Guía para **PREVENIR** el robo de identidad

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

10 consejos útiles
para proteger tu identidad

1

Mantén seguros tus documentos personales en casa y cuando viajes

Todos los documentos personales o archivos electrónicos, así como NIP, password y claves dinámicas deben conservarse en un lugar seguro, para evitar que personas extrañas tengan acceso a ellos. Utiliza un buzón con llave, recoge tu correspondencia lo antes posible y notifica de inmediato a los remitentes cualquier cambio de domicilio.

2

Destruye tus documentos personales cuando hayan dejado de ser necesarios

Al deshacerte de los documentos que contengan información personal o financiera, o tarjetas de crédito o débito vencidas, destrúyelos perfectamente.

3

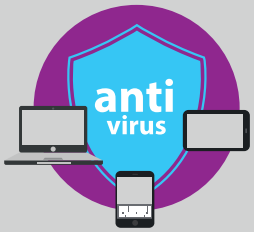
Piensa antes de publicar o compartir información personal

No compartas ni publiques más de lo necesario y configura niveles de privacidad entre tus contactos. Nunca envíes tus claves y NIP por correo electrónico y jamás los compartas con nadie.

4

Protege tu computadora smarthphone y Tablet

Instala software de seguridad (antivirus) y contraseñas seguras, que no se relacionen con datos personales como fechas de nacimiento, números telefónicos o nombres de familiares, y utiliza combinaciones de letras mayúsculas, minúsculas y números.

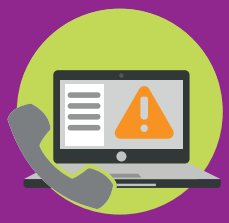


5

Limita el número de documentos personales que traes contigo

Procura traer sólo aquéllos que vayas a utilizar.

6



Ten cuidado cuando te soliciten información en persona, por internet o teléfono

Verifica la identidad de quien te la solicita y requiere información para descartar que se trate de un fraude. Elimina cualquier mensaje sospechoso o que solicite información personal o financiera, es mejor no abrirlos. Nunca ingreses tus contraseñas en algún sitio que te haya llegado por correo electrónico o chat. Ingresa directamente a la dirección oficial de la institución.

7

Investiga si recibes tarjetas de crédito, servicios o artículos que no hayas solicitado

Debes estar también pendiente de la correspondencia que te haga falta.

8

Mantente alerta ante cualquier transacción bancaria inusual

Verifica tus estados de cuenta y consulta tus movimientos, para identificar los que no recuerdes haber realizado, y revisa tu reporte de crédito de manera frecuente.

9

Procura tener siempre a la vista tu tarjeta de crédito o débito

Solicita que lleven a donde estés los medios de cobro

10

Realiza transacciones seguras

No utilices equipos públicos para realizar movimientos bancarios o de compras por internet. Tu información puede quedar grabada en ellos con el uso de un software maligno. Asegúrate que el sitio que visitas para compras en Internet sea totalmente seguro y confiable. El proveedor debe informar su identidad, denominación legal, políticas de venta y privacidad, así como datos de su ubicación física.

Contenido

Objetivo

La presente guía busca proporcionar información relevante con relación al robo de identidad, con la finalidad que las personas cuenten con herramientas para conocer cómo proteger sus datos personales y así poder reducir el riesgo de que su identidad sea robada. De igual forma, se incluyen referencias para conocer qué hacer y ante quién acudir en caso de haber sido víctima de robo de identidad.

¿Qué es el robo de identidad?

Es la apropiación de la identidad de una persona, para hacerse pasar por ella, asumir su identidad frente a terceros públicos o privados, a fin de obtener ciertos recursos o beneficios a su nombre.

El robo de identidad implica la obtención y uso **NO** autorizado e ilegal de **datos personales.**

Los datos personales son cualquier información relativa a la persona, que la identifica o hace identificable. Es la información que nos describe, que nos da identidad, nos caracteriza y diferencia de otros individuos.

¿Cómo puede afectarte el robo de identidad?

Tu identidad es una de las cosas más importantes que posees, por lo tanto, debes saber cómo protegerla.

El robo de identidad tiene consecuencias graves que pueden requerir de tiempo y recursos económicos para resolverse. Por lo general, a las víctimas les lleva mucho tiempo darse cuenta de que su identidad ha sido robada, y una vez que sucede es muy difícil recuperarla y es común tener problemas en el futuro.

El uso de fuentes de fácil acceso y ricas en información, por ejemplo las redes sociales, en las que se puede obtener información sobre una persona, tal como: nombre, edad, fecha de nacimiento, fotografía, información de tipo familiar, escolar, laboral, entre otra, facilita a los delincuentes el robo de identidad.

México se ubica en el 8° lugar en el mundo y en 3er lugar de América Latina por robo de identidad, según firmas especializadas.[1]

1 Fuente: CPP México http://mexico.cppdirect.com/ y Reporte de Fraude de enero de 2014 elaborado por RSA http://mexico.emc.com/emc-plus/rsa-thought-leadership/online-fraud/index.htm

Actualmente, cuando se piensa en robo de identidad, se le asocia con información relacionada a la actividad financiera (números de tarjetas de crédito u operaciones bancarias), pero en realidad, el robo de identidad puede afectar otras esferas de la persona, como su reputación.

A continuación se ejemplifican los tipos de acciones que llevan a cabo quienes roban tu identidad y las consecuencias de las mismas para tu persona:

Como ha sido señalado, las consecuencias del robo de identidad pueden afectarte en distintos aspectos y en ciertos casos de forma permanente, por lo que es importante que conozcas los métodos o técnicas más comunes mediante los cuales los delincuentes se pueden apropiar de tu información personal, y tengas en cuenta los consejos que encontrarás más adelante para disminuir el riesgo de ser víctima de este ilícito.

¿Cómo pueden robar tu identidad?

