Seguridad financiera a tu alcance

El poder de tus biométricos

Eficiencia en el mundo digital

BOLETÍN ESPECIAL

Prevención de fraudes | Ciberseguridad | Biométricos

EJEMPLAR GRATUITO | CONTIENE MATERIAL INTERACTIVO

Banco Azteca
Sueñas. Decides. Logras.

Aprende y Crece

Carta Editorial

Queridos lectores:

Imaginar un mundo donde las transacciones bancarias son tan simples y seguras como saludar a un amigo suena bastante emocionante, ¿no lo creen? Lo mejor es que ya es una realidad con la biometría en la banca digital.

En este boletín especial les explicaremos qué es el reconocimiento facial, cómo funciona y cómo protege sus cuentas bancarias. Además, exploraremos las herramientas que aseguran su información y los previenen de cualquier intento de suplantación.

¡Pero eso no es todo! También compartiremos historias de jóvenes que han adoptado esta tecnología y la utilizan de forma exitosa en su vida diaria. Y porque en la actualidad es fácil caer en noticias falsas, desmentiremos mitos comunes sobre la biometría y les mostraremos cómo ésta puede facilitar su vida financiera.

¡Bienvenidos!

Contacto

aprendeycrece@bancoazteca.com

BancoAzteca *@BancoAzteca* */BancoAzteca* *Banco-Azteca*

Contenido

LA CLAVE DE TU IDENTIDAD

Caras vemos, identidad desconocemos. ¡Y qué cierto es! Cada persona posee un conjunto único de características que los hace especiales y diferentes de los demás.

En el mundo bancario, la identidad es la llave maestra que valida quiénes somos. Por eso, cuando abres una cuenta, se crea un perfil de usuario compuesto por varios datos que aseguran la seguridad de tus transacciones financieras.

Estos son:

- **Reconocimiento facial:** Es una tecnología que identifica o verifica a las personas mediante el análisis de su rostro. Para ello examina la geometría y los rasgos faciales con el fin de medir distancias entre los ojos, frente, nariz y boca, así como descubrir la profundidad de las cuencas oculares y la forma de los pómulos, labios, orejas y barbilla. Y de esta forma convertir estos datos en una llave biométrica.

- **Huella dactilar:** Al ser una característica única y distintiva de cada individuo, formada por los patrones presentes en la piel, se utiliza ampliamente en la identificación biométrica bancaria, ya que es difícil de falsificar o replicar.

- **NIP (Número de Identificación Personal):** Es un pequeño, pero poderoso, código que eliges como clave secreta para tus aplicaciones bancarias. Solo tú deberías conocerlo, pues su uso añade una capa extra de protección, asegurando que solo el verdadero titular pueda acceder a la cuenta.

Juntas hacen que las experiencias bancarias sean más fáciles y confiables dentro de la App de Banco Azteca*.

¡Utilízalas!

*Consulta términos y condiciones de contratación y activación del servicio de Banco Azteca Móvil en www.bancoazteca.com.mx

Conoce el poder de tu huella

El poder de tus biométricos

Hace tan solo unos años estabas acostumbrado a demostrar tu identidad únicamente mediante el INE. Pero, ¿alguna vez te imaginaste estar en un banco y realizar todas las operaciones solamente con tu rostro?

¡La biometría ha hecho esto posible!

Pues analiza las características únicas de cada persona, como huellas dactilares, patrones faciales, voz o incluso la manera en que escriben, para autenticar su identidad.

¿Cómo lo ha aprovechado la banca digital?

La banca digital es una plataforma que te permite acceder a un sistema en línea para realizar tus movimientos bancarios, por ello no es de extrañar que haya adoptado la biometría. Y es que esta tecnología no solo mejora la seguridad, sino que también hace que las interacciones con el banco sean más fáciles y rápidas.

Antes

Era forzoso pasar a una ventanilla bancaria para abrir una cuenta.

Ahora

Los bancos permiten a los usuarios abrir cuentas en línea mediante la verificación de su identidad a través del reconocimiento facial o el escaneo de documentos oficiales combinados con datos biométricos.

Antes

Tenías que ir a una sucursal y presentar algún documento oficial o contraseña para acceder a tus cuentas bancarias y realizar cualquier operación bancaria.

Ahora

Puedes realizar operaciones bancarias dentro de tu aplicación únicamente con tu rostro para autenticarte.

¡Descubre el poder de tus biométricos!

