# GUÍA PARA DENUNCIAR FRAUDES CIBERNÉTICOS

denuncia.org
IMPUNIDAD CERO
FRIEDRICH NAUMANN FOUNDATION For Freedom. México

Guía para denunciar fraudes cibernéticos

**Directora ejecutiva de Impunidad Cero**
Catalina Kühne Peimbert

**Investigación y redacción de texto**
Darío Preisser Rentería

**Diseño e ilustración**
Andrea Vallejo (Fugitiva)



Impunidad Cero agradece a la Fundación Friedrich Naumann por su apoyo para la elaboración de la presente guía.



## ÍNDICE

# GUÍA PARA DENUNCIAR FRAUDES CIBERNÉTICOS



## *Introducción*

La evolución de la tecnología, el acceso a internet y la transformación digital han traído enormes beneficios, pero también han multiplicado las oportunidades para que ocurran fraudes cibernéticos. En México, este tipo de delitos han crecido de manera alarmante en los últimos años, lo que ha afectado a millones de ciudadanos. Tan sólo durante 2023 se registraron 8.1 millones de reclamaciones por fraudes financieros, de las cuales 71% corresponden a estafas realizadas por internet (fraudes cibernéticos) y 29% a fraudes tradicionales.[1] Estas cifras nos hablan de la dimensión del problema y la urgente necesidad de prevenirlo.

Los datos de las autoridades de seguridad pública, así como las estadísticas nacionales, refuerzan esta preocupación. De acuerdo con la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (Envipe) del 2024, realizada por el Instituto Nacional de Estadística y Geografía (Inegi), el fraude es el delito más frecuente que sufre la población en México. Paradójicamente, también es de los menos denunciados: se estima que alrededor del 97% de los fraudes ni siquiera se reporta a las autoridades, lo que se conoce como *cifra negra*.[2] Este subregistro significa que la magnitud real de estos crímenes cibernéticos es mayor a la que reflejan las cifras oficiales, ya que muchas personas no buscan ayuda por desconfianza en las autoridades, por no saber cómo proceder o porque lo consideran una pérdida de tiempo.

Los ciberdelincuentes actualizan constantemente sus métodos para aprovechar vulnerabilidades humanas y tecnológicas. Las autoridades han advertido que los estafadores se hacen pasar por bancos, empresas de paquetería, plataformas de *streaming* u otras entidades legítimas para ganarse la confianza de la víctima.

Este entorno de amenazas en constante evolución hace indispensable prevenir. Conocer las tácticas de los defraudadores y actuar con precaución es la mejor defensa contra estas estafas.

---

[1] Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (2024). *Informe de autoevaluación. Enero-junio 2024.* https://www.condusef.gob.mx/documentos/transparencia/IA_ENERO-JUNIO-2024.pdf

[2] Instituto Nacional de Estadística y Geografía. (2024). *Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (Envipe) 2024.* https://www.inegi.org.mx/programas/envipe/2024/#documentacion

Impunidad Cero desarrolló esta guía de denuncia para contribuir a la cultura de la prevención, ayudando a las personas a identificar un posible fraude cibernético y, lo más importante, saber qué hacer cuando se es víctima de este tipo de delito. En esta guía encontrarás información sobre las principales modalidades de fraude cibernético y su forma de operación, recomendaciones prácticas de prevención, medidas de seguridad digital, consejos para proteger datos personales y señales de alerta a las que hay que prestar atención, así como los procedimientos para notificar a las instituciones financieras o de consumo involucradas.



## *¿Qué son los fraudes cibernéticos?*

Un fraude cibernético es cualquier estafa o engaño realizado a través de medios digitales como el internet, dispositivos móviles, cajeros, etc., con el fin de obtener un beneficio ilícito en perjuicio de otra persona.

En esencia, se trata de los mismos fraudes de siempre, pero cometidos por vía electrónica. De acuerdo con el Código Penal Federal de México, "comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido". [3] Cuando ese engaño se realiza mediante herramientas tecnológicas, hablamos de un fraude cibernético.

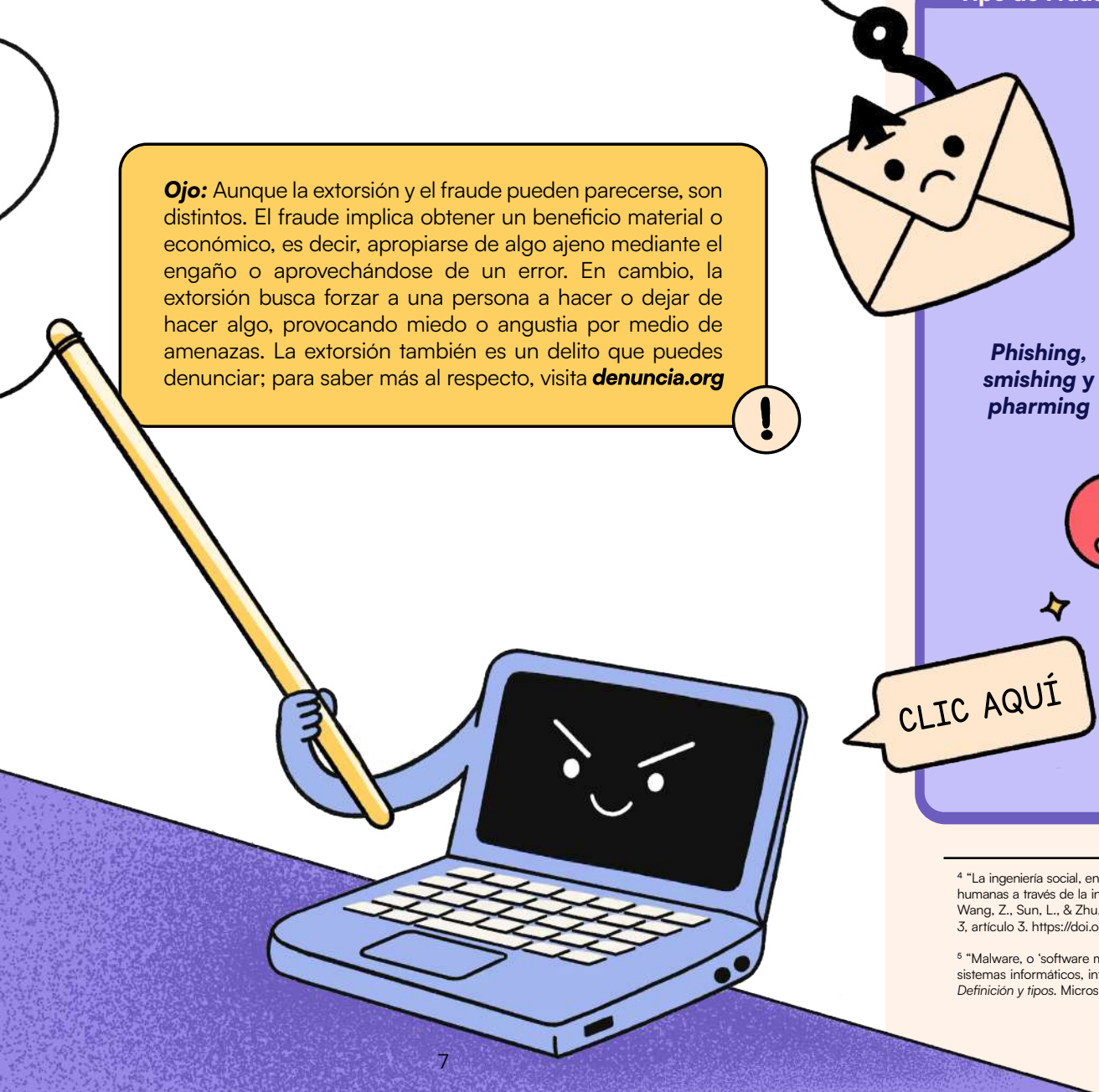
En general, cualquier conducta engañosa a través de la red o sistemas informáticos que busque robar dinero, bienes o datos, sean o no personales, puede considerarse un fraude cibernético; sin embargo, no toda conducta irregular o ilícita que se da en el ciberespacio entra en esa categoría; para que estemos ante un fraude cibernético, lo importante es que exista un engaño y un beneficio indebido.

Los bancos suelen estar en el centro de muchos fraudes cibernéticos, ya sea como objetivo principal —cuando los delincuentes buscan acceder a cuentas bancarias, tarjetas de crédito, banca en línea, etc.— o como medio utilizado en el engaño. Si bien los estafadores con frecuencia suplantan a estas entidades para ganar la confianza de la víctima, no siempre tiene lugar la participación de un banco, o la apariencia de su participación, para la comisión de un fraude cibernético.