Los métodos más comunes que se utilizan para el robo de identidad se pueden clasificar en tres tipos:

1) Aquéllos que se realizan de forma tradicional, sin acceso a internet;
2) los que sin acceso a internet se apoyan de alguna herramienta tecnológica; y,
3) finalmente, los que se realizan con acceso a internet.

A continuación se explica cada uno de ellos.[2]

Sin acceso a internet

Para aplicar cualquier técnica ubicada en esta categoría, ni la victima potencial ni el estafador necesitan hacer uso de algún punto de acceso a internet, sólo basta la sagacidad del estafador y el descuido de la víctima. Las técnicas que se han encontrado actualmente son:

Ingeniería social: es una técnica utilizada para obtener información de las personas teniendo como base la interacción social, la manipulación y el engaño, y ocurre típicamente en conversaciones directas entre el delincuente y la víctima. El estafador consigue que su víctima no se dé cuenta cómo ni cuándo dio todos los datos necesarios para el robo de su identidad. En esta práctica se recurre a la manipulación de la psicología humana mediante el engaño. El delincuente actúa a partir de la premisa de que en la cadena de seguridad de la información, el ser humano es el eslabón más débil: la propia víctima es la que otorga su información, algunas formas de ataque que incluyen ingeniería social son:

Pretexting: es una variación de la ingeniería social, con la diferencia de que para realizarla, el atacante debe tener un estudio previo de la información de la víctima potencial, para así, crear y utilizar un escenario favorable con el objetivo de persuadir a una víctima y obtener información. El atacante puede acoplarse a una víctima específica de manera que aumenta la posibilidad de conseguir información o que la víctima realice acciones específicas a su voluntad.

Extorsión telefónica: es una variación de la ingeniería social, en la cual, el atacante realiza una llamada telefónica a la víctima haciéndose pasar por alguien más, por ejemplo, un técnico de soporte o un empleado de alguna organización con el

2 Para la elaboración de las descripciones de los tipos de robo de identidad se tomaron como referencias los siguientes documentos: qué debe saber para evitar el robo de identidad, disponible en http://promos.mcafee.com/es-MX/PDF/mx_id_theft_e_guide.pdf y Corrompiendo la mente humana, de la revista de la UNAM Seguridad Cultura de Prevención para TI. Para la elaboración de las descripciones de los tipos de robo de identidad se tomó como referencia el siguiente documento: http://promos.mcafee.com/es-MX/PDF/mx_id_theft_e_guide.pdf

objetivo de obtener datos de la víctima, de un modo muy efectivo, lo único que se requiere es un teléfono.

Observación: la observación es una técnica muy antigua que se centra en poner atención a las acciones que realiza la víctima y que son de interés para el atacante. El atacante debe guardar discreción para no ser descubierto, por esta razón, se auxilia utilizando herramientas destinadas al espionaje (por ejemplo binoculares, aparatos para escuchar a distancia, entre otros). El objetivo de esta técnica es obtener información preliminar para cometer ataques.

***Shoulder surfing* o espionaje por encima del hombro**: es una técnica derivada de la observación, la particularidad que tiene es que el espionaje a los usuarios se realiza de cerca, para obtener información confidencial. Sólo basta con permanecer observando sigilosamente por la espalda de la víctima las teclas que digita, el monitor o cualquier otro soporte de información que pueda ser de interés para obtener información. Esta técnica se utiliza comúnmente para obtener contraseñas, números PIN, códigos de seguridad y datos similares.

***Eavesdropping* o parar la oreja:** esta técnica trata de explotar el sentido del oído para capturar información privilegiada cuando se está cerca de conversaciones privadas. Por ejemplo, cuando un administrador de sistemas le comenta a un ejecutivo cuál es la clave que puso en una aplicación crítica.

Dumpster diving: es una técnica que se centra en buscar información valiosa en la basura. Tirar cualquier tipo de documentos sin un debido proceso de destrucción es una práctica que puede resultar riesgosa, pues se pueden rescatar de la basura datos importantes contenidos en documentos desechados sin ser destruidos previamente.

Asalto al buzón de correo: es un delito centrado en el robo de la correspondencia que se encuentra en los buzones de correo sin seguro, de los cuales se pueden sustraer documentos con información valiosa (estados de cuenta bancarios o de tarjetas de crédito, o cualquier otro documento).

Sin acceso a internet y con apoyo de alguna herramienta tecnológica

En esta categoría, se recopilan las técnicas que no requieren tener acceso a un punto de conexión de internet, pero que se refuerzan con la ayuda de algún dispositivo electrónico. Dentro de estas técnicas se pueden encontrar:

***Skimming* o clonación de tarjetas (crédito o débito):** esta técnica consiste en realizar una copia de una tarjeta sin el consentimiento del dueño. Los estafadores utilizan diferentes tipos de dispositivos electrónicos (clonadoras) programados para guardar los datos

contenidos en la cinta magnética (número de tarjeta, fecha de vencimiento, código valor de verificación, banco, nombre del titular), para posteriormente reproducir o clonar la tarjeta en un plástico diferente. Este método sólo puede ser utilizado en el momento en que la víctima realiza una transacción con su tarjeta.

Vishing: es una práctica criminal fraudulenta realizada por teléfono, en la cual a través de ingeniería social se pretende obtener información. El término vishing es una combinación de las palabras voice (voz) y phishing (método de suplantación de identidad). En un intento de vishing, el estafador llama pretendiendo ser miembro de algún corporativo y para informar sobre actividad sospechosa reportada en las cuentas de la víctima. Basándose en esta mentira, envuelve a la víctima para que ésta "verifique" información por teléfono.

SMiShing: consiste en una variante fraudulenta del phishing, donde a través de técnicas de ingeniería social se realizan envíos selectivos de mensajes SMS dirigidos a usuarios de telefonía móvil con el fin de que visiten una página web fraudulenta. Mediante reclamos atractivos con alertas urgentes, ofertas interesantes o suculentos premios, tratan de engañar al usuario aprovechando las funcionalidades de navegación web que incorporan los dispositivos móviles actuales.