Desenmascara mitos

GUARDIANES DE TU INFORMACIÓN

En la actualidad, mantener tu información bancaria segura es más importante que nunca. ¡Pero no te preocupes! Ahora tú, al ser un usuario financiero, tienes mayores herramientas que te ayudan a proteger tu información.

¿Cuáles son?

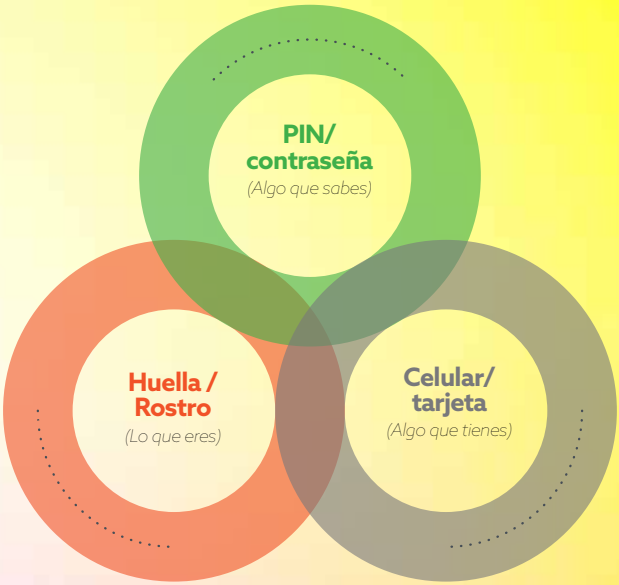
1. Métodos de autenticación
Como lo has visto anteriormente, los bancos han implementado tecnologías como la biometría dentro de sus servicios físicos y digitales, que permiten que solo tú puedas acceder a tu cuenta utilizando tu huella dactilar, tu cara o incluso el iris de tu ojo.

De esta forma, es como si tuvieras un guardián detrás de ti cada que ingresas a tu *app*, solicitas un préstamo o mueves tu dinero, el cual evita que alguien más se intente hacer pasar por ti.

2. Doble autenticación

Para añadir un nivel extra de seguridad, los bancos usan el doble factor de autenticación. Esto significa que, además de tu contraseña, necesitarás un código especial que te envían a tu celular, garantizando así que sólo tú seas quien accede a tu información.

Con estas dos herramientas es como si tuvieras un escudo integral que te protege con todo lo que te pertenece:



Y para darle más seguridad a tu información, las instituciones bancarias utilizan la encriptación de datos; es decir, cada vez que haces una transacción desde tu *app* bancaria, tus datos viajan en un código secreto que nadie más puede entender. Este proceso, llamado encriptación, asegura que aunque alguien intente espiar tu información, solo verá un montón de caracteres indescifrables.

¡Tu seguridad está en buenas manos!

Seguridad financiera a tu alcance

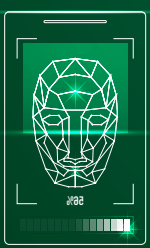
Tanto para la banca tradicional como para la móvil, la biometría trae consigo un montón de ventajas que hacen tu vida más segura y sencilla.

Te dan un mayor nivel de seguridad

La probabilidad de encontrar dos huellas dactilares similares a la tuya es de 1 en 64 mil millones, lo que proporciona una capa adicional de verificación que ayuda a reducir el fraude. Esto hace que sea casi imposible para los ladrones entrar en tu cuenta.

Mejoran la precisión

Las tecnologías biométricas reducen la posibilidad de errores que pueden ocurrir con otros métodos de autenticación.



Optimizan la experiencia del usuario

Con el uso de tecnologías como el reconocimiento facial, de voz y huellas dactilares, las transacciones se vuelven más rápidas, pues eliminan la necesidad de recordar múltiples contraseñas o llevar consigo documentos físicos.

Con estos avances, tus servicios financieros están cada vez más protegidos.

¡Anímate a descubrirlos!

EFICIENCIA EN EL MUNDO DIGITAL

Hoy en día, las oportunidades para aprovechar las ventajas del mundo digital son infinitas, especialmente cuando se trata de gestionar las finanzas. Si aún no te has decidido a utilizar sus herramientas, aquí te presentamos dos ejemplos de jóvenes que las han aprovechado al máximo.