[3] Cámara de Diputados del H. Congreso de la Unión. (1931, 14 de agosto). Código Penal Federal [Artículo 386, última reforma del 16 de julio de 2025]. *Diario Oficial de la Federación*. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

**Cualquier conducta que involucre el engaño mediante el uso de herramientas tecnológicas se considera un fraude cibernético.**

***Ojo:*** Aunque la extorsión y el fraude pueden parecerse, son distintos. El fraude implica obtener un beneficio material o económico, es decir, apropiarse de algo ajeno mediante el engaño o aprovechándose de un error. En cambio, la extorsión busca forzar a una persona a hacer o dejar de hacer algo, provocando miedo o angustia por medio de amenazas. La extorsión también es un delito que puedes denunciar; para saber más al respecto, visita ***denuncia.org***






## *¿Qué tipos de fraude puedes denunciar?*

Hay muchas modalidades de fraude cibernético, pero te compartimos las más comunes, que puedes denunciar si eres víctima de este tipo de delito.

| Tipo de Fraude | ¿En qué consiste? | Ejemplo: |
|---|---|---|
| ***Phishing, smishing y pharming*** | Son fraudes basados en ingeniería social[4] para robar información confidencial. Las tres modalidades buscan engañarte para que entregues voluntariamente tus datos creyendo que interactúas con una entidad real, cuando en realidad se los estás dando a un delincuente.<br><br>El ***phishing*** es la suplantación de identidad vía correo electrónico, que tiene como objetivo engañar al usuario para robar sus contraseñas, número de tarjeta, NIP u otros datos confidenciales.<br><br>El ***smishing*** es una variante del phishing, pero vía SMS (mensaje de texto al celular). La comunicación falsa aparenta ser de un banco u otra entidad popular, como Amazon, Mercado Libre e incluso Netflix y TikTok, e incluye un enlace a una página fraudulenta.<br><br>El ***pharming*** consiste en redirigirte automáticamente a un sitio web falso para robar tu información, a veces mediante ventanas emergentes o *malware*.[5] | El ***phishing*** ocurre cuando recibes un correo electrónico que aparenta ser de tu banco y te pide actualizar o confirmar datos ingresando a un enlace falso.<br><br>En el ***smishing***, un SMS podría decir "Banco X: Detectamos un cargo sospechoso. Verifícalo en este enlace...".<br><br>El ***pharming*** se da cuando estás navegando en un sitio web y se abre una ventana emergente que dice "¡Felicidades, eres el visitante 1 millón! Haz clic aquí para reclamar tu premio".<br><br>**¡Cuidado!**<br>**Si caes en la trampa, los delincuentes podrían acceder a tus cuentas, hacer transferencias o incluso solicitar créditos a tu nombre.** |

[4] "La ingeniería social, en el contexto de la ciberseguridad, describe un tipo de ataque en el que el atacante explota vulnerabilidades humanas a través de la interacción social para violar los objetivos de seguridad (como confidencialidad, integridad y disponibilidad)". Wang, Z., Sun, L., & Zhu, H. (2020). Defining social engineering in cybersecurity: A domain ontology and typology. *Cybersecurity, 3*, artículo 3. https://doi.org/10.1186/s42400-021-00094-6).

[5] "Malware, o 'software malicioso', es cualquier programa o fragmento de código informático diseñado con la intención de dañar sistemas informáticos, interrumpir su funcionamiento o acceder a ellos sin autorización" (Microsoft. [2025]. *¿Qué es el malware? Definición y tipos*. Microsoft Security).

| Tipo de Fraude | ¿En qué consiste? | Ejemplo: |
|---|---|---|
| **Cargos no reconocidos en tarjetas o cuentas** |  <br>Se refiere al uso de tus datos bancarios para hacer transacciones que tú no autorizaste. | Esto pasa cuando notas que te cobraron algo en tu tarjeta de crédito o débito o que hay un retiro de tu cuenta que no recuerdas haber hecho.<br><br>Puede ser que alguien haya obtenido los datos de tu tarjeta (por clonación o filtración) y los haya usado para hacer compras en línea, o que mediante otro tipo de fraude se hayan hecho cargos a tu cuenta. |

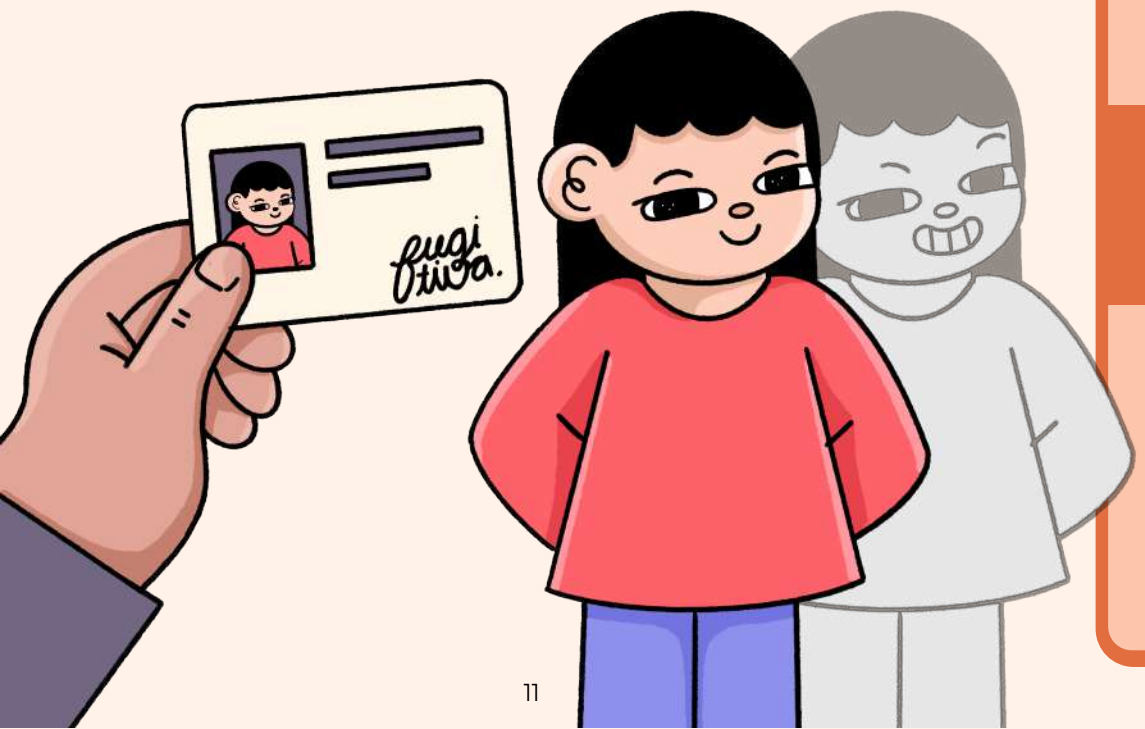

| Tipo de Fraude | ¿En qué consiste? | Ejemplo: |
|---|---|---|
| **Clonación de tarjetas bancarias *(skimming)*** | La clonación de tarjetas ocurre cuando delincuentes copian de manera ilegal la información contenida en la banda magnética o el chip de tu tarjeta, con el fin de crear una copia idéntica y usarla para hacer compras o retiros sin tu autorización.<br><br>Esto suele suceder en cajeros automáticos o terminales de pago donde se colocan dispositivos llamados *skimmers*, los cuales leen y almacenan los datos de tu tarjeta en el momento en que la insertas o la deslizas.<br><br>Por lo general, junto con el *skimmer*, también intentan capturar tu NIP (por ejemplo, con cámaras ocultas o mirillas en el cajero) para poder retirar dinero en efectivo.<br><br>La clonación de tarjetas es un delito explícitamente reconocido en la ley. | La clonación puede ocurrir, por ejemplo, cuando en algún establecimiento comercial pasan tu tarjeta por un lector escondido. |