Con acceso a internet

Para explotar cualquier tipo de técnica descrita a continuación, lo único que se necesita es que el usuario haga uso de alguna aplicación en internet o acceda a un correo electrónico.

Spam: se puede considerar como spam a cualquier mensaje de correo electrónico enviado a varios destinatarios que no solicitaron tal mensaje, también llamado correo electrónico basura; un mensaje de spam debe cumplir con varios aspectos: ser enviado de forma masiva, ser un mensaje no solicitado por el usuario y tener contenido engañoso (habitualmente de tipo publicitario).

Una vez que el usuario accede al contenido engañoso provisto por el spam, se pueden presentar dos escenarios, el primero, cuando el usuario es direccionado a una página web controlada por el atacante en donde mediante el llenado de formularios proveerá información personal que posteriormente se utilizará para cometer un fraude; el segundo escenario se presenta cuando el usuario descarga el contenido adjunto al spam, lo que se traduce en una invasión a su equipo de cómputo mediante un virus que roba la información del dispositivo.

SPim: es un caso específico de spam a través del cual se envían mensajes instantáneos cuyo contenido puede incluir spyware, registradores de pulsaciones, virus, vínculos a sitios de phishing o invitaciones para suscribirse a servicios o promociones falsas mediante el

envío de mensajes instantáneos a un servidor controlado por el atacante, cuyo objetivo es tomar el control de la lista de contactos para suplantar la identidad del afectado.

Registradores de pulsaciones: un registrador de pulsaciones es una forma de software espía que guarda las letras que fueron pulsadas en un documento de texto. Cuando un usuario que tiene este software instalado está navegando en la web, visitando sitios de comercio electrónico o banca electrónica, el registrador de pulsaciones puede registrar los caracteres digitados. Este software es una combinación cuidadosamente elaborada en formato HTML, en la que entre las hojas de estilo, capas, cuadros de texto y objetos de contenido, un usuario al estar escribiendo, lo hace en un marco invisible controlado por un atacante.

Phishing o suplantación de identidad: es una estafa en línea, a través de la utilización de spam, sitios web falsos, mensajes de correo electrónico, mensajes instantáneos, cuya finalidad es obtener de los usuarios de internet información confidencial, tales como contraseñas o información detallada sobre tarjetas de crédito u otra información bancaria. El término proviene de la palabra fishing (pesca) y hace alusión a pescar usuarios para obtener información financiera y sus contraseñas. Los autores del fraude, conocidos como "phishers" simulan ser empresas legítimas, y pueden utilizar el correo electrónico para solicitar información personal e inducir a los destinatarios a responder a través de sitios web maliciosos.

Los "phishers" suelen utilizar tácticas alarmistas o solicitudes urgentes para tentar a los destinatarios a responder. Los sitios de robo de identidad parecen sitios legítimos, ya que tienden a utilizar las imágenes de Copyright de los sitios legítimos; sin embargo, no incluyen el protocolo seguro de transferencia de hipertexto (identificado en las direcciones electrónicas como el https://). Los mensajes fraudulentos generalmente no están personalizados y es posible que compartan propiedades similares, como detalles en el encabezado y en el pie de página.

Pharming: es una vulneración que tiene la finalidad de redirigir a un usuario de internet que navega en páginas web a una página falsa diseñada para robarle información personal. A diferencia del phishing, el pharming está programado para atacar al equipo de la probable víctima; hace que la navegación web se redireccione a servidores plagados de sitios controlados que tienen un aspecto similar al que el usuario trata de ingresar, es decir, cuando la víctima introduce una dirección electrónica correcta, ésta es enrutada o redireccionada hacia el servidor del atacante. En pocas palabras, el pharming es una granja de víctimas.

¿Cómo proteger tu identidad?

La protección de tus datos personales es una herramienta en contra del robo de identidad, a continuación se presenta una serie de consejos que pueden ser útiles para evitar el robo de tu identidad.

Sin conexión a internet (offline)

Para documentos de identificación

- Limita el número de documentos con información personal que traes contigo, procura traer sólo aquéllos que vayas a utilizar.
- Ten copias de tus documentos importantes y mantenlos en un lugar seguro, podrán ser útiles en caso de que extravíes los originales.
- Mantén seguros tus documentos personales en tu casa y cuando viajes. En caso de ya no ser necesarios destrúyelos.
- Antes de tirar la basura revisa que no contenga documentos con información personal, en caso de que así sea, destrúyelos por completo y verifica que no sea posible extraer información personal por parte de terceros.

Para información financiera

- Al acudir a un cajero automático llévate contigo los comprobantes de la operación, no los dejes en los botes de basura que se encuentran ahí.
- Revisa que el cajero automático no cuente con dispositivos extraños en el lector de tarjetas, de ser el caso, utiliza otro cajero automático.
- Cuando teclees tu NIP en el cajero electrónico, o cuando llenes algún tipo de formulario con información personal debes tener cuidado con las personas que se encuentran a tu alrededor.
- Evita proporcionar información personal o financiera por teléfono.
- Al pagar con tarjeta, no la pierdas de vista, solicita que te lleven la terminal al lugar donde te encuentres, por ejemplo, en restaurantes o gasolineras.
- Revisa constantemente tus estados de cuenta con la finalidad de que te cerciores que los cargos correspondan efectivamente a los que hayas realizado. Si detectas un error realiza la aclaración correspondiente lo antes posible.
- Si recibes una llamada telefónica en donde te solicitan teclear tus datos personales cuelga, las instituciones bancarias no solicitan información a través de este medio.
- Revisa constantemente tu reporte de crédito, a fin de detectar movimientos sospechosos.
- Suscríbete al servicio de ahorro de papel que ofrecen algunas instituciones financieras y compañías de servicios, para sustituir el envío en papel de tus estados de cuenta a tu domicilio, por el envío de éstos a tu correo electrónico, disminuyendo con esto la circulación de tu información personal.