Ejemplos que inspiran:

La estudiante organizada

Sofía es una joven de 24 años que acaba de terminar la universidad y para gestionar mejor sus ahorros y pagos decidió abrir una cuenta digital. Ahora, gracias a la App de Banco Azteca*, realiza todas sus operaciones desde el celular: paga servicios, ahorra para proyectos futuros e incluso invierte el dinero que le sobra. ¡Todo al alcance de un clic!

El emprendedor digital

Carlos, un joven de 28 años, es otro ejemplo de cómo las herramientas digitales pueden transformar la gestión financiera. Y es que, gracias a la banca digital, maneja las finanzas de su emprendimiento de manera sencilla: recibe pagos, paga a sus proveedores y organiza su presupuesto de forma rápida y eficiente.

¿Te animas?

Al igual que Sofía y Carlos, tú también puedes empezar a gestionar tus finanzas de manera más fácil, rápida y segura.

La digitalización está al alcance de todos, ¡aprovéchala!

*Consulta términos y condiciones de contratación y activación del servicio de Banco Azteca Móvil en www.bancoazteca.com.mx

¿Mito o verdad sobre la autenticación biométrica?

La tecnología biométrica está aquí para quedarse. Pero sabemos que, a medida que esta avanza, surgen mitos que generan desconfianza. Por eso, hoy queremos ayudarte a desentrañarlos y encontrar la verdad.

01

MITO
Mis huellas digitales están expuestas.

VERDAD
Aunque los datos biométricos se extraen inicialmente de una imagen, ésta no se usa en el proceso de autenticación; es decir, no se almacena como imagen completa, sino como códigos matemáticos difíciles de extraer.

02

MITO
La biometría atenta contra la privacidad.

VERDAD
Ninguna entidad que tenga tus biométricos puede hacer uso de ellos. De hecho, según la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, el usuario tiene el derecho legal de estar informado sobre cómo se utilizan sus datos personales.

03

MITO
La autenticación biométrica es más lenta.

VERDAD
Con esta tecnología dejarás de esperar minutos para acceder a tu cuenta, pues con sólo un toque o mirada podrás realizar ciertas operaciones dentro de la aplicación.

¡Despídete de esos mitos y abraza este nuevo sistema de autenticación!

BIOMETRÍA Y AFORE = AHORROS A SALVO

Como te has dado cuenta, la biometría ha ido tomando lugar en muchos campos, debido a sus grandes beneficios. Y las administradoras de los ahorros para el retiro no han sido la excepción. Sin embargo, tras su utilización, han surgido algunas afirmaciones que desinforman a los usuarios.

¿Cuáles son?

1. Es fácil falsificar datos biométricos y que otra persona acceda a tus ahorros.

Lo cual es falso, ya que esta tecnología no sólo ofrece un nivel adicional de seguridad, sino también está diseñada para detectar intentos de fraude, haciendo casi imposible la suplantación.

2. La biometría solo beneficia a las Afore, no a los usuarios.

La implementación de la biometría ofrece beneficios tanto para las Afore como para los usuarios. Para las Afore permite una administración más segura y eficiente de las cuentas, mientras que para los usuarios significa mayor protección contra el robo de identidad y fraudes, acceso más rápido y seguro a sus fondos, y una experiencia de usuario mejorada.

3. No tendrás control sobre tus datos biométricos.

¡Falso! Los usuarios tienen pleno control sobre sus datos biométricos. Las Afore están sujetas a regulaciones que garantizan la protección de los datos personales y biométricos. Además, los usuarios pueden solicitar en cualquier momento información sobre cómo se utilizan y protegen sus datos, así como ejercer sus derechos de acceso, rectificación y cancelación.

No le temas a esta tecnología, ¡mejor sácale provecho!

Banco Azteca

Sueñas. Decides. Logras.

Ahora sé cómo puedo seguir cumpliendo mis metas.

Con el diplomado en línea **e-Learning Financiero Aprende y Crece*,** te damos las herramientas para fortalecer tus finanzas personales de manera fácil y gratuita.

Regístrate

*Para más información sobre las herramientas para la administración de tu dinero, visita www.bancoazteca.com.mx/app/adminitración-dinero.html

ESCUDO
contra la suplantación de identidad

En la era digital hacer trámites bancarios es más fácil; sin embargo, con el auge de las redes sociales y el comercio electrónico también han crecido los riesgos de que alguien se haga pasar por ti.