| | ¿En qué consiste? | Ejemplo: |
|---|---|---|
|  <br>**Transferencias electrónicas no autorizadas** |  <br>Este fraude ocurre cuando se realiza una transferencia de dinero desde tu cuenta bancaria sin tu consentimiento. Puede suceder de 2 maneras:<br><br>1. Acceso ilícito a tu banca en línea: el delincuente entra a tu cuenta porque obtuvo tu contraseña, hackeó tu dispositivo o hizo *phishing* y, desde allí, transfiere fondos a otra cuenta.<br><br>2. Engaños: tú mismo realizas la transferencia creyendo que es por una causa legítima. | 1. Recibes un correo que parece del banco en el que te piden "verificar tu identidad" porque hubo movimientos inusuales en tu cuenta. El correo incluye un enlace parecido al de la página oficial del banco. Sin darte cuenta de que es un sitio falso, ingresas tu usuario y contraseña.<br><br>2. Esto suele suceder con las ofertas o premios falsos: te contactan (por correo, mensaje o incluso llamada) diciendo que ganaste algo o que hay un producto muy atractivo a la venta; en el primer caso, te piden una transferencia a una cuenta determinada para asegurarlo; en el segundo, te piden pagar un costo mínimo. Una vez que envías el dinero, descubres que el producto o premio nunca existió, era todo un engaño. |

| Tipo de Fraude | ¿En qué consiste? | Ejemplo: |
|---|---|---|
| **Acceso no autorizado a banca electrónica o aplicaciones bancarias** | Sucede cuando un tercero logra entrar a tu cuenta bancaria en línea o a tu aplicación móvil sin tu permiso.<br><br>Así, el delincuente puede revisar tu información financiera, robar datos personales o efectuar movimientos.<br><br>El acceso ilícito a sistemas informáticos es una conducta delictiva definida en la ley. | Esto generalmente implica que la persona responsable obtuvo tus credenciales de acceso (usuario, contraseña, NIP, código de verificación) mediante algún fraude previo y luego inició sesión como si fueras tú.<br><br>Este tipo de intrusión suele detectarse al notar movimientos extraños o recibir notificaciones de accesos hechos desde dispositivos no reconocidos. |

| Tipo de Fraude | ¿En qué consiste? | Ejemplo: |
|---|---|---|
| **Uso indebido de datos personales con fines financieros** | El robo de identidad es, en sí mismo, un delito señalado en la ley, que consiste en la obtención ilícita de datos personales con el fin de cometer un fraude o delito a nombre de la víctima.<br><br>Esta categoría abarca desde abrir una cuenta bancaria o trámite a tu nombre, solicitar un préstamo o tarjeta de crédito, contratar un servicio, hasta intentar vaciar tus cuentas existentes. | Esto sucede cuando, de manera ilegal, alguien obtiene información tuya —nombre completo, CURP, RFC, copias de identificaciones, estado de cuenta, etc.— y la usa para hacerse pasar por ti en alguna transacción financiera como solicitud de préstamos.<br><br>La víctima suele enterarse de este tipo de fraude cuando ya hay un daño. Empieza a recibir cobranzas de créditos que nunca solicitó, notificaciones de cuentas desconocidas o movimientos sospechosos en el Buró de Crédito. |







| Tipo de Fraude | ¿En qué consiste? | Ejemplo: |
|---|---|---|
| **Venta fraudulenta de productos o servicios por internet** | Son estafas en las que se aparenta ofrecer un producto o servicio en línea que, en realidad, no existe.<br>Este tipo de engaños es común en sitios de comercio informal, anuncios en redes sociales e incluso en páginas que imitan ser legítimas. | Un ejemplo típico es cuando ves un producto muy atractivo —un celular, una consola, un electro-doméstico— a buen precio en Facebook Marketplace o en una tienda en línea. Luego de contactar al "vendedor", éste te pide un pago por adelantado (por transferencia, depósito o envío de dinero) para apartar o enviar el artículo. Una vez hecho el pago, el vendedor desaparece y tú nunca recibes el producto.<br><br>En algunos casos, incluso pueden proporcionar facturas apócrifas o enlaces de pago falsos, es decir, envían un link que aparenta ser una pasarela de pago legítima (como la de un banco, mercado digital o app de envío de dinero), pero en realidad está diseñada para robar el dinero o los datos bancarios de la persona usuaria |

| Tipo de Fraude | ¿En qué consiste? | Ejemplo: |
|---|---|---|
| **Extorsión digital relacionada con cuentas bancarias** | Se da en situaciones en las que el estafador se comunica contigo (por teléfono, correo electrónico, redes sociales u otro medio digital) y te amenaza o te engaña para que le entregues dinero o información, usando como gancho tus cuentas bancarias o tu dinero.<br><br>A diferencia de un *phishing* que puede ser menos agresivo, la extorsión tiende a involucrar amenazas, engaños o manipulación emocional.<br><br>Otras formas de extorsión digital pueden incluir mensajes o correos de chantaje e incluso los llamados secuestros virtuales, donde vía telefónica hacen creer a la víctima que un ser querido está retenido y exigen transferencias de dinero a cambio de dejarlo en libertad. | Un ejemplo común son las llamadas telefónicas fraudulentas (*vishing*) en las que el delincuente finge ser del banco o parte de alguna autoridad: te dice que identificó un problema serio con tu cuenta (“notamos cargos extraños en su tarjeta”, “su cuenta fue hackeada”, “un familiar la usó indebidamente”, etc.) y que para “solucionarlo o evitar un mal mayor” necesitas proporcionarle información confidencial o incluso transferir tu dinero a una “cuenta segura temporal”.<br><br>Todo esto es falso y busca asustarte para que caigas en el fraude. |




| Tipo de Fraude | ¿En qué consiste? | Ejemplo: |
|---|---|---|
| **Engaños por inversión en plataformas falsas o *trading* fraudulento** | La estafa consiste en convencer a la víctima de que invierta dinero en algún esquema que promete ganancias extraordinarias, generalmente a través de un sitio web o aplicación móvil.<br><br>Los defraudadores suelen utilizar publicidad engañosa en internet y redes sociales, incluso recurriendo a la imagen de personajes famosos, a quienes hacen aparecer falsamente como si respaldaran la inversión para generar confianza.<br><br>En estos fraudes de inversión, inicialmente pueden dejarte “invertir” pequeñas cantidades y mostrarte en la plataforma falsos incrementos de saldo para engancharte a meter más dinero. Pero cuando quieres retirar tus supuestas ganancias, te ponen excusas, te cobran comisiones inesperadas o simplemente desaparecen con todo el dinero.<br><br>Algunos de estos esquemas son piramidales, es decir, usan el dinero de nuevos inversionistas para pagar rendimientos a los antiguos hasta que colapsan. | Recientemente, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) alertó sobre videos fraudulentos donde incluso se usó inteligencia artificial para imitar la voz e imagen de Carlos Slim, el empresario más rico de México, promocionando una supuesta aplicación de inversión que prometía “ganar $21,000 pesos diarios”. Todo resultó ser un montaje para que la gente diera clic a un enlace y entregara su dinero. |

| Tipo de Fraude | ¿En qué consiste? | Ejemplo: |
|---|---|---|
| **Préstamos falsos o usura digital (“monta deudas”)** | En esta categoría están las estafas relacionadas con préstamos de dinero engañosos por medios digitales.<br><br>Se ofrecen préstamos por aplicaciones que proliferan en tiendas no oficiales, o bien anuncios en los que prometen prestarte en minutos cierta cantidad con mínimos trámites.<br><br>Si bajas la aplicación, suele pedirte permisos excesivos (acceso a tus contactos, cámara, ubicación, etc.) y también te solicita fotos de tu identificación, datos personales y bancarios con el argumento de depositarte el préstamo.<br><br>Una vez que aceptas, pueden pasar dos cosas:<br><br>1. Nunca te dan el préstamo y sólo recopilaron tus datos para otro fraude, o te piden un pago por adelantado “para liberarlo” y luego desaparecen.<br><br>2. Sí depositan una pequeña cantidad a tu cuenta, pero en condiciones totalmente abusivas. Empieza así la usura digital: intereses impagables, comisiones no claras y un método de cobro basado en la extorsión.<br><br>Si no pagas puntualmente, las mismas personas detrás de la aplicación comienzan a hostigarte y amenazarte. Como les diste acceso a tus contactos, les envían mensajes a tus familiares y amigos diciéndoles que eres un deudor fraudulento; pueden llegar a enviarte montajes con tus fotos, amenazar con exhibirte o, incluso, con hacerte daño si no pagas.<br><br>Estas prácticas son totalmente ilícitas y violan múltiples leyes, desde protección de datos personales hasta extorsión y usura. | Por lo general todo empieza con la oferta de un préstamo fácil e inmediato, prácticamente sin requisitos, a través de una aplicación de celular. |


***Importante:*** No es tu obligación conocer la tipificación del delito para presentar una denuncia. Identificar de qué delito se trata es responsabilidad del Ministerio Público, no de la persona denunciante.

