del presidente de Ucrania en el que supuestamente envía un mensaje a las fuerzas de su país para que se rindan ante el ejército ruso en medio del conflicto entre ambos países en marzo del 2022. Este caso tiene aún más relevancia debido a que los atacantes lograron emitir el video falso en un canal de televisión ucraniano, acto que afectó a la población de ese país y por el que las propias autoridades tuvieron que emitir un pronunciamiento para evitar que más personas caigan en la desinformación.

**Gartner** en su informe *"How to Mitigate Deepfake Identity Impersonation Attacks"* habló con diferentes proveedores del mercado, esta investigación muestra que no existen estándares sobre cómo evaluar la precisión de las soluciones de detección de voces deepfake.

Los líderes de IAM (Identity and Access Management) deben tener en cuenta que el detectar un deepfake mediante el uso de algoritmos de autenticación y verificación de datos, entre otras capas de seguridad, no son suficientes.

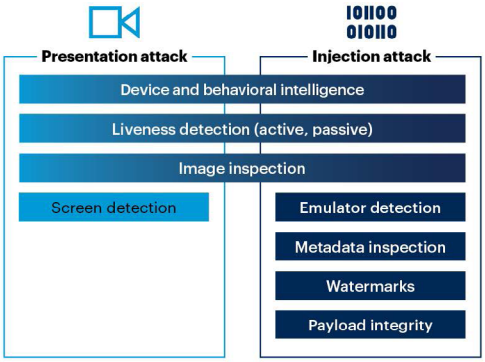
Todos los proveedores con los que Gartner habló como parte de esa investigación dieron cifras similares sobre la precisión de sus soluciones:

- Aproximadamente un 99% de precisión cuando se presenta una voz deepfake creada con una herramienta de generación de voz sintética que su equipo de inteligencia de amenazas ya ha descubierto y en la que su sistema de detección ha sido entrenado.
- Aproximadamente un 90% de precisión cuando se presenta un "ataque de día cero", lo que significa que la voz deepfake fue creada con una herramienta en la que su sistema de detección no ha sido entrenado.

Solo la detección de "vivacidad" y la inspección de imágenes podrían detectar potencialmente que se está utilizando un deepfake, y también podrían detectar ataques que no involucren un deepfake

Por ejemplo, un ataque en el que se esté reproduciendo un deepfake en una cámara virtual podría ser detectado porque se descubrió la presencia de una cámara virtual, en lugar de identificar el deepfake en sí. Esto subraya la importancia de considerar más estrategias, además del uso de tecnología, para detectar deepfakes.


**Techniques to Detect Presentation and Injection Attacks Involving Deepfakes**




Source: Gartner
823618_C

## ¿Cómo protegerse? No contestar. No responder.

La gran ironía de las amenazas telefónicas es que protegerse es tan sencillo como probable es que las personas no logren distinguir una llamada o mensaje falso en el momento oportuno. **La concientización sobre estas amenazas es crucial**, pero siempre será insuficiente, ya que las personas, inmersas en su rutina diaria, tienden a olvidar las señales claras que indican un intento de fraude, estafa o extorsión telefónica.

## Tips para reducir el riesgo:

No contestes llamadas con identificador restringido ó anónimo.

Asegúrate de tener registrados como contactos a las personas con las que hablas más frecuentemente o consideras importantes.

**"PAVLOVKSY"**

Ten una palabra clave especial que solo tú y tus más cercanos conozcan para usarla como palabra de confirmación en caso de sospecha de extorsión real.

**+001(895)455-1008**

Si el identificador de llamadas empieza con ceros, muestra símbolos y números, desconfia inmediatamente y no contestes. Si decides contestar, házlo con precaución.

NUNCA compartas datos personales al teléfono, como nombre, domicilio, RFC, datos de tarjetas bancarias, datos de credenciales INE, datos de pasaporte y factores de autenticación.

Si te llaman con ofertas, promesas de regalo y descuentos para cambio de compañía celular, desconfía inmediatamente y cuelga. Si deseas cambiar de compañia, visita la página web del proveedor o llama directo.

Si te llaman de un número desconocido y la llamada se corta inmediatamente o no escucha, nunca llames de regreso al número y agrégalo a lista de números bloqueados.

NUNCA aceptes seguir instrucciones del interolucutor para entrar a páginas web, enviar mensajes, hacer depósitos o transferencias. Si crees estar hablando con alguien conocido, cuelga y marca directo.

Si te llaman para ofrecer productos que sí deseas adquirir, visita primero la página web del producto, verifica la información y llama directo para ordenar.

Desconfía y ten precaución si recibes llamadas y mensajes de texto haciendo referencia a un mismo asunto.

**Protección automática y siempre vigente.**

Nuestro servicio de IKUSI **PROTECCIÓN TELEFÓNICA** hace que cumplir con estas recomendaciones sea mucho más fácil y efectivo, ejecutando controles de forma automática para proteger el conmutador y los celulares en todo momento.