Para otros servicios

- Protege tu correspondencia utilizando un buzón con llave y recogiéndola lo más pronto posible. Notifica de inmediato cualquier cambio de domicilio a los remitentes de la misma.
- Protege tus contraseñas, no las escribas o coloques en tu celular o en algún otro lugar que sea susceptible de ser visto por terceros.
- Si acudes a alguna institución o negocio para solicitar la cancelación de un servicio que no solicitaste, recuerda que podrás ejercer tus derechos de acceso, rectificación, cancelación y oposición, que prevén el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, las leyes de las entidades federativas en materia de transparencia o protección de datos personales, y demás normatividad en la materia.
- Haz caso omiso de los mensajes en los que te comunican que has ganado un premio o te hacen una oferta especial, al menos que tengas seguridad plena de la autenticidad de los mensajes.
- Antes de que proporciones información personal, solicita el aviso de privacidad o leyenda de información, para que puedas conocer quién utilizará tus datos personales, para qué fines, con quién se compartirán en su caso, cómo podrás ejercer tus derechos, entre otras características del tratamiento al que serán sometidos tus datos personales.
- No dejes documentos personales en tu auto cuando uses el servicio de valet parking.
- Cuando te soliciten tus huellas dactilares, asegúrate de limpiar la superficie del equipo electrónico en el que las hayas puesto, a fin de que no quede su imagen expuesta y pueda ser retomada de manera indebida. Una técnica común y sencilla de "robar" huellas dactilares es pasar una cinta adhesiva encima del equipo electrónico donde la persona proporcionó su huella, para copiar la imagen.

Con conexión a Internet (online)

Para proteger tus cuentas y dispositivos electrónicos

- Evita usar computadoras públicas para acceder a tu información personal, de ser necesario, recuerda limpiar el historial al terminar tu navegación. Si utilizas equipos públicos para acceder a internet, evita realizar operaciones en la banca en línea.
- Si requieres abrir una cuenta personal en una computadora de acceso público, asegúrate de cerrarla correctamente al concluir el uso del equipo.
- Si en el navegador aparece una ventana emergente que te recomienda recordar tus contraseñas, indica siempre la opción "NO".
- Al terminar de usar el navegador, borra los datos del navegador: el historial de descargas y navegación, los datos de formularios almacenados, cookies, contraseñas y licencias de contenido. El borrado lo puedes hacer accediendo a la configuración

del navegador y seleccionando la opción "Borrar datos de navegación".

- Asegúrate de cambiar tus contraseñas y claves de acceso con regularidad. De igual forma, construye una contraseña segura,[3] recuerda que se deben cumplir con una serie de requisitos, por ejemplo, tener una longitud mayor a seis caracteres e incluir letras mayúsculas y minúsculas, números, símbolos y distintos caracteres.
- Protege tu computadora, teléfono inteligente o Tablet con un software de seguridad (antivirus) y contraseñas seguras.
- Utiliza contraseñas para tus dispositivos móviles y computadora y no las compartas con terceros.
- No permitas el acceso remoto a tu computadora.
- Protege la información personal de tu dispositivo, no te conectes a redes inalámbricas que no tengan contraseñas.
- Descarga aplicaciones de tiendas oficiales y de desarrolladores confiables.
- Evita almacenar cantidades excesivas de datos personales sin cifrar en un dispositivo móvil, tales como nombres de usuario, palabras clave, información crediticia o de identificación personal, para evitar que tus datos sean interceptados si el dispositivo es extraviado.
- Antes de que dejes de utilizar, vendas o deseches tus dispositivos electrónicos, asegúrate de borrar tu información personal y restaurar la configuración de fábrica.

En redes sociales

- Utiliza distintas contraseñas y nombres de usuario para diferentes sitios.
- Antes de crear una cuenta en alguna red social asegúrate de haber leído sus políticas de privacidad.
- Configura la privacidad de tus redes sociales, no aceptes cualquier solicitud de amistad a menos que te encuentres seguro de conocer de forma personal a quien te la envía.
- Piensa antes de publicar información personal.
- No compartas más información de la necesaria en redes sociales, de igual forma configura niveles de privacidad entre tus contactos.

Al navegar en internet

- Evita intercambiar información personal o contraseñas en sitios no seguros.
- Ten cuidado de las ofertas que se publican en internet que son demasiado buenas para ser reales.
- No des click en links o vínculos que descarguen archivos y cierra las ventanas emergentes que puedan abrirse al navegar.
- No abras archivos adjuntos de un correo electrónico que provengan de un remitente desconocido.

3 Si requiere conocer más información sobre contraseñas seguras, consulte la siguiente página: https://www.microsoft.com/es-es/security/online-privacy/passwords-create.aspx

- Sé cuidadoso de la información que compartes en línea, verifica que tu información personal sea utilizada para propósitos legítimos.
- Instala en tu computadora paquetes de seguridad que te protejan contra amenazas tecnológicas y mantenlos actualizados.
- No proporciones información personal por correo electrónico ni por internet, a menos que tengas certeza que el sitio sea legítimo.
- Revisa las políticas de privacidad de los sitios que visitas para conocer el uso que se le dará a la información que proporciones.

Al hacer uso de datos financieros

- Siempre que se ingrese al portal de un banco o realices alguna compra en línea en donde te sean solicitados datos de tus tarjetas, verifica que la dirección que aparece en la barra del explorador empiece con HTTPS, ya que la "S" significa que se trata de una página segura.
- No respondas a correos electrónicos o mensajes emergentes en los que te soliciten información personal o financiera, ni hagas click en los hipervínculos.
- Haz caso omiso de los correos en los que te soliciten actualizar tus datos bancarios.
- En caso de recibir una notificación por correo electrónico en la que te informen que tu cuenta fue bloqueada reporta esta situación al banco mediante la línea de atención telefónica, y no a través de los teléfonos que en dicha notificación hayas recibido.
- Nunca reveles el número de tu tarjeta de crédito o el código de seguridad de la misma como respuesta a un mensaje que sospeches que es spam.
- Revisa los estados de cuenta bancarios regularmente para asegurar que no hay cargos extraños en la cuenta.