## *Recomendaciones para prevenir fraudes cibernéticos*

Aunque las autoridades y los bancos pueden apoyar en caso de ser víctima de un fraude, la experiencia demuestra que muchas veces no es posible recuperar todo el dinero ni revertir completamente los daños, además de que se trata de procesos largos y tediosos.

Por eso, resulta fundamental que cada persona adopte medidas de seguridad digital en su vida diaria. Estas prácticas preventivas no requieren conocimientos técnicos avanzados: se trata de hábitos fáciles de aplicar y que reducen el riesgo de padecer un fraude cibernético.

A continuación, te compartimos algunos consejos prácticos para protegerte en el uso cotidiano de medios digitales, cuidar los datos bancarios y personales, identificar señales de páginas y mensajes fraudulentos, y saber cómo actuar rápidamente si ya se ha caído en una estafa, con especial atención a niñas, niños, adolescentes, personas adultas mayores y otros grupos vulnerables.

También existen delitos cibernéticos relacionados con la violencia digital, como la ***sextorsión***, que ocurre cuando alguien amenaza con difundir imágenes íntimas o información personal para obtener dinero o más contenido sexual. Para saber más sobre estas formas de violencia, visita **violencia.digital**

## Recomendaciones para proteger tu información al usar medios digitales

***Actualiza tus sistemas operativos y/o utiliza un antivirus.***
Mantén tus dispositivos protegidos instalando un software antivirus de confianza y actualizando siempre tu sistema operativo y aplicaciones. Las actualizaciones corrigen fallos que los ciberdelincuentes podrían aprovechar, pero el antivirus añade una capa extra de protección: detecta y bloquea virus, fraudes en línea o archivos sospechosos en tiempo real. Para la mayoría de las y los usuarios, Windows Defender (gratuito e integrado en Windows) puede ser suficiente si se combina con buenos hábitos digitales. Para tener más seguridad, puedes optar por antivirus como Bitdefender o Kaspersky.[6]

***Mejora tus contraseñas.***
Utiliza contraseñas robustas y únicas para cada una de tus cuentas (combina mayúsculas, minúsculas, números y símbolos). De ser posible, utiliza administradores de contraseñas seguras en los navegadores de tus dispositivos personales a los que nadie más tenga acceso, como 1Password o Bitwarden.[7]

***Autenticación de dos pasos.***
Siempre que sea posible, activa la autenticación en dos pasos para añadir una capa extra de protección de acceso a tus cuentas sensibles. Estas medidas dificultan enormemente que terceros no autorizados accedan a tu información personal.

***Protege tu conexión.***
Sé precavido al navegar por internet y al utilizar tus cuentas en línea; evita conectarte a redes de wifi públicas o abiertas para realizar operaciones delicadas (por ejemplo, banca en línea), porque esas conexiones pueden ser inseguras y propensas a la interceptación de datos.

***Navegación segura.***
Comprueba que los sitios web que visitas sean legítimos y seguros, buscando el ícono del candado en la barra de direcciones y asegurándote de que la URL comience con “https://”.

[6] Roach, J. (2025, abril 28). Bitdefender vs Kaspersky: Picking the best antivirus for 2025. *Clowards.* https://www.cloudwards.net/bitdefender-vs-kaspersky/
[7] Micere, G. (2025, abril 26). The 10 best password manager tools in 2025: safest paid and free apps for all platforms. *Clowards.* https://www.cloudwards.net/best-password-manager/



***Cuidado con enlaces.***
No descargues archivos ni *software* de fuentes extrañas, tampoco des clic en enlaces sospechosos, ya que podrían contener *malware*. Algunos ciberdelincuentes suelen clonar páginas de confianza que pueden parecer legítimas, pero siempre cambia algo, ya sea el nombre de la página o el dominio del correo del que te escribieron. Algunos ejemplos son la página apócrifa *“www.amazonweb.com.mx”* o el correo falso*“facebook@messages.com”*. Sabemos que puede ser confuso y justamente ése es el objetivo de los defraudadores. Si tienes duda acerca de un correo o una página web, haz una búsqueda rápida en tu navegador de internet preferido para que puedas cotejar el sitio web o el correo electrónico.

***No compartas información personal*** sensible y mantén tus perfiles de redes sociales privados. Evita publicar en redes sociales, foros o formatos de registro información como tu número de identificación, domicilio, contraseñas, etc. Cualquier dato o foto que publicas en internet puede volverse accesible para terceros. Mantener discreción sobre tu información privada reduce las posibilidades de que alguien la use de forma malintencionada.

***Comparte buenas prácticas.***
Educa y protege a los miembros más vulnerables de tu familia. Las niñas, niños y adolescentes deben aprender a usar internet de forma segura: explícales los riesgos de hablar con desconocidos en línea y asegúrate de que sepan que nunca deben compartir datos personales ni contraseñas con nadie que conozcan sólo por internet.

***Supervisa la actividad de menores de edad.***
En la medida de lo posible, establece límites claros de tiempo en dispositivos móviles y, si es necesario, utiliza herramientas de control parental para bloquear contenido inapropiado o prevenir descargas peligrosas. Los delincuentes saben que las niñas y niños tienden a confiar en enlaces llamativos y descargas “gratuitas”.

### *Cuidado de personas adultas mayores.*

Ten en cuenta que, a veces, nuestros padres, abuelos u otros familiares de la tercera edad deben utilizar dispositivos móviles e internet para mantenerse en contacto con sus seres queridos, y muchas veces pueden no ser expertos en su uso, lo que puede volverlos un blanco fácil de las estafas digitales. Acompáñalos en el uso de dispositivos y explícales las recomendaciones básicas de seguridad, como que nunca deben dar contraseñas o códigos bancarios por teléfono, tampoco hacer clic en enlaces de mensajes sospechosos ni en anuncios en redes sociales. Si algo les genera duda, por ejemplo, una actualización o una alerta en el teléfono, recuérdales que es mejor pedir ayuda. Las actualizaciones son necesarias y seguras, y lo más recomendable es realizarlas con el apoyo de alguien de confianza.

### *Cuidado con el uso de la inteligencia artificial.*

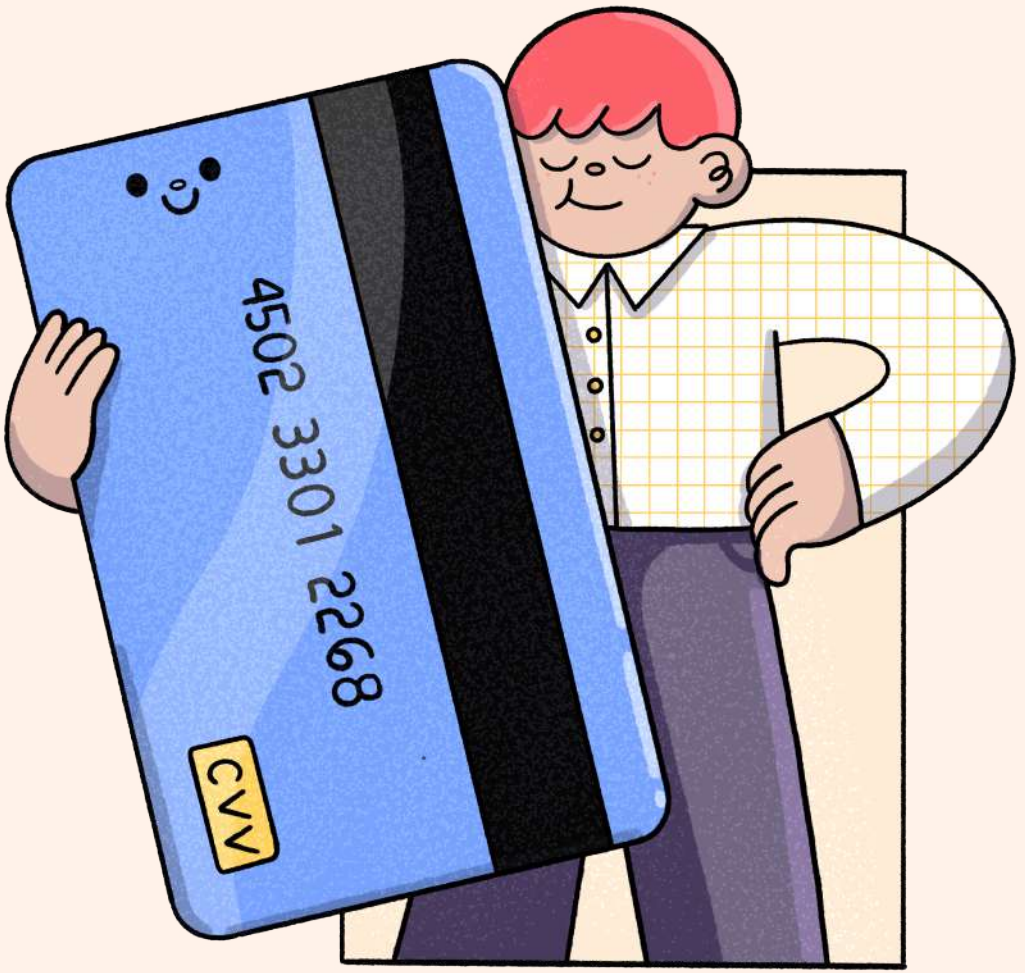
Los delincuentes digitales están empezando a utilizar herramientas de inteligencia artificial para hacer sus engaños cada vez más creíbles. Ahora pueden generar imágenes falsas *(deepfakes)* de personajes famosos o incluso políticos, como presidentes, que te invitan a invertir en una nueva herramienta que promete altos rendimientos; imitar voces humanas con gran precisión (como si te hablara un familiar o una persona de tu banco), o escribir mensajes perfectos, sin errores de ortografía o redacción, que parecen totalmente reales. Incluso pueden "entrenar" sistemas para que conversen contigo en tiempo real simulando ser un asesor bancario o técnico de soporte. Ante esto, nunca tomes decisiones apresuradas. Si recibes una llamada sospechosa, cuelga y llama directamente a la persona o institución desde un número oficial. No des clic en enlaces que no pediste, aunque parezcan legítimos. No compartas datos sensibles por teléfono o chat, aunque la persona diga que "ya tiene tu información". Verifica siempre por otro medio. Es mejor desconfiar y confirmar, que ser víctima de un fraude.