Este delito es la suplantación de identidad e implica que alguien use tus datos personales sin tu permiso. Para ello, los estafadores suelen hacerse pasar por tu banco, solicitando tus datos por llamada, mensaje, correo o redes sociales, fingiendo premios o requiriendo validaciones para operaciones bancarias.

¡No temas! Mejor juega estratégicamente: cuanto menos sepan los estafadores, más difícil será que te engañen.

¿Cómo protegerte?

1. Antes de dar clic en enlaces de correos o mensajes, confirma la autenticidad llamando directamente a la empresa o institución bancaria.
2. Nunca compartas datos sensibles por correo, mensaje o llamadas no solicitadas.
3. Usa contraseñas únicas y difíciles para cada cuenta.
4. Verifica tus estados de cuenta regularmente.
5. Destruye documentos con información personal antes de deshacerte de ellos.

Aunque los estafadores pueden hacerse pasar por las entidades bancarias, también pueden suplantar tu identidad directamente y realizar fraudes a tu nombre. La mejor defensa es compartir poca información siempre.

Si ya fuiste víctima, actúa rápido y acude a la **CONDUSEF**, en donde te ayudarán a bloquear tu buró de crédito y denunciar ante el Ministerio Público lo sucedido, protegiendo tus derechos y evitando repercusiones legales.

Recuerda: tu identidad es un tesoro en el entorno digital. Mantente informado y evita caer en la trampa de la suplantación bancaria.

¡Sé el héroe de tu propia identidad!

CONOCE, EVITA Y DEFIÉNDETE DE LOS MENSAJES FRAUDULENTOS

Bien dicen que el conocimiento es poder, sobre todo cuando se trata de tu propia seguridad. Por eso queremos que en lugar de espantarte, te coloques el chaleco antifraudes y aprendas a esquivar o hacerle frente a los diversos fraudes cibernéticos que podrían ponerte en riesgo.

Uno de los más comunes es la suplantación de identidad por mensaje de texto, mediante el cual los delincuentes envían mensajes SMS para robar datos personales, que luego emplean en fraudes.

Y lo hacen mediante métodos diferentes...

Enlace de URL: Te envían un enlace para que descargues lo que pareciera una aplicación legítima y luego introduzcas información confidencial. Una vez que lo haces, roban tu información.

Sitio web falso: Un enlace te lleva a una web que solicita tus datos personales, mismos que ocupan en tu contra.

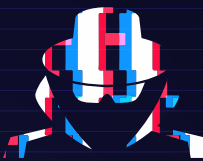
Ejemplos comunes son aquellos mensajes que parecen de una institución financiera confiable pidiendo información personal, pero su sentido de urgencia los delata. ¡No caigas en la trampa!

Mejor colócate tu protección y pon en práctica los siguientes consejos:

- Evita proporcionar datos personales o financieros por mensajería.
- No abras ningún enlace de remitentes desconocidos.
- Bloquea y reporta números sospechosos desde las aplicaciones de mensajería instantánea.
- No guardes información sensible en el teléfono.
- No respondas ni para negar la información.

Si caíste en este fraude, no te sientas avergonzado; mejor informa del ataque a tu institución bancaria, la cual te ayudará a bloquear las tarjetas que pudieron ser vulneradas; cambia contraseñas y códigos e informa a la policía cibernética comunicándote al 088.

Reconoce las señales



¡Correos sospechosos a la vista!

¿Sabías que existe un tipo de ciberataque que se realiza mediante la suplantación de identidad por correo electrónico?

Sí, nos referimos a una estafa a través de la cual se envían correos electrónicos que suplantan la identidad de compañías u organismos públicos y solicitan información personal y bancaria al usuario.

Así funcionan:

1. Envían un correo electrónico convenciendo u orillando al usuario a dar clic a un enlace.
2. Una vez que dio clic en el enlace adjunto, lo redirigirán a una página web fraudulenta para obtener sus datos o para que introduzca su número de tarjeta de crédito y la contraseña de acceso a su banca en línea.

¡Ojo! Estos correos electrónicos fraudulentos suelen incluir el logotipo o la imagen de marca de la entidad, pero en muchas ocasiones pueden contener errores gramaticales y usar un tono de urgencia que los delata.

¿Cómo protegerse?

- Verifica el remitente del correo para confirmar que proviene de la dirección oficial.
- Desconfía de enlaces y archivos.
- Recuerda que ninguna compañía o institución te pedirá información sensible a través de un enlace por correo electrónico.
- Asegúrate de descargar aplicaciones desde mercados oficiales; nunca desde enlaces en correos sospechosos.