¿Cómo saber si he sido víctima de robo de identidad?

Por lo general, no te das cuenta que tu identidad ha sido robada hasta que pasa algo que te permite suponerlo, por lo tanto, deberás estar atento a las señales de alarma, tales como:

- Llamadas de despachos de cobranza con respecto a deudas que no hayas adquirido.
- Si recibes tarjetas de crédito que no hayas solicitado.
- Si te niegan solicitudes de crédito de forma inesperada.
- Si no recibes correspondencia que esperabas o se reduce la cantidad de esta.
- Si observas cargos o retiros en tu crédito o tarjeta de débito que no hayas realizado.
- Tus tarjetas son denegadas.
- Encuentras en tu reporte de crédito cuentas o cargos no reconocidos.
- Recibes la notificación de vulneración de una empresa que tiene en posesión tus datos personales.

¿Qué debo hacer si mi información se perdió o quedó expuesta?

Dependiendo del tipo de información que se perdió o quedó expuesta existen acciones que te pueden ayudar a protegerte contra el robo de identidad, como a continuación se explica:

Tipo de información o documento	Recomendaciones
Nombre de usuario o contraseña	• Inicia sesión en esa cuenta y cambia tu contraseña. De ser posible cambia también tu nombre de usuario. • De igual forma cambia las contraseñas que sean iguales a la que fue vulnerada. • Si la contraseña pertenece a un sitio de banca en línea revisa tus cuentas para ver si encuentras cargos que no reconozcas.
Tarjeta de débito o crédito	• Ponte en contacto con el banco o con la compañía de crédito para cancelar tu tarjeta y solicitar una nueva. • Si tienes pagos domiciliados comunícate con las compañías para actualizar el nuevo número de cuenta.
Información de cuenta bancaria	• Comunícate con tu banco para cerrar la cuenta y abrir una nueva. • Consulta tu estado de cuenta para validar que las transacciones realizadas sean las correctas. • Procura tener contacto con el ejecutivo de las sucursales bancarias o entidades financieras de manera regular, donde se tengan contratados productos de crédito, para que te ubiquen como cliente, y ante cualquier eventualidad o problema, la atención sea expedita.
Credencial de elector	En caso de robo o pérdida de la credencial para votar, podrás consultar qué puedes hacer para obtener su reposición a través de la página del Instituto Nacional Electoral (INE): http://www2.ine.mx/archivos2/portal/credencial/pdf-credencial/TramitesMAC2014.pdf

Tipo de información o documento	Recomendaciones
Pasaporte	En caso de robo, pérdida o destrucción del pasaporte, la Secretaría de Relaciones Exteriores (SRE) recomienda cumplir con lo siguiente: **a)** Cuando el hecho ocurra en el territorio nacional, se deberá levantar un acta ante el Ministerio Público o autoridad competente y entregarla en original a la SRE, comunicándole a la vez y bajo protesta de decir verdad, el hecho y las circunstancias en que ocurrió, a través del formato que será proporcionado de manera gratuita. **b)** Si el hecho ocurrió en el extranjero, se deberá entregar el acta levantada ante la Oficina Consular o autoridad competente del país de que se trate. La SRE podrá requerir que el acta esté legalizada o apostillada y traducida al español. Para mayor información consulta: http://sre.gob.mx/renovacion?id=281
Visa americana	Este acontecimiento debe reportarse a la embajada o consulado en el que se tramitó originalmente la visa. Si su visa ha sido extraviada o robada deberá obtener un reporte policial de las autoridades locales, enviar un correo a **mexcityvisastolen@state.gov** y agendar una cita para la reposición. Para obtener más información consulte: http://spanish.mexico.usembassy.gov/es/visas/pasaportes/visas-perdidos-o-robados.html

Tipo de información o documento	Recomendaciones
Teléfono celular	• En caso de robo o pérdida del teléfono celular, deberás de reportarlo directamente a la compañía telefónica para inhabilitarlo, dando la clave conocida como Código Internacional de Identidad del Equipo Móvil (IMEI, por sus siglas en inglés). Para conocer esta clave, debes pulsar *#06# en tu celular y pulsar el botón de llamar. Para obtener más información consulte: http://www.ift.org.mx/multimedia/como-obtengo-el-imei-de-mi-celular • En caso de que el teléfono sea un dispositivo inteligente, existen aplicaciones para rastrear, bloquear y borrar, dependiendo del sistema operativo del dispositivo, será la aplicación que cumpla con estos propósitos. Para **Sistema Operativo Android**, existe una función que se llama *Administrador de dispositivos Android* que tiene que ser habilitada siguiendo las instrucciones que da el proveedor. Para obtener más información consulte: https://support.google.com/accounts/answer/3265955?hl=es Para **Sistema Operativo iOS**, existe una aplicación ligada a la configuración de la cuenta del dispositivo, esta aplicación se llama *Buscar mi iPhone* y para poder activarla deberás seguir las indicaciones del proveedor. Para obtener más información consulte: https://www.apple.com/mx/icloud/find-my-iphone.html

¿Qué debo hacer si he sido víctima de robo de identidad?

Recuerda que entre más rápido actúes podrás minimizar el daño. Es importante que tomes en cuenta el siguiente plan de acción para enfrentar el robo de identidad:

Si sospechas que has sido víctima del robo de identidad actuar rápido es la mejor forma de limitar el daño

ACCIÓN 1 Presentar denuncia ante las autoridades penales correspondientes.

ACCIÓN 2 Reportar la pérdida de los documentos a quien corresponda.