***Importante:*** Busca reforzar una cultura de ciberseguridad familiar en la que todos, desde el integrante más joven hasta el mayor, sigan buenas prácticas, ésta es la mejor forma de prevenir fraudes cibernéticos.



## *Recomendaciones para proteger tus datos bancarios y personales*

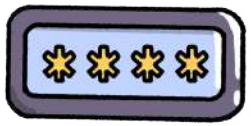
La información bancaria (como contraseñas, números de tarjetas, NIP/PIN de tarjetas, códigos de verificación, etc.) y los datos personales (números de identificación oficial, información financiera, etc.) son muy valiosos para los delincuentes. Los fraudes financieros en línea están en constante mutación y quienes los perpetran siempre buscan nuevas formas de engañar a los usuarios. Por ello, debes manejar estos datos con extrema precaución en todo momento para evitar robos de identidad o pérdidas económicas. Aquí te compartimos algunas recomendaciones para proteger tu información personal:



- Procura acceder a tu banca en línea sólo desde dispositivos y redes de confianza, nunca desde una red de wifi pública.

- Mantén protegidos tu nombre de usuario y contraseña de banca en línea; no los compartas con nadie y cámbialos de forma periódica. Ten en cuenta que un delincuente, si obtiene esas credenciales, podría vaciar tus cuentas rápidamente e incluso bloquearte el acceso cambiando la contraseña, sin que puedas recuperarla.

- Nunca reveles tu NIP o PIN de tarjeta a terceros; este código de 4 dígitos es la llave de tu dinero en cajeros y comercios, y si alguien más lo conoce, podría realizar retiros o compras no autorizadas fácilmente.



- Cuando pagues en línea, protege los datos de tu tarjeta (número, fecha de vencimiento, código CVV). Con esta información, un estafador podría realizar compras en tu nombre como si tuviera tu tarjeta física.

- Para mejorar tu seguridad en compras por internet, considera utilizar tarjetas digitales o funciones de tarjeta virtual que generen códigos CVV dinámicos, de modo que, aunque los datos fueran interceptados, no puedan reutilizarse por mucho tiempo. Estas precauciones reducen el riesgo de que tu información bancaria sea utilizada indebidamente.

- Mantén la guardia alta frente a intentos de ingeniería social dirigidos a tus finanzas. Como regla general, nunca proporciones información personal ni bancaria a desconocidos por teléfono, correo electrónico o mensajes de texto. Los bancos legítimos nunca te van a pedir por estos medios que les reveles tu contraseña de banca en línea, tu NIP, el código de tu token de seguridad ni los números completos de tus tarjetas.

- Si alguien afirma contactarte de parte del banco en el que tienes dinero o tarjetas y te solicita ese tipo de datos confidenciales, cuelga de inmediato, es casi seguro que se trata de un fraude. En caso de duda, puedes tomar la iniciativa de llamar directamente al número oficial de atención a clientes de tu banco (o acudir a una sucursal) para verificar cualquier asunto, en lugar de confiar en una llamada o enlace no solicitado.

- Desconfía de correos electrónicos supuestamente bancarios que incluyan enlaces para “verificar tu cuenta” u ofrecerte algún servicio, pues podrían dirigirte a sitios falsos que imitan a tu banco. Es más seguro escribir tú mismo la dirección web oficial del banco en el navegador o usar su aplicación móvil, en vez de seguir enlaces inesperados.

- Realiza un monitoreo frecuente de tus cuentas bancarias y estados de cuenta. Revisa periódicamente tus movimientos bancarios (saldos, transacciones recientes) para detectar cualquier cargo o transferencia extraña.

- Si identificas una transacción que no reconoces, notifícalo de inmediato a tu banco para que tomen las medidas correspondientes (por ejemplo, bloquear la tarjeta, revertir el cargo o cambiar credenciales de acceso) y así evitar daños mayores. Llevar este control rutinario te permite reaccionar a tiempo ante cualquier actividad sospechosa; al final del día, el mayor filtro de seguridad eres tú mismo.

## *Recomendaciones para identificar páginas y mensajes fraudulentos*

Los estafadores suelen hacerse pasar por empresas o personas de confianza para engañarnos, ya sea mediante sitios web falsificados, correos electrónicos o mensajes de texto. Su objetivo es que hagas clic en un enlace malicioso, descargues un archivo infectado o les reveles datos confidenciales creyendo que estás interactuando con una entidad legítima. Por eso, es fundamental aprender a reconocer las señales de alerta de un posible fraude en línea antes de caer en la trampa. Te compartimos algunos tips para que te sea más fácil identificar páginas o mensajes fraudulentos:

• **Desconfía de los mensajes que generan urgencia o alarma de manera inesperada.** Es común que los estafadores envíen comunicaciones diciendo, por ejemplo, que se detectó actividad sospechosa en tu cuenta (cuando en realidad no la hay), como:

- Que hay un problema con un pago que hiciste, o que debes "confirmar" tus datos personales o financieros urgentemente.
- Mostrarte facturas falsas de compras que nunca realizaste.
- Prometerte un reembolso de impuestos o un premio/cupón gratuito, e incluso amenazar con consecuencias si no actúas de inmediato. Este tipo de mensajes suelen tener un tono alarmista y apremiante ("¡última advertencia!", "su cuenta será bloqueada hoy", "oferta limitada, actúe ahora"), precisamente para que no te detengas a pensar. Ante cualquier mensaje de este tipo, mantén la calma y sospecha de comunicaciones con demandas inusuales o demasiado buenas para ser verdad.
- Presta mucha atención a los detalles del remitente y la forma de contacto. Si recibes un correo electrónico sospechoso, revisa la dirección del remitente: muchas veces, aunque el nombre que aparece pueda ser "Banco X" o "soporte técnico", se acompaña de un dominio desconocido o con ligeras alteraciones (por ejemplo, @bancoXYZ.com en lugar de @bancoXY.com).



- En mensajes de texto o llamadas telefónicas, ten presente que los estafadores pueden falsificar el número de origen para que en tu identificador aparezca el nombre o número de una institución confiable.
- No confíes únicamente en lo que ves en la pantalla: que un mensaje diga venir de tu banco o que una llamada muestre en el identificador "servicio al cliente" no garantiza que realmente provengan de esas fuentes.
- Si la comunicación te pide algo sospechoso (como datos personales, contraseñas, códigos), lo más prudente es no responder ni hacer clic en ningún enlace. En su lugar, verifica la situación por tu cuenta: abre tú mismo el sitio web oficial de la empresa en cuestión escribiendo la dirección en el navegador, o llama al número de su centro de atención (el que viene en tu tarjeta, estado de cuenta o sitio web legítimo) para confirmar si efectivamente hay algún problema. Por ejemplo, si un correo electrónico dice ser de tu banco y solicita que "revalides tus credenciales", puedes llamar al banco directamente para preguntar, casi con seguridad te responderán que ese mensaje era falso.
- Recuerda que los enlaces adjuntos y archivos en mensajes no solicitados pueden contener malware, por ello, nunca los abras sin tener certeza de su procedencia. Es preferible descartar o eliminar el mensaje sospechoso antes que arriesgarte a una infección por curiosidad.

