SU DINERO CUENTA
ROBO DE IDENTIDAD

HSBC Bank

Juntos prosperamos

ÍNDICE

¡El programa "Your Money Counts" de HSBC le puede ayudar!
Comuníquese con nuestros socios en GreenPath Financial Wellness para hablar personalmente con un experto del bienestar financiero al 866.692.2659 y visite us.hsbc.com/yourmoneycounts & greenpath.org.

¿QUÉ ES EL ROBO DE IDENTIDAD?

El robo de identidad es el crimen de usar la información personal, historial de crédito, u otras características identificativas de otra persona para hacer compras o pedir dinero prestado sin el permiso de esa persona. Desafortunadamente, la mayoría de las personas no consideran el impacto del robo de identidad hasta que han sido víctimas. Cada año, millones de personas son afectadas y puede ocurrir de muchas formas diferentes.

Es fácil asumir que nuestra información personal está segura, sin embargo, 19 personas se convierten en víctimas de robo de identidad cada minuto. Es un número alarmante, pero no debe asustarse, ya que hay pasos que puede tomar para proteger su identidad.

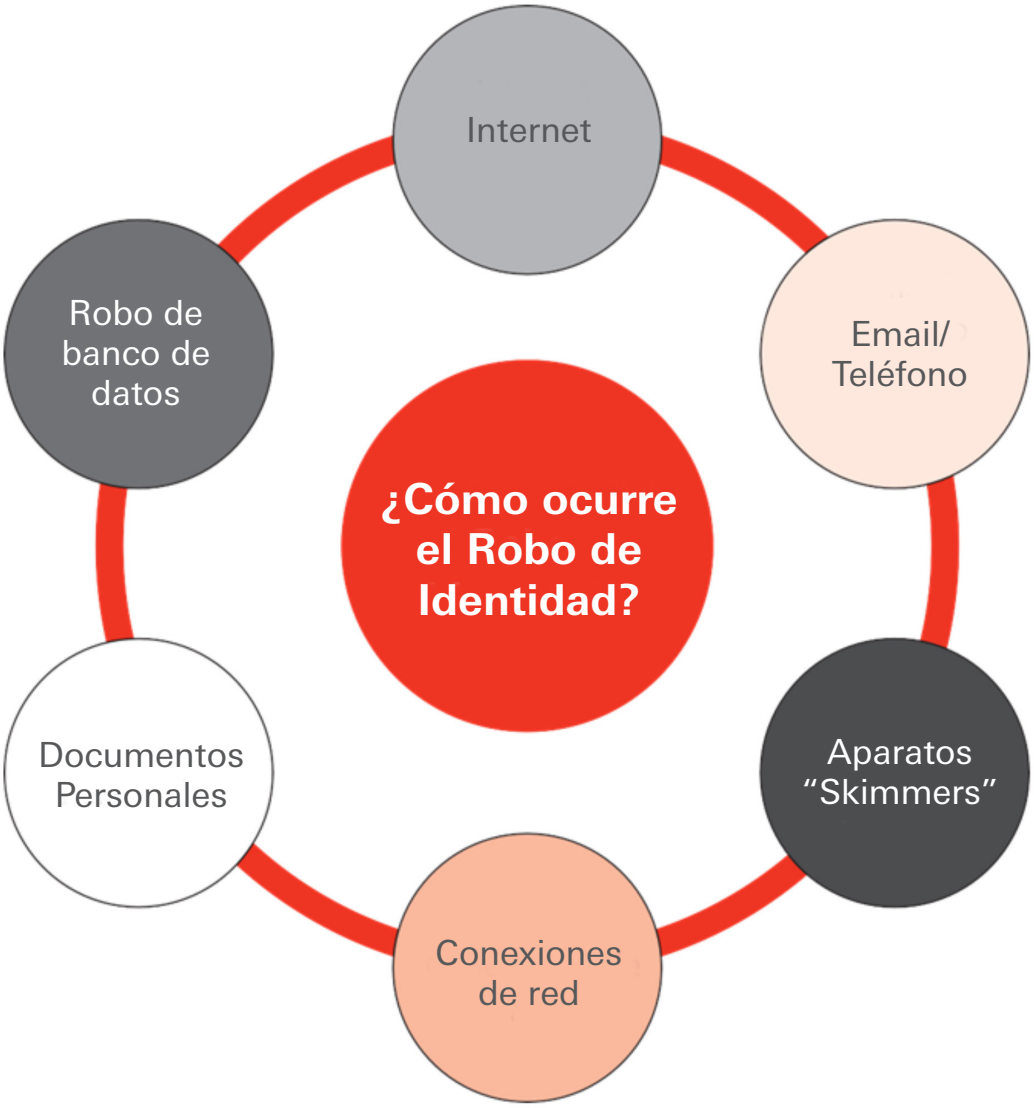
CÓMO USAN SU INFORMACION LOS LADRONES DE IDENTIDAD