ACCIÓN 3 Contactar y reportar a la institución financiera de las afectaciones en tus cuentas o de cuentas que hayan sido aperturadas a tu nombre sin tu consentimiento. De igual forma recuerda que podrás acudir a la **Condusef** para presentar una queja en caso de que tengas algún inconveniente en el trámite con la institución financiera que corresponda.

ACCIÓN 4 Cancelar cuentas o servicios no autorizados que se hayan contratado a tu nombre. Si tienes problemas con relación a la cancelación de los servicios que hayan sido contratados podrás acudir a la **Profeco**.

ACCIÓN 5 Solicitar una copia de tu reporte de crédito, el cual puedes solicitar de forma gratuita una vez al año al Buró de Crédito http://www.burodecredito.com.mx/ o al teléfono 01 800 640 7920. También lo puedes solicitar a la Condusef, de manera gratuita, para mayor información en http://www.condusef.gob.mx/ y a los teléfonos (55)5340 0999 y (01 800) 999 80 80 .

ACCIÓN 6 Reportar a las redes sociales sobre las vulneraciones que hayan sido identificadas en tus cuentas.

ACCIÓN 7 Contactar al **INAI** por el mal uso de tus datos personales. El INAI no investiga de manera directa el robo de identidad, pues la persecusión de este delito corresponde a las autoridades penales. Sin embargo, el INAI puede investigar el indebido tratamiento de datos personales vinculado con el robo de identidad, como por ejemplo la falta de medidas de seguridad.

¿A quién puedo acudir?

A continuación se hace referencia a las dependencias o instituciones ante las cuales puedes acudir en caso de ser víctima de robo de identidad.

Denuncia ante la Procuraduría que corresponda a tu localidad

Denuncia en la procuraduría de justicia que corresponda a tu localidad si fuiste víctima del delito de robo de identidad, con independencia de que en tu entidad federativa no se reconozca penalmente el delito de robo de identidad, pues puede haber figuras similares a través de las cuales se pueda abordar tu denuncia, como fraude, uso indebido de la información, usurpación de identidad, robo, entre otros.

Cuando acudas a denunciar, lleva contigo una identificación oficial y la información que te sirva como prueba del ilícito cometido en tu contra, por ejemplo, la tarjeta de crédito que no solicitaste, correos electrónicos, estados de cuenta, o cualquier otro documento que consideres de utilidad para acreditar tu dicho, ya que la autoridad te solicitará que realices una relatoría o narración de los hechos que denuncias. Asimismo, el Ministerio Público podrá solicitarte información adicional a la antes descrita, como por ejemplo un domicilio, no obstante, la solicitud de información por parte de la autoridad debe ser acorde con el objeto de la denuncia y deberá estar debidamente justificada.

Actualmente no se prevé el delito de robo de identidad en el Código Penal Federal, sin embargo, se encuentra regulado en las siguientes entidades federativas:

BAJA CALIFORNIA
Procuraduría General de Justicia del Estado de Baja California http://www.pgjebc.gob.mx/

COLIMA
Procuraduría General de Justicia del Estado de Colima http://www.pgj.col.gob.mx/2013/index.php#
Denuncia en Línea: http://www.pgj.col.gob.mx/denuncia/denuncia_index.php

Citas al Ministerio Público: realiza tu cita con el Ministerio Público desde la comodidad de tu casa al teléfono 01-800-50-68-360.

Correo electrónico: citas@pgje.gob.mx

DISTRITO FEDERAL
Procuraduría General de Justicia del Distrito Federal http://www.pgjdf.gob.mx/

MP Virtual: https://mpvirtual.pgjdf.gob.mx/CiberDenuncia/Bienvenida.aspx

Teléfono de atención ciudadana: 52 00 90 00.

Llama sin costo al 01.800.00.PGJDF (74533).

DURANGO
Fiscalía General del Estado http://www.fiscaliadurango.gob.mx/index.php

Denuncia las 24 horas, los 365 días del año, a los teléfonos (618)137-35-00 2. (618)137-35-76.

ESTADO DE MÉXICO
Procuraduría General de Justicia del Estado de México www.edomex.gob.mx/pgjem

QUINTANA ROO
Procuraduría General de Justicia del Estado http://pgje.qroo.gob.mx/portal/

TAMAULIPAS
Procuraduría General de Justicia http://procuraduria.tamaulipas.gob.mx/

TLAXCALA
Procuraduría General de Justicia del Estado http://pgjtlaxcala.gob.mx/
Correo electrónico: procuraduria@pgjtlaxcala.gob.mx

Agencias del Ministerio Público: http://sistemas.tlaxcala.gob.mx/tramites/tar/pdf_tramite.php?recno=412

ZACATECAS
Procuraduría General de Justicia del Estado de Zacatecas http://pgje.zacatecas.gob.mx/sitio/

Denuncia por Internet: http://sistemapgj.zacatecas.gob.mx/denuncia_internet/

Ten en cuenta que presentar tu denuncia es sólo una de las acciones que puedes realizar ante el robo de tu identidad, a la par existen otras medidas que puedes tomar, como las señaladas en los apartados 7 y 8 de esta guía.

Acude a...

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef)

Cuando el robo de identidad recaiga sobre información financiera relacionada con cuentas bancarias, tarjetas de débito o crédito, créditos otorgados a tu nombre, cargos no

reconocidos en tus cuentas, y si habiendo acudido a la institución financiera correspondiente, no has recibido una respuesta o la misma no es satisfactoria, podrás acudir a la Condusef, para presentar una queja. Los datos de contacto para hacerlo son: Tel. (55)5340 0999 y (01 800) 999 80 80.

Domicilio: Av. Insurgentes Sur #762 Col. Del Valle México D.F. C.P 03100.