## *¿Si ya fuiste víctima, qué puedes hacer para evitar más afectaciones?*

- Si lamentablemente ya fuiste víctima de un fraude cibernético, es importante actuar rápido para minimizar los daños. Lo primero es interrumpir cualquier comunicación con el estafador: deja de responder mensajes, llamadas o correos electrónicos sospechosos, tampoco realices más pagos ni proporciones más información. Luego, según el tipo de incidente ocurrido, toma las siguientes medidas lo antes posible:

- Si proporcionaste datos de acceso (usuario, contraseñas) o crees que infectaron tu dispositivo con *malware,* cambia de inmediato las contraseñas de tus cuentas comprometidas y de cualquier otra cuenta donde uses la misma clave. Crea contraseñas nuevas, robustas y distintas para cada servicio. Activar la verificación en dos pasos también es recomendable después de un incidente así.

- Actualiza y ejecuta tu *software* de seguridad (antivirus) en el dispositivo afectado para detectar y eliminar posibles programas maliciosos que se hayan instalado. Deja que el antivirus haga un escaneo completo y elimine cualquier amenaza encontrada. Si sospechas que tu computadora o teléfono sigue comprometido, considera desconectarlo de internet y, de ser necesario, llévalo con un técnico de confianza para una revisión más profunda o, incluso, formateo.

- Si compartiste información financiera, ya sean datos de tarjetas o cuentas bancarias, o realizaste un pago a un estafador, comunica de inmediato lo sucedido a tu banco o a la entidad financiera correspondiente. Por ejemplo, si entregaste detalles de tu tarjeta de crédito/débito o notas movimientos extraños, llama al banco y reporta el cargo o transferencia como fraudulento. Solicita el bloqueo de la tarjeta o cuenta afectada y, si es el caso, la reversión de la transacción y la expedición de una tarjeta nueva. Los bancos suelen tener protocolos para estas situaciones y mientras más pronto los notifiques, mejor posibilidad habrá de frenar o revertir los cargos indebidos.



Si un estafador logró hacer una transferencia desde tu cuenta, informa al banco que fue una operación no autorizada y pide que la cancelen y reviertan. Después de informar al banco, mantente alerta a tus estados de cuenta bancarios y de tarjetas en las semanas posteriores, también verifica y reporta cualquier cargo adicional que no reconozcas. Tu banco te puede guiar en pasos extra (como cambiar tus contraseñas de banca en línea, activar alertas de movimiento, etc.) para proteger tus fondos. De igual manera, recuerda guardar evidencia de lo ocurrido (correos electrónicos, capturas de pantalla, conversaciones), por si es necesaria más adelante.

Si sospechas que tu identidad pudiera estar comprometida (por ejemplo, entregaste datos muy sensibles como número de seguro social, CURP, RFC u otra información personal de identificación), además de las acciones anteriores, comienza a monitorear tu información crediticia y financiera de cerca. En México existen agencias de crédito u organismos gubernamentales que te permiten vigilar si alguien está usando tu identidad para abrir cuentas o contraer deudas, como el Buró de Crédito. También sería prudente colocar alertas o bloqueos temporales en tu historial crediticio para dificultar que alguien pueda abrir nuevas líneas de crédito a tu nombre sin verificación adicional. En nuestro país, puedes colocar alertas o bloqueos temporales en tu historial crediticio a través de los burós de crédito autorizados, como Buró de Crédito y Círculo de Crédito. Estas herramientas se llaman comúnmente Alertas Buró o Bloqueo de Reporte de Crédito, y sirven para que te notifiquen si alguien intenta abrir un crédito a tu nombre, o bien para impedirlo directamente.

Si un delincuente obtuvo acceso a tu computadora o teléfono (por hackeo directo, control remoto o suplantación de tu SIM telefónica), toma medidas inmediatas para recuperar el control de tus equipos y cuentas. Si el acceso fue a tu computadora de escritorio o laptop, desconéctala de la red y luego utiliza otro dispositivo seguro para cambiar las contraseñas de tus cuentas más sensibles por precaución.

Actualiza el sistema y ejecuta tu antivirus en el equipo comprometido para eliminar cualquier *puerta trasera* digital.[8] En caso de que el estafador haya tomado control de tu número de teléfono (por ejemplo, mediante duplicado de SIM), contacta a tu operador móvil de inmediato para reportar la situación y recuperar tu número telefónico cuanto antes. La compañía telefónica probablemente desactivará la tarjeta SIM fraudulenta y te dará una nueva.

Una vez que tengas nuevamente control de tus dispositivos o número, revisa a detalle la configuración de tus cuentas y asegúrate de que el estafador no haya agregado dispositivos de confianza ni

[8] Una puerta trasera (backdoor) es una construcción intencional dentro de un sistema que compromete su seguridad esperada al facilitar el acceso a funciones o información que normalmente están restringidas. Thomas, S. (2018, septiembre). Backdooring Neural Architectures via Architectural Weight Perturbations. En 21st International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2018), Québec, Canadá. Recuperado de https://www.s3.eurecom.fr/docs/raid18_thomas.pdf



cambiado tus métodos de recuperación; asimismo, verifica que no haya configurado reenvío de mensajes en tu correo u otras cuentas.

Vigila también tus cuentas bancarias y de tarjetas para identificar movimientos no autorizados, tal como se indicó antes, y repórtalos inmediatamente. Puede ser útil también ejecutar herramientas *antimalware* adicionales o, si tienes respaldos recientes, restaurar tus dispositivos a un punto anterior al incidente para asegurar que el intruso no mantenga acceso.

## *¿Dónde y cómo puedes denunciar?*

### Bancos

Si se trata de un fraude cibernético relacionado con tu banco, contáctalo de inmediato por sus canales oficiales. Todos los bancos cuentan con líneas telefónicas de atención al cliente, aplicaciones móviles o sucursales para reportar cargos no reconocidos, robo de identidad o posibles estafas.

**¿Sabes qué es la UNE?**

La Ley de Protección y Defensa al Usuario de Servicios Financieros establece que cada banco debe contar con una unidad especializada de atención a usuarios (UNE) para atender quejas e inconformidades. Por ello, si necesitas orientación o tienes algún problema con el banco, acércate a la UNE y contarás con apoyo especializado.

Fuente: Asociación de Bancos de México.

Es importante solicitar que bloqueen tu tarjeta o cuenta de forma preventiva y levantar una reclamación formal interna. Al presentar esta queja, el banco debe proporcionarte un número de folio y un acuse de recibo con fecha y hora.

Por ley, el banco está obligado a investigar tu situación y, en la mayoría de los casos de cargos no reconocidos, abonar provisionalmente el monto reclamado dentro de las 48 horas posteriores mientras realiza la investigación (misma que puede demorar hasta 45 días).

Durante ese tiempo, el banco no puede cobrarte intereses ni reportar la deuda al Buró de Crédito por el monto en disputa. Recuerda conservar toda la documentación que te entreguen (folios, estados de cuenta, comprobantes), ya que serán útiles si necesitas escalar el caso.



### Condusef

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros es el organismo público que te asesora y defiende en problemas con instituciones financieras. Si el banco no resuelve tu reclamación satisfactoriamente o consideras que tus derechos como usuario financiero fueron vulnerados, puedes presentar una queja ante esta institución.

Actualmente, la Condusef ofrece un Portal de Queja Electrónica (https://tramites.condusef.gob.mx/QuejaElectronica/index.php), donde puedes ingresar tu caso, seleccionando el banco y el motivo de tu queja.

También puedes acudir a cualquiera de sus unidades de atención a usuarios de manera presencial o pedir orientación telefónica. Condusef te orienta en el proceso y funge como mediador: una vez que reciba tu queja, solicitará al banco una respuesta formal y con soporte documental, buscando una solución equitativa.

Incluso si fuiste víctima de un fraude por parte de alguna entidad financiera falsa o no regulada, la Condusef recopila reportes a través de su Portal de Fraudes Financieros (disponible en https://phpapps.condusef.gob.mx/fraudes_financieros/index.php), donde cualquiera puede denunciar números telefónicos, páginas web, perfiles de redes sociales y correos electrónicos utilizados para fraudes.

Para asesoría inmediata, puedes contactar con la Condusef al número telefónico 55 5340 0999 o vía correo electrónico a asesoria@condusef.gob.mx; de esta manera, podrás conocer los pasos a seguir y los documentos necesarios para tu caso.