Al igual que con los mensajes falsos, si ya fuiste víctima de este engaño, informa del ataque a tu institución bancaria y a la autoridad competente, quienes te ayudarán a bloquear tus tarjetas y denunciar este hecho.

¡Mantente alerta y protege tu información!

FRAUDES
A LA PUERTA DE TU CASA

Te hemos mantenido al tanto sobre los distintos fraudes cibernéticos que implican la suplantación de identidad de empresas o bancos. Sin embargo, ahora queremos alertarte sobre una nueva táctica que los delincuentes están empleando: *visitar tu domicilio*.

Sí, lo leíste bien. Los estafadores se hacen pasar por empleados de instituciones bancarias y llegan a tu hogar con excusas como el cambio de tu tarjeta de crédito por vencimiento, o para informarte sobre una atractiva promoción o premio. Todo esto con el único objetivo de obtener tu información financiera.

¡SIEMPRE DESCONFÍA!

Estos delincuentes suelen tener algunos de tus datos personales, como tu nombre, dirección y el banco con el que tienes tu cuenta, lo que puede hacer que confíes en ellos.

RECUERDA...

En Banco Azteca nunca enviaremos a nuestros colaboradores a tu domicilio, y bajo ninguna circunstancia te pediremos tus contraseñas y claves ni tomaremos fotografías de tus tarjetas.

¡Protege tu información!

Protege tu tarjeta

RING RING LLAMADA FRAUDULENTA ENTRANTE

La inmediatez de las llamadas telefónicas puede poner en aprietos a cualquiera, ya que muchas veces llegan cuando las personas están ocupadas o en situaciones que dificultan la comunicación. Precisamente por esta razón, los delincuentes se aprovechan para realizar engaños.

Con esto nos referimos a la suplantación de identidad mediante llamadas telefónicas, que consiste en una forma de fraude mediante el cual una persona se hace pasar por una empresa, institución bancaria o incluso una persona de confianza, con el fin de obtener información personal de sus víctimas.

¿Cómo operan estos estafadores?

01 Primero, los ciberdelincuentes suelen iniciar el fraude obteniendo información personal mediante correos electrónicos engañosos, sitios web falsos o haciéndose pasar por ejecutivos del banco.

02 ¡Llega la llamada decisiva! Con la información preliminar en mano, llaman solicitando datos sensibles como contraseñas, firmas electrónicas o códigos de verificación.

03 En este punto crítico es cuando se debe activar el escudo antifraudes: ¡Duda, verifica y actúa! Recuerda que ningún banco te pedirá información confidencial por teléfono para realizar cualquier operación.

¿Y si ya caíste en la trampa?

¡Actúa rápido!

1. Contacta a tu banco y revisa todas tus cuentas en busca de actividades sospechosas.
2. Si te pidieron instalar alguna aplicación durante la llamada, desinstálala de inmediato.
3. Si compartiste información de inicio de sesión, cambia tus contraseñas inmediatamente y habilita la autenticación de dos factores para mayor seguridad.
4. Denuncia el incidente a la policía cibernética.

La prevención es tu mejor defensa.

¡Mantente alerta y no dejes que los estafadores se salgan con la suya!

Tu dinero a salvo en cajeros automáticos

Recibir una transferencia, beca o algún apoyo económico es un momento de alivio y satisfacción, pero también implica un reto: retirar el dinero de manera segura. Por eso, te dejamos aquí unos consejos para que tu experiencia en los cajeros automáticos sea siempre segura.

Para que esto no te suceda, aquí te van unos tips:

1. Evita los cajeros automáticos en lugares oscuros, aislados o con poca gente; especialmente de noche.
2. Si ves personas sospechosas, busca otro cajero. Tu seguridad es lo primero.
3. Ten tu tarjeta a la mano antes de llegar al cajero, así evitarás distracciones y reducirás el riesgo de que alguien se aproveche de tu momento de vulnerabilidad.
4. Mira bien el cajero antes de usarlo. Si notas algo extraño, como partes sobrepuestas o alteradas, mejor busca otro.
5. Si el cajero tiene fallas, cancela la operación y retírate.
6. No permitas que nadie te distraiga mientras realizas tus transacciones.

En caso de emergencia...

Si el cajero retiene tu tarjeta, contacta inmediatamente a tu banco para bloquearla y prevenir fraudes, pero nunca aceptes ayuda de un extraño.