Página de internet: http://www.condusef.gob.mx/

De manera adicional podrás consultar los siguientes materiales que sobre el robo de identidad la Condusef ha puesto a disposición del público:

- Artículo con consejos para proteger tu identidad financiera http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos/307-protege-tu-identidad
- Conduguía: Protege tu identidad http://www.condusef.gob.mx/PDF-s/educacion_financiera/conduguias/conduguia-protege-tu-identidad.pdf

Procuraduría Federal del Consumidor (Profeco)

En caso de que la información obtenida a través del robo de identidad se haya utilizado para la contratación de un servicio a tu nombre, lo cual tenga como resultado que las compañías prestadoras del servicio te requieran del pago de los mismos, como por ejemplo, si contratan una línea de telefonía celular o tarjetas de crédito de tiendas departamentales a tu nombre, podrás acudir a la Profeco o comunicarse a los números telefónicos 5568 8722 en el D.F. o al 01800 468 8722 del interior de la República.

Domicilio: Av. José Vasconcelos 208, Col. Condesa CP 06140, Del. Cuauhtémoc, Distrito Federal.

Página de internet: http://www.profeco.gob.mx

Ahora bien, para evitar el spam telefónico, puedes inscribirte al Registro Público para Evitar Publicidad (REPEP), el cual es un mecanismo de protección al consumidor operado por la Profeco. Para mayor información puedes consultar el siguiente vínculo electrónico: http://rpc.profeco.gob.mx/rpc.jsp

De manera adicional, podrás consultar los siguientes materiales que sobre el robo de identidad la Profeco ha puesto a disposición del público:

- Webcast acerca del Robo de Identidad http://revistadelconsumidor.gob.mx/?tag=robo-de-identidad
- Phishing: Robo de identidad http://revistadelconsumidor.gob.mx/?p=188

Procuraduría de la Defensa del Contribuyente (PRODECON)

En caso de que la información obtenida a través del robo de identidad se haya utilizado para suplantar tu identidad con el objetivo de presentar declaraciones ficticias y reportar saldos a favor del Impuesto Sobre la Renta (ISR) y depósitos a cuentas bancarias de terceros ante el Sistema de Administración Tributaria (SAT), podrás acudir a la PRODECON o comunicarte al siguiente número telefónico para recibir asesoría: (55)12 05 90 00 y 01 800 611 0190.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)

El INAI es la autoridad garante del derecho a la protección de datos personales, por lo tanto, podrás acudir ante esta autoridad cuando tengas conocimiento de un tratamiento indebido de los datos personales, y hacer uso de los procedimientos señalados en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, cuando resulten procedentes.

Es importante reiterar que el INAI no está facultado para investigar de manera directa el robo de identidad, pues la persecución de este delito corresponde a la autoridad penal. No obstante, el Instituto puede investigar el indebido tratamiento de datos personales vinculados con el robo de identidad, como por ejemplo, la falta de medidas de seguridad para la protección de los datos personales.

Los procedimientos que sustancia el Instituto, vinculados con la protección de los datos personales son:

- **Procedimiento de protección de derechos:** mediante este procedimiento se podrá presentar una solicitud de protección de derechos ante el INAI, a fin de que el Instituto resuelva si procede o no la respuesta que les fue otorgada a los titulares, por parte de los responsables del tratamiento, ante una solicitud de ejercicio de derechos de acceso, rectificación, cancelación y oposición, o requiera al responsable que atienda dicha solicitud. Se inicia a instancia del titular de los datos o de su representante legal, expresando con claridad el contenido de su reclamación.

- **Procedimiento de verificación:** tiene como objeto denunciar ante el INAI cualquier tratamiento indebido de datos personales, o hechos que se considere sean presuntas violaciones o incumplimientos de las obligaciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y demás ordenamientos aplicables, así como la falta de atención a una solicitud de revocación del consentimiento. El procedimiento de verificación podrá iniciarse de oficio o a petición de parte, la verificación de oficio

procederá cuando se dé el incumplimiento a resoluciones dictadas con motivo de procedimientos de protección de derechos o se presuma fundada y motivadamente la existencia de violaciones a la ley.

- **Recurso de revisión:** podrás presentar ante el INAI un recurso de revisión cuando una dependencia o entidad de la Administración Pública Federal no haya atendido debidamente una solicitud del ejercicio de tus derechos de acceso, rectificación, corrección, cancelación u oposición de tus datos personales.

Si requieres mayor información o asesoría sobre los procedimientos del INAI o el derecho de protección de datos personales en general, ponemos a tu disposición los siguientes canales de comunicación:

Vía telefónica: Si deseas asesoría vía telefónica relacionada con cualquiera de los temas mencionados, te invitamos a comunicarte con nosotros al 01-800-835 4324. Te recordamos que tu llamada es gratuita desde cualquier estado de la República con un horario de atención de lunes a jueves de 9:00 a 18:00 horas, y los viernes de 9:00 a 15:00 horas.

Vía postal: Puedes escribirnos directamente al Centro de Atención a la Sociedad (CAS) a la siguiente dirección: Insurgentes Sur No. 3211, Col. Insurgentes Cuicuilco, Delegación Coyoacán, C.P. 04530, México, Distrito Federal.

Vía correo electrónico: Ponemos a tu disposición la siguiente dirección electrónica: atencion@inai.org.mx

Asesoría personalizada: Te invitamos a visitar personalmente el Centro de Atención a la Sociedad (CAS) en la siguiente dirección: Insurgentes Sur No. 3211 Col. Insurgentes Cuicuilco, Delegación Coyoacán, C.P. 04530, México, Distrito Federal, con un horario de atención de lunes a viernes de 9:00 a 18:00 horas.

Página de Internet: Puedes visitar nuestra página de Internet www.inai.org.mx

Checklist de vulnerabilidad

¿Qué tan vulnerable eres ante el robo de identidad?