## Ministerio Público

Si has sido víctima de un delito como fraude, extorsión, robo de identidad u otra conducta ilícita, tienes el derecho de presentar una denuncia ante el Ministerio Público.

En México, esto puede hacerse ante la fiscalía o procuraduría de justicia de tu estado o ciudad, o bien ante la Fiscalía General de la República (FGR) si se trata de un asunto de competencia federal.

La denuncia normalmente se realiza de manera presencial acudiendo a la agencia del Ministerio Público más cercana a tu domicilio. Muchas fiscalías estatales cuentan con agencias especializadas en delitos cibernéticos o financieros; el personal ahí podrá tomar tu declaración.

Algunos ministerios públicos ofrecen opciones electrónicas o telefónicas para iniciar el proceso de denuncia de forma preliminar. En ciertos estados es posible iniciar la denuncia en línea llenando un formulario o llamar a números de atención para que te orienten y generen un reporte inicial; sin embargo, generalmente deberás acudir de manera presencial al Ministerio Público para ratificar la denuncia.

Cuando acudas al Ministerio Público, lleva una identificación oficial y toda la evidencia disponible, ya sean grabaciones de llamadas telefónicas, capturas de pantalla de mensajes o publicaciones, transacciones bancarias, etc. En la siguiente sección te explicamos a detalle lo que debes llevar. Al levantar la denuncia, no olvides pedir el número de carpeta de investigación y los datos de contacto del agente del Ministerio Público que llevará tu caso, pues con esa información podrás dar seguimiento a la denuncia.

Denunciar ante el Ministerio Público es un paso importante, ya que así se inicia la investigación legal y la autoridad podrá solicitar información a bancos, empresas telefónicas u otras entidades para perseguir a los responsables.



## Policía Cibernética

En paralelo a la denuncia tradicional, México cuenta con unidades especializadas de Policía Cibernética a nivel federal y estatal. Estas unidades se dedican a prevenir, investigar y combatir delitos cometidos por medios digitales, como fraudes por internet, extorsiones telefónicas, hackeos, acoso en línea, etc.

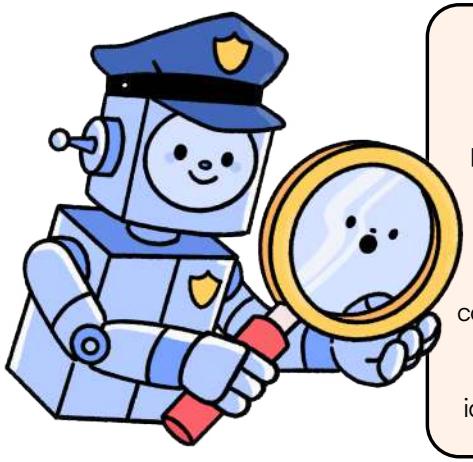
La Policía Cibernética brinda asesoría técnica a las víctimas y puede ayudarte a canalizar tu caso a la autoridad correspondiente.

A nivel federal, la Guardia Nacional opera el Centro de Respuesta a Incidentes Cibernéticos.

Puedes reportar delitos cibernéticos federales enviando un mensaje con los detalles del caso al correo electrónico ceac@sspc.gob.mx. Asimismo, está disponible el número 088, también de la Guardia Nacional, que funciona 24/7 a nivel nacional para atender reportes de incidentes de seguridad. Al llamar al 088, puedes informar de un fraude cibernético o extorsión y recibir orientación inmediata (ten en cuenta que el 088 genera un reporte, mas no sustituye la denuncia formal). Considera que de igual manera puedes comunicarte al 089 para denunciar de forma anónima cualquier tipo de delito.

En el ámbito local, varias entidades cuentan con su propia Policía Cibernética. En la Ciudad de México, por ejemplo, la Policía Cibernética de la Secretaría de Seguridad Ciudadana (SSC) atiende reportes vía telefónica (55 5242 5100, ext. 5086) y por medio de su correo electrónico policia.cibernetica@ssc.cdmx.gob.mx. Estos canales te permiten advertir sobre estafas en redes sociales, mensajes sospechosos, suplantación de identidades o cualquier ciberdelito, a fin de que estas instancias investiguen y, en su caso, colaboren con el Ministerio Público.

Otras entidades, como el Estado de México, Jalisco y Nuevo León, tienen unidades cibernéticas similares. Puedes encontrar sus contactos en las páginas oficiales de las secretarías de seguridad estatales.



Involucrar a la **Policía Cibernética** es útil porque pueden conservar pruebas digitales, orientarte sobre medidas de protección, como preservar conversaciones o cerrar cuentas comprometidas, y, en algunos casos, realizar acciones encubiertas en línea para identificar a los delincuentes.

## Otras instancias

Dependiendo del tipo de fraude o conducta, existen otras instancias oficiales donde puedes levantar quejas o alertas:

• **Procuraduría Federal del Consumidor (Profeco):** si la estafa involucra la compra de un producto o servicio (por ejemplo, agencias de viaje fantasmas, ofertas falsas de comercio electrónico o cualquier fraude en relaciones de consumo), puedes acudir a la Profeco para presentar una queja comercial. Esta institución protege a los consumidores frente a empresas establecidas, en otras palabras, si la empresa existe legalmente, la Profeco puede mediar para recuperar tu dinero o sancionar prácticas abusivas. Ponte en contacto mediante el teléfono del consumidor 55 5568 8722, en la Ciudad de México, o al 800 468 8722, lada nacional, así como en sus delegaciones estatales. Si la "empresa" resultó ser ficticia o un delincuente individual, Profeco quizás no logre resarcir el daño, pero tu queja sirve para alertar a otras personas y para que las autoridades acumulen información.



• **Líneas de emergencia y denuncia anónima:** en caso de recibir una amenaza inminente o extorsión en curso, llama al 911 para recibir ayuda inmediata de la policía. En caso de recibir llamadas de extorsión telefónica, cuelga y reporta el número al 089, el número de denuncia anónima donde puedes reportar de forma confidencial delitos como extorsión, narcomenudeo u otros ilícitos. El 089 es una línea gratuita y disponible 24/7 que enlaza a la ciudadanía con autoridades de seguridad, sin requerir datos personales. Tu reporte anónimo será canalizado a la autoridad competente para su investigación. Muchas denuncias de extorsión telefónica se recaban a través del 089 a nivel nacional. Si optas por esta vía, proporciona toda la información que tengas (números telefónicos que te llamaron, horarios, modus operandi, etc.). Cada denuncia al 089 genera un folio de seguimiento oficial que puedes utilizar para aportar datos adicionales después.

• **Otras instancias especializadas:** en ciertos casos particulares, podría ser útil notificar a alguna otra autoridad. Por ejemplo, si el fraude implicó el uso indebido de tus datos personales, puedes informar a la Secretaría Anticorrupción y Buen Gobierno para solicitar asesoría sobre protección de datos. Si sospechas que tu identidad fue robada para contratar créditos, además de denunciar ante el Ministerio Público, considera alertar a las sociedades de crédito (Buró de Crédito y Círculo de Crédito) para que coloquen una alerta en tu historial. Además, algunas dependencias gubernamentales tienen canales de reporte en caso de que los defraudadores se hagan pasar por ellas.

Aprovecha todos los canales oficiales disponibles: no hay problema en denunciar un mismo hecho ante varias instancias, pues cada una tiene un rol distinto y complementario en la protección de la víctima.

**Tip:** Encuentra más información sobre el proceso de denuncia, sus etapas, cómo puedes intervenir en la investigación, cómo reportar irregularidades y otros recursos en **www.denuncia.org**

## *¿Qué necesitas para denunciar?*

Cuando decidas interponer una denuncia o queja, es fundamental preparar un paquete de información y pruebas que respalde tu caso. A continuación, se describen los elementos más importantes que debes reunir antes de acudir a cualquier instancia:

### Documentos, pruebas y capturas de pantalla

Reúne toda la evidencia posible relacionada con el fraude o incidente. Esto incluye documentos físicos y digitales. Si la estafa ocurrió por internet, es importante que conserves los mensajes de chat, correos electrónicos, fotografías, conversaciones de WhatsApp o redes sociales involucradas, con el objetivo de que los presentes como evidencia. En caso de que el fraude se haya perpetrado por la vía telefónica, conserva los registros de llamadas o de mensajes SMS que recibiste.