IKUSI velatia | VoiSek®

# IKUSI **PROTECCIÓN TELEFÓNICA**

Nuestro servicio avanzado de protección telefónica, identifica, bloquea o redirecciona llamadas que se realicen con fines de fraude, extorsión, suplantación de identidad, robo de telefonía, interrupción y/o saturación de la red telefónica.

Este servicio avanzado de colaboración cuenta con tecnología que analiza en tiempo real las llamadas entrantes y salientes. Combinamos el análisis de comportamiento, políticas de control, listas negras y atributos telefónicos especiales, con nuestra experiencia en ciberseguridad y redes.

## Beneficios

+ Reducir casos de extorsión telefónica
+ Reducir la exposición de empleados a fraude
+ Evitar pérdida de información o económica
+ Cumplimiento de leyes de protección de datos
+ Asegurar la continuidad de servicios de centros de contacto
+ Optimizar el tiempo de autenticación de usuarios de centro de contacto

## Casos de uso

| | |
|---|---|
| **Rentabilidad de la estrategia multi-canal**<br>Los Centros de Contacto llegan a generar un volumen de más de 30 intentos de llamada simultáneos por agente, buscando que al menos uno de los números conteste, mientras que los usuarios reciben hasta 40 llamadas falsas al mes generando que simplemente los usuarios no contesten por confusión, o por temor al fraude. | IKUSI **PROTECCIÓN TELEFÓNICA** permite al usuario final distinguir entre una llamada real y una llamada falsa, y le dan el poder al usuario de validar, aun estando en conversación, si una llamada o un mensaje son legítimos en cualquier momento. |
| **Cultura de la seguridad digital y concientización**<br>Las campañas de concientización y de alerta sobre riesgos informan, pero también infunden temor, alejando al cliente del uso de los canales digitales para hacer sus operaciones. | IKUSI **PROTECCIÓN TELEFÓNICA** proporciona un mecanismo efectivo, transparente y sin fricción para neutralizar el fraude telefónico, generando una sensación de confianza y pertenencia entre empresa y cliente, ayudando a educar y concientizar de forma más efectiva en beneficio de ambas partes. |
| **Retorno de inversión**<br>Es una inversión efectiva pues propicia una disminución real en los costos de gestión de aclaraciones a la vez que incrementa la productividad de la estrategia de contacto multicanal y coadyuva a promover la adopción de los servicios digitales en el móvil. | Las iniciativas de IKUSI **PROTECCIÓN TELEFÓNICA** satisfacen los criterios de inversión tecnológica basados en la visión de cambios estructurales para mejorar la cadena de valor con innovaciones radicales en la protección de los clientes, así como también los criterios de inversión enfocados en generar rentabilidad directa en el corto plazo. |
| **Experiencia del cliente en la transformación digital**<br>Balancear una estrategia efectiva de prevención de fraude con los objetivos comerciales buscando un nivel mínimo de fricción con los clientes es retador. Mientras el cliente traslada la responsabilidad al proveedor, exige además una grata experiencia en la utilización de las apps. | IKUSI **PROTECCIÓN TELEFÓNICA** salvaguarda a las personas de manera natural con una herramienta común: el teléfono que usan todos los días. En paralelo, las herramientas habilitan a la empresa para deslindar responsabilidades cuando el cliente o el empleado hace caso omiso de las recomendaciones de seguridad. |

## ¿Por qué Ikusi?

En Ikusi despliegamos servicios de integración, ingeniería y desarrollo tecnológico para la transformación digital de negocios. Colaboramos con los clientes para comprender las peculiaridades de su negocio y, a partir de ahí, hacer que evolucione utilizando todo el potencial de la tecnología y de los servicios asociados.

Somos una empresa de servicios tecnológicos, especializada en digitalización, ciberseguridad, centros de datos, herramientas de colaboración y observabilidad.

## El valor diferencial de Ikusi Once

Llevamos a cabo toda la operación de los servicios gestionados a través del centro de operaciones unificado, Ikusi Once. Desde él monitorizamos, damos soporte y gestionamos proactivamente tus infraestructuras de TI.

Te ofrecemos atención, resolución y análisis de incidentes para asegurar la continuidad de tu negocio.

**IKUSI MÉXICO**
CIUDAD DE MÉXICO • MONTERREY • GUADALAJARA
**mexico@ikusi.com · www.ikusi.com**

### Notas

1* *Este gráfico fue publicado por Gartner, Inc. como parte de un documento de investigación más amplio y debe ser evaluado en el contexto de todo el documento. El documento de Gartner está disponible a solicitud de Ikusi.*

### Referencias

*Gartner, How to Mitigate Deepfake Identity Impersonation Attacks. 5 February 2025 - By: Akif Khan.*


*Gartner, Using Voice Biometrics and Phone Printing to Secure Telephony and Authenticate Callers. Refreshed 3 April 2017, Published 30 July 2013 - By Analysts Avivah Litan*


*Voisek | Guía para empresas. Todo lo que necesitas saber para que tu empresa esté a salvo de la amenaza #1 en el mundo digital: la ingeniería social.*

*https://www.scworld.com/analysis/morgan-stanley-wealth-management-accounts-breached-in-vishing-attacks*

*https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia*

Gartner®