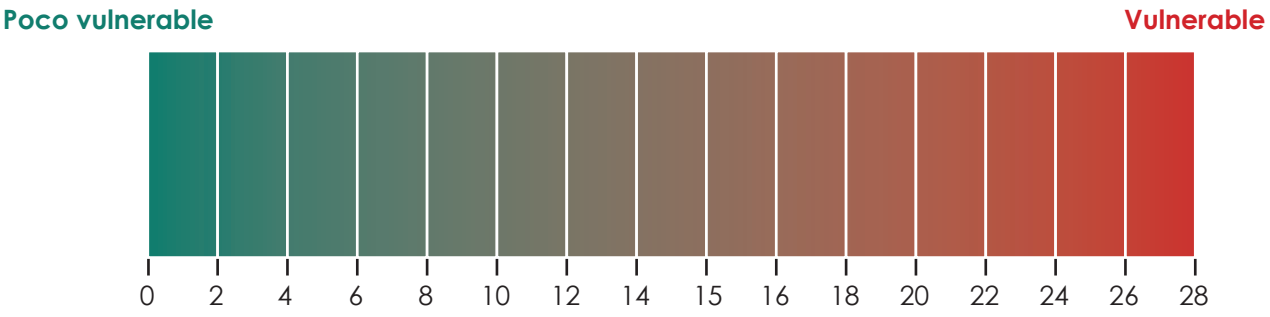
Seguridad en tus datos personales	Si / No
1. Cuando pagas con tarjeta ¿la terminal se encuentra lejos de ti?	
2. ¿Dejas expuestos tus documentos personales que te llegan por correspondencia?	
3. ¿Dejas sin protección o candados tu buzón de correspondencia?	
4. En caso de usar servicio de valet parking ¿dejas papeles personales en la guantera del automóvil?	
5. ¿Tiras a la basura documentos que contienen información personal o datos sensibles, sin destruirlos previamente?	
6. ¿Llevas más de un año sin revisar tu historial crediticio?	
7. ¿Tienes desactualizada tu dirección personal a la cual te llegan tus recibos bancarios o de servicios?	

Seguridad en tu computadora	Si / No
8. ¿Olvidas cambiar periódicamente tus contraseñas?	
9. ¿Mantienes información personal en tu computadora sin medidas de seguridad para su acceso?	
10. ¿El software de protección antivirus está desactualizado?	
11. ¿Has dejado pasar más de 15 días sin ejecutar algún rastreo en tu equipo en busca de virus?	
12. ¿Mantienes desactivado el firewall?	
13. ¿Utilizas una conexión inalámbrica sin protección de una contraseña para acceder a internet?	
14. ¿Utilizas computadoras de café internet o públicas?	

Seguridad en tus redes sociales	Si / No
15. ¿Publicas información personal sensible o que te comprometa en redes sociales?	
16. ¿Tienes la misma contraseña en tus redes sociales y correos electrónicos personales?	
17. ¿Tienes vinculada tu cuenta de redes sociales a aplicaciones como juegos o extensiones que soliciten ligar tu cuenta de red social?	
18. ¿No tienes configurada la privacidad en tus redes sociales?	
19. ¿Te has registrado a alguna página utilizando tus datos de acceso a una red social?	
20. ¿No tienes configurada la seguridad para agregar solicitudes para incluir en tus círculos sociales a nuevas personas y para controlar quién puede ver tus publicaciones?	
21. ¿Haz publicado fotos de documentos personales?	

Seguridad en tus dispositivos móviles	Si / No
22. ¿Mantienes encendido tu ***wi-fi*** o ***bluetooth*** aunque no los estés utilizando?	
23. ¿Tu dispositivo no cuenta con alguna contraseña o patrón de bloqueo para acceder a éste?	
24. ¿Instalas aplicaciones sin conocer los permisos de acceso a funciones del mismo o sin leer los términos y condiciones de las mismas?	
25. ¿Tienes tus cuentas de redes sociales y comunicación activas en el dispositivo en todo momento?	
26. ¿Has realizado modificaciones al software de fábrica del dispositivo?	
27. ¿Haz instalando aplicaciones que no provengan de la tienda oficial de aplicaciones de tu dispositivo?	
28. ¿Guardas en tu dispositivo móvil notas de texto que contengan claves de acceso personal?	

Entre más respuestas afirmativas tengas, más vulnerable eres de convertirte en víctima de robo de identidad, utiliza la siguiente imagen:

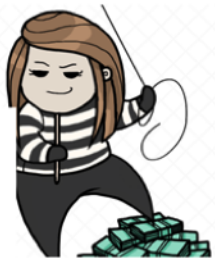


Historia de Marcela

Ella es **Marcela**, su historia: en tres meses hicieron transacciones a su nombre por más de **$500,000.00 pesos**

Sin que Marcela se diera cuenta, un par de bandidos le robaron su cartera.

Marcela recibe una llama del área de **"Prevención de Fraudes"** del banco, le notifican cargos a su tarjeta por mas de **$30,000.00**

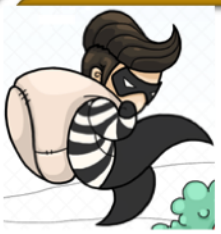


Marcela a través de la consulta de su buro de crédito descubre que a su nombre Se autorizaron **9 tarjetas de crédito**, además de un préstamo bancario por **$200,000.00 pesos**, sumando mas de **$500,000.00 pesos GASTADOS EN 3 MESES**

12 Octubre 10:30 h

Marcela acude a una cafetería a desayunar.

12 Octubre 10:40 h



12 Octubre 11:30 h

Se realizaron compras en tres diferentes tiendas departamentales con las tarjetas de Marcela.

12 Octubre 12:40 h

15 Noviembre 10:00 h

Marcela recibe sus estados de cuenta de tarjetas que tenia en su cartera por un monto de **$30,100.00 pesos** Además descubre que robaron **$15,000.00 pesos** de su cuenta de ahorro.

16 Diciembre 10:00 h

Noticia publicada en http://www.excelsior.com.mx/nacional/2013/06/09/903192

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Comisión de Normatividad de Datos Personales

Coordinación de Protección de Datos Personales

y Dirección General de Prevención y Autorregulación