Los ladrones de identidad utilizan su información personal de varias maneras. Por ejemplo, ellos:

- Usan sus cuentas de débito y crédito para comprar mercancía.
- Abren nuevas cuentas de crédito, las usan y puede que no paguen las facturas, lo que causa que las facturas retrasadas aparezcan en su reporte de crédito. En otras ocasiones, quizá hagan los pagos mínimos para mantener la línea de crédito abierta y activa.
- Establecen servicio de teléfono o de internet usando su nombre.
- Abren cuentas bancarias y escriben cheques sin fondos.
- Sacan préstamos a su nombre y compran bienes de consumo.
- Obtienen un pasaporte, empleo, seguro de salud o licencia para conducir.

CÓMO OCURRE EL ROBO DE IDENTIDAD

Un ladrón de identidad obtiene alguna pieza de información personal sin su conocimiento y la usa para cometer fraude y/o robo. Algunos ejemplos de formas en que los ladrones pueden acceder a su información son:



INTERNET

Pharming

Pharming es una forma de robo de identidad que ocurre a través del Internet cuando una persona (Pharmer) dirige a los usuarios a sitios de web comerciales fraudulentos y captura la información personal introducida por los usuarios. Se le puede dirigir a estos sitios fraudulentos por medio de un correo electrónico.

Vea los ejemplos de sitios web abajo. Puede que al principio no note ninguna diferencia. Sin embargo, si mira más de cerca, ¿puede identificar qué está mal? Este sitio es sospechoso. Si examina el texto, verá que no es Facebook.com. Se ve muy similar pero no termina en .com y además, no es un sitio seguro (no tiene el símbolo de candado o el https://). Si introdujese su correo electrónico y contraseña en el segundo sitio, la información puede ser guardada y utilizada por un ladrón de identidad, poniéndolo a usted en riesgo. Así que, ¡tenga cuidado! Asegúrese de buscar el símbolo de candado o el https: adelante de la dirección del sitio web y léala con cuidado para asegurarse que está en el sitio web correcto.

Los sitios de internet de buena reputación requieren que el inicio de sesión sea seguro. Sitios falsos capturaran su información de acceso y posiblemente robar sus datos.

SUGERENCIAS PARA EVITAR PHARMING:

- Esté al tanto de donde se encuentra en el internet. ¿Estás en el sitio que pensabas?
- No mande su información personal o financiera por email tampoco introdúzcala en un sitio de internet del que no está seguro.
- Asegúrese que se halla en un sitio seguro y codificado Un sitio seguro generalmente se designa por una URL que comienza con "https" donde la "s" significa seguro. También puede que tenga un icono de candado.