¡Cuida tu dinero y mantente alerta!

LA AMENAZA INVISIBLE EN LOS CAJEROS Y TERMINALES DE PAGO

Cada vez es más habitual insertar una tarjeta de débito o crédito en terminales de pago o cajeros automáticos, gracias a la comodidad que este método ofrece. Sin embargo, hay una nueva amenaza de fraude que debes conocer.

¿Has escuchado sobre el tallado de tarjeta

Es una técnica empleada por delincuentes para robar la información almacenada en la banda magnética de las tarjetas. Para ello utilizan dispositivos que colocan en cajeros automáticos, terminales de pago en tiendas y otros lugares donde se deslice una tarjeta, con el fin de clonar la información.

Al utilizar tu tarjeta en un dispositivo que ha sido alterado, todos los datos de tu tarjeta pueden ser capturados y almacenados. Los delincuentes luego emplean esta información para clonar la tarjeta y realizar compras fraudulentas.

¿Cómo puedes protegerte?

1. Antes de usar un cajero automático o terminal de pago, revisa si hay algún dispositivo suelto o partes que no encajen bien.

2. Usa tu mano para cubrir el teclado mientras introduces tu PIN, pues así dificultarás que cámaras ocultas lo capturen.

3. Activa notificaciones instantáneas en tu banca móvil para recibir alertas cada vez que se realice una transacción con tu tarjeta.

¡Infórmate y evita ser víctima de este tipo de fraude!

Cuida tu información

En esta época de compras, evita los fraudes de paquetería

Si has recibido SMS, WhatsApps, correos o llamadas para avisarte de la entrega de un supuesto paquete a tu nombre y argumentan que para darte información es necesario ingresar a un link.

El paquete no existe, se trata de un engaño.

Cuando das clic al link, das acceso al delincuente para robarte:

- Números de contactos.
- Cuentas bancarias.
- Información personal o de identidad.

Con esa información pueden cometer extorsiones, sacar créditos a tu nombre o cometer algún otro delito.

Sigue estos consejos

- Verifica la autenticidad del contacto.
- No compartas códigos ni contraseñas de tu dispositivo.
- Protege tus cuentas y dispositivos activando la autenticación en dos pasos.
- Mantente alerta a fraudes comunes.

Para recibir más consejos como este, suscríbete enviando un correo a educacionfinanciera@condusef.gob.mx

CONDUSEF
COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS

Banco Azteca
Sueñas. Decides. Logras.

Una llamada del banco puede no ser del banco.

Recuerda que Banco Azteca **nunca te pedirá información confidencial** al contactarte y mucho menos que ingreses a ligas o descargues aplicaciones para brindarte ayuda o soporte a distancia.

Si te encuentras en esta situación:

- **Detente** y mantén la calma.
- **Duda,** ¿estás seguro que es alguien del banco quien te contactó?
- **Verifica** por ti mismo cualquier movimiento o problema en tu cuenta a través de Línea Azteca, en la App de Banco Azteca Móvil o en una sucursal.

Recuerda que cuando tú llamas a Línea Azteca nuestros asesores pueden verificar tu identidad mediante breves preguntas de validación.

Descubre cómo protegerte de fraudes en **www.bancoazteca.com.mx/antifraudes**

Protege tu dinero. **Ponte atento.**

La amenaza oculta:

FRAUDES FINANCIEROS CON IA

¿Recuerdas la tecnología que utilizaban los villanos en las películas de Hollywood?

Bueno, hoy en día la realidad supera la ficción. Nuevas tecnologías, como la Inteligencia Artificial (IA), han servido como herramientas para facilitar nuestras actividades e incluso para hacernos más productivos en diferentes aspectos de nuestra vida diaria.

Sin embargo, los "villanos", que eran de ficción, se han transformado en una realidad, y pronto han encontrado cómo hacer un mal uso de esta tecnología, con el objetivo de robar nuestro dinero.

Hoy en día se han hecho más constantes los fraudes financieros y el robo de datos a través de la clonación de tu voz con IA. Este nuevo método de suplantación de identidad *[phishing]* se da cuando consiguen tu información a través de aplicaciones en tus dispositivos que han sido vulnerados, incluso del contenido que subes a tus redes sociales.