No borres nada. En su lugar, haz capturas de pantalla (pantallazos) de las conversaciones o páginas web relevantes, y anota las direcciones URL de sitios web sospechosos. Guarda también archivos adjuntos (PDF, imágenes, audios, etc.), o cualquier cosa que el defraudador te haya enviado.




Si recibiste documentos falsos —como supuestos contratos, comprobantes de transferencia o identificaciones de terceros—, imprímelos o guárdalos. Toda esta información digital servirá como prueba.

La Policía Cibernética suele recomendar no seguir interactuando con el estafador una vez que sospeches que estás siendo víctima de un delito, pero sí resguardar la evidencia: tomar foto o video de la pantalla donde se aprecia el perfil fraudulento, el número telefónico o correo del estafador, la oferta engañosa, etc.

Si el delito fue grabado en videollamadas o si tienes videos tomados por cámaras, ya sean de otras personas, de establecimientos comerciales o de la red pública, solicita u obtén copias de esos videos.

Entre más pruebas entregues, más sólido será tu caso. Las capturas de pantalla son aceptadas como indicio. Aunque por sí solas podrían requerir una validación técnica en un juicio, son muy útiles para que las autoridades entiendan lo ocurrido.

Es aconsejable también llevar una narración escrita de los hechos con fechas y detalles, para que no olvides nada al momento de rendir tu declaración, y que la documentación, fotos, videos o cualquier evidencia que hayas recopilado se entregue en dispositivos de almacenamiento como USB. De igual manera, es recomendable que guardes una copia para ti.

**Recuerda:** Aunque no cuentes con todas las pruebas posibles, ninguna autoridad puede negarte el derecho a presentar una denuncia o recibir atención. Si fuiste víctima de un fraude cibernético, tienes derecho a que tu caso sea escuchado y registrado. Reúne la mayor cantidad de información que puedas, pero no esperes a tener toda la información para pedir ayuda. La denuncia es el primer paso para protegerte y activar una posible investigación.

## *Comprobantes de movimientos bancarios o cargos no reconocidos*

Si el problema involucra dinero, es importante llevar tus comprobantes financieros, como estados de cuenta bancarios donde aparezcan los cargos no reconocidos o las transacciones relacionadas con el fraude, recibos de depósito o transferencias que realizaste (si tú enviaste dinero al estafador), comprobantes de retiros en cajeros o movimientos en tus aplicaciones financieras. Marca o resalta en esos documentos las operaciones fraudulentas para identificarlas fácilmente.

Reúne cualquier comunicación con el banco sobre el tema, ya sean correos del banco confirmando que reportaste el cargo tal día o respuestas que te hayan dado. La Condusef señala que, para presentar una reclamación formal, es necesario un documento que compruebe tu relación con la institución financiera afectada (puede ser el contrato de apertura, la carátula o simplemente un estado de cuenta donde se vean tu nombre y número de cuenta). Esto es para demostrar que eres cliente y legitimar tu queja.

Aporta el documento donde se sustenta la queja, por ejemplo, el estado de cuenta con el cargo indebido, la póliza del seguro cobrada indebidamente, el comprobante del cargo doble en tu tarjeta, etc.

Si fuiste víctima de *phishing* (te robaron contraseñas y vaciaron tu cuenta), solicita o descarga el historial de movimientos que muestre las transferencias no autorizadas. En el caso de un fraude con tarjeta, lleva el plástico (si aún lo tienes) y el comprobante o folio de que reportaste el suceso.

En resumen, cualquier papel o registro bancario que evidencie el perjuicio económico debe acompañar tu denuncia. Las autoridades examinarán dichos documentos para determinar responsabilidades y eventualmente calcular el monto a recuperar.






## *Registro de llamadas o números utilizados*

En caso de fraudes que involucren comunicaciones telefónicas (como llamadas de extorsión, *vishing* donde se hicieron pasar por banco, mensajes SMS engañosos, etc.), es necesario documentar la información de éstas. Anota los números de teléfono desde los cuales te llamaron o enviaron mensajes fraudulentos.

Si recibiste múltiples llamadas, lleva un registro de todas, por ejemplo, "llamada del número 55-5555-5555 el día X a las 10:30 a.m., duración de 5 minutos" y un breve resumen de lo que te dijeron. No borres los registros de llamadas de tu celular; haz capturas de pantalla de la lista de llamadas en las que aparezcan el número sospechoso y las fechas.

Si el fraude fue mediante mensajes SMS o WhatsApp, toma capturas de pantalla de la conversación completa, incluyendo el número o perfil del remitente.

En casos de extorsión telefónica, las autoridades recomiendan no confrontar al delincuente, pero sí tratar de grabar la llamada si es posible. En caso de que hayas logrado grabar la llamada de estafa o extorsión, informa a la policía de que cuentas con ese audio y consérvalo en un dispositivo USB para entregarlo.

Anota características de la llamada, como el género y tono de voz de la persona, acento, ruidos de fondo, lo que te pidieron, cualquier dato que te haya parecido extraño. Toda esta información será valiosa para la Policía Cibernética o el Ministerio Público.

En algunos estados, las fiscalías cuentan con bases de datos de números reportados por extorsión, por lo que, al proporcionar este dato, pueden verificar si ya ha sido usado en otros casos.

Si el fraude cibernético involucró comunicaciones por correo electrónico, guarda no sólo las direcciones desde las cuales te escribieron, sino también las **cabeceras completas del mensaje**. Las cabeceras son un bloque de información técnica que no siempre se ve a simple vista y que contienen datos clave como la ruta que siguió el correo, los servidores por los que pasó y la dirección IP de origen.

Para hacerlo, abre el mensaje sospechoso y busca una opción como “ver original”, “mostrar original” o “ver detalles del mensaje”. Esta opción varía según el proveedor de correo:

- En **Gmail**: abre el mensaje, haz clic en los tres puntos (⋮) en la esquina superior derecha del correo y selecciona “mostrar original”.
- En **Outlook**: abre el mensaje, haz clic en los tres puntos (⋮) y luego en “ver origen del mensaje”.
- En **Yahoo Mail**: abre el mensaje, da clic en “más” y selecciona “ver encabezado completo”.

Una vez que se abra la cabecera, copia todo el texto (incluyendo códigos y líneas técnicas) y pégalo en un archivo de texto (como .txt o .docx). Guarda ese archivo con un nombre claro (por ejemplo, “cabecera_correo_fraude.docx”) para poder entregarlo como parte de tu denuncia.

Compartir las cabeceras con la unidad cibernética puede ser muy útil, porque permite rastrear de dónde proviene realmente el mensaje, incluso si los estafadores usaron un nombre falso o suplantaron una dirección.

**Recuerda que cada detalle cuenta.**
Un número telefónico, por ejemplo, podría llevar a identificar una red de fraude si coincide con otros reportes. Por ello, es importante entregar todas estas referencias en tu denuncia.

Presentar un caso bien documentado facilita la investigación y aumenta las probabilidades de recuperar tu dinero o de que las autoridades identifiquen y sancionen a los responsables.



## *Conclusión*

Como hemos visto, hay numerosas modalidades de fraude cibernético, y las técnicas de los delincuentes evolucionan constantemente para confundirnos y atraparnos. Sin embargo, así como hay muchas formas de caer en estos fraudes, también hay múltiples maneras de protegernos. La prevención sigue siendo la mejor defensa.

Adoptar hábitos digitales seguros, mantener dispositivos y sistemas actualizados, y vigilar nuestras interacciones en línea son pasos importantes para protegernos. Además, la educación digital continua permite a cada persona desempeñar un papel activo en su propia seguridad, ya que desarrolla resiliencia y capacidad para anticipar amenazas y responder de manera segura ante posibles engaños.

Aun tomando precauciones, nadie está exento de ser víctima de un fraude cibernético. Por ello, es importante actuar con rapidez y denunciar el delito ante las autoridades. La denuncia no sólo facilita la recuperación de lo perdido y la sanción de los responsables, sino que también contribuye a generar estadísticas más precisas y alertar a otros sobre nuevas modalidades de estafa.

La lucha contra los fraudes cibernéticos constituye una responsabilidad compartida. La ciudadanía puede y debe protegerse, pero el Estado también debe fortalecer los mecanismos de prevención, investigación y sanción. Actualizar la legislación, mejorar la capacidad de las autoridades y reforzar la educación digital son pasos indispensables. Recordemos: el delito que no se denuncia permanece impune.

Facebook - @ImpunidadCeroMx
X - @ImpunidadCeroMx
Instagram - @ImpunidadCeroMx
Tiktok - @ImpunidadCeroMx

www.impunidadcero.org
contacto@impunidadcero.org
www.denuncia.org