Te explico cómo sucede: con algunas aplicaciones de IA, generan la clonación de tu voz y se contactan con alguna persona cercana a ti, por ejemplo, tus papás, hermanos o pareja; lo hacen a través de apps de mensajería o por llamada, donde reproducen un audio con tu voz diciendo que te encuentras en una emergencia y que necesitan ciertos datos bancarios, como el NIP de alguna tarjeta o transferencias de grandes cantidades de dinero.

¡Ya sé! Suena como de ficción, pero el robo de identidad es uno de los delitos que han aumentado entre los usuarios de servicios financieros. Por ello, aplica las siguientes recomendaciones, que seguro te ayudarán a evitar caer en estos nuevos métodos de estafa:

- Revisa la configuración de privacidad en todos tus dispositivos móviles, para saber qué información estás exponiendo.
- Renueva tus contraseñas que creas vulnerables.
- Siempre genera doble o múltiple autenticación en tus dispositivos o aplicaciones bancarias, para que sea más difícil que entren en ellas. (Si no sabes cómo, revisa algunos videos).
- Siempre busca señales en audios, llamadas, fotos o videos que te parezcan sospechosos o raros y si es posible, comunícate con la persona involucrada; confía en tu instinto.

Si crees que tú o alguien cercano a ti ya cayó, te platico qué hacer: primero comunícate a las instituciones financieras que utilices y ponlas en alerta de lo sucedido, así evitarás perder tu dinero o hasta tener problemas legales. Y lo más importante: cuidarás tu salud financiera.

También puedes comunicarte a la CONDUSEF, donde recibirás asesoría para realizar tu denuncia.

Mantente al día con más contenido como este en:

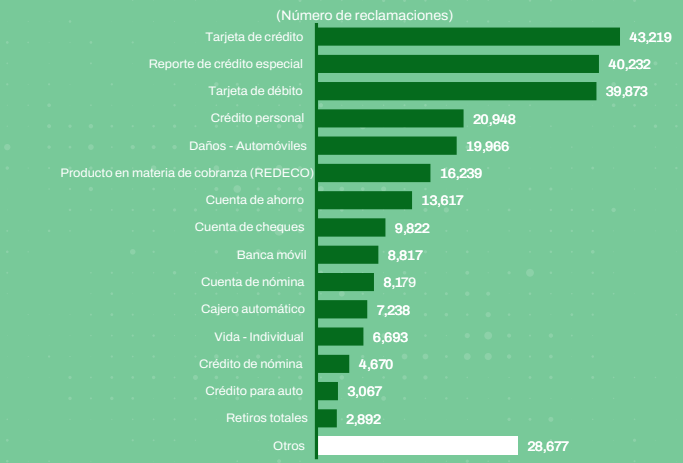
/Condusefoficial

CONDUSEF
COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS

ESTADO ACTUAL DE LA INCLUSIÓN FINANCIERA EN MÉXICO

De acuerdo con el Panorama Anual de Inclusión Financiera 2024, la CONDUSEF recibió más de 270 mil reclamaciones en 2023. Y los principales productos involucrados en estas reclamaciones fueron las tarjetas de crédito y el reporte de crédito especial. Además de productos como los siguientes:

- **Distribución de reclamaciones por producto**



CNBV. (2024). Panorama Anual de Inclusión Financiera.

Perfil de los afectados

Por edad

61%: adultos entre 30 y 59 años.
29%: mayores de 60 años.
10%: jóvenes de 18 a 29 años.

Por género

53%: hombres
47%: mujeres

Los estados con mayor número de casos reportados son:

1. Ciudad de México: 44,942
2. Estado de México: 32,887
3. Jalisco: 22,998
4. Chihuahua: 13,416
5. Puebla:10,981
6. Tabasco: 3,484
7. Tlaxcala: 2,728
8. Zacatecas: 2,645
9. Campeche: 2,229
10. Baja California Sur: 1,788

Existen muchas áreas de oportunidad para mejorar los servicios financieros y garantizar una mayor inclusión para todos los usuarios.

Mantente informado en:
https://www.gob.mx/cnbv

Banco Azteca

Sueñas. Decides. Logras.

Todo tu banco en un clic.

Ahora también puedes pagar tu crédito con la App*.

Además

- Abre una cuenta sin ir al banco
- Olvídate de las filas
- Consulta tu saldo cuando quieras
- Envía dinero de celular a celular

Aprovecha

*Consulta términos y condiciones de contratación y activación del servicio de Banco Azteca Móvil en www.bancoazteca.com.mx