EMAIL

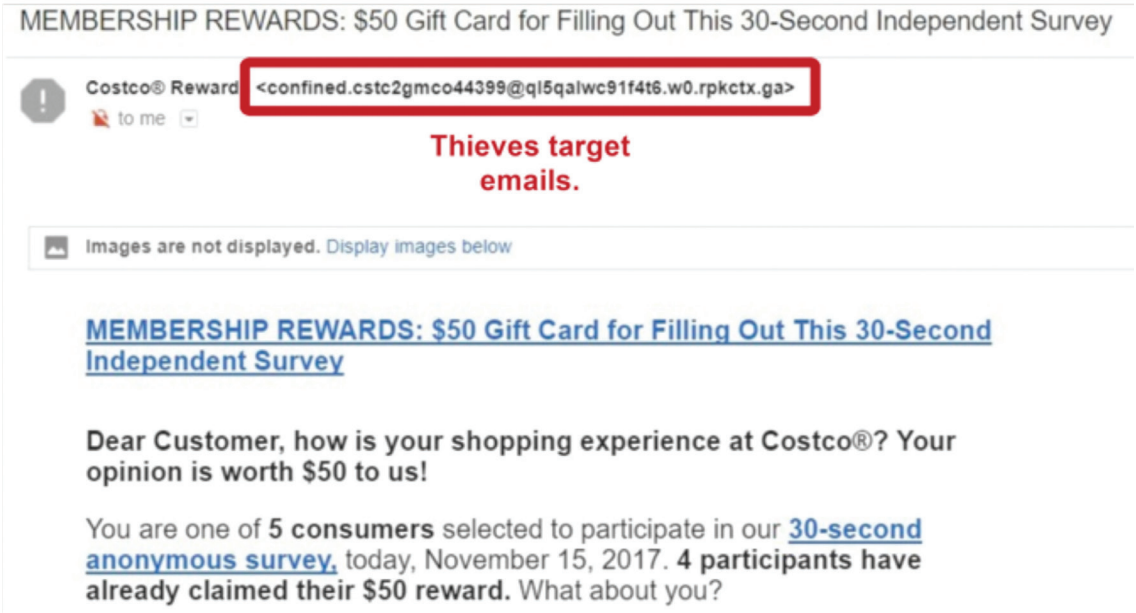
Phishing

Phishing es una práctica en la que los ladrones de identidad intentan "pescar" por contraseñas e información financiera usando el correo electrónico. Los estafadores construyen un sitio falso y envían miles de correos electrónicos falsos con un enlace al sitio falso. Las víctimas hacen clic en el enlace del correo pensando que es legítimo. El sitio les insta a introducir su información personal. Los estafadores recopilan la información personal robada y la venden en línea o la utilizan para sí mismos.

Mira al ejemplo de correo electrónico abajo. ¿Qué hay de sospechoso con este correo? ¿Haría clic en el enlace de este correo electrónico?

Este es un ejemplo de un correo spam donde el ladrón de identidad está "phishing" (pescando?) por su información personal. La dirección de correo del remitente tiene un conjunto de letras y símbolos aleatorios en vez de una dirección de correo tradicional como @costco.com o una dirección parecida de corporación. Si hiciera clic en el enlace del correo, será dirigido a un sitio sospechoso donde un ladrón está esperando robar su nombre de usuario y contraseña.

Puede que reciba un email parecido que el ladrón de identidad hace ver como que viene de su banco. Favor de notar que HSBC nunca le mandará un correo pidiendo su información personal y ningún otro banco tampoco. Use la misma diligencia y lógica para determinar la validez de este tipo de correo. Si no está seguro, ¡no haga clic!



SUGERENCIAS PARA EVITAR PHISHING:

- Borre correos desconocidos y no descarge anexos o haga clic en enlaces incluidos en el correo.
- No permita que la conveniencia remplace la seguridad. No haga clic en enlaces de correos que no esperaba o si esta inseguro de quien los manda
- Contacte a la empresa o individuo por teléfono y confirme la validez del correo. No de respuesta al correo.

TELÉFONO

Vishing

"Vishing" o phishing por voz es un tipo de ataque hecho por teléfono. Los estafadores llaman y intentan de manipular a las personas a tomar acción o suministrar información. Un visher puede tratar de conseguir información sobre la familia o la vida personal de la víctima por medio de preguntas. La víctima desconocidamente suministra la información que se usa para estafarle. Un Visher también puede utilizar tácticas de miedo, como diciendo que un familiar está en dificultades y necesitan que le mande dinero. Vishers pueden fingir llamar de su institución bancaria y lograr que usted revele contraseñas, números de clave o números de tarjetas de crédito y usar la información para que puedan tener acceso a sus cuentas. Si no conoce al llamador, ¡no de información personal o confidencial!

SMShing

SMShing o SMiShing (un término bastante nuevo en el mundo cibernético) es el equivalente de phishing a través de un dispositivo móvil. SMShing ocurre cuando usted recibe un mensaje SMS (texto) en su teléfono que afirma venir de una fuente confiable y le pide información personal.

SUGERENCIAS PARA EVITAR VISHING AND SMSHING:

1. No revele información confidencial por teléfono o texto. Instituciones bancarias nunca le pedirán sus contraseñas o números clave.
2. Si está inseguro que el llamador o mandador de texto es quien afirma ser, avísele que terminará la llamada y comuníquese con la empresa directamente.
3. Registre su número en la lista nacional Do Not Call para remover su número de la mayoría de las listas de telemercaderes. Regístrese en www.donotcall.gov.
   - Tenga en mente que la lista Do Not Call es respetada por las organizaciones legítimas. Los estafadores no obedecen esta ley.

SKIMMERS

Un skimmer es un aparato pequeño utilizado para robar información de las tarjetas de crédito o débito durante una transacción legítima. Cuando una tarjeta se pasa por un skimmer, el aparato captura y guarda los detalles de la banda magnética de la tarjeta. Los skimmers son comunes en los cajeros automáticos (ATM) y las bombas de gasolina.

SUGERENCIA PARA EVITAR SKIMMERS:

- Utilice una bomba de gasolina que esté a la vista del empleado.
- Cuando le sea posible, utilice los cajeros automáticos en su banco.

CONEXIONES DE RED

El acceso de los ladrones de identidad a información personal es en gran medida a través de las conexiones de red (internet) inseguras. Así que es importante que usted use conexiones de Wi-Fi seguras cuando utilice sus aparatos móviles o computadoras.

Vea las imágenes de conexión abajo. ¿Cómo sabe si está conectado a una red segura de su aparato móvil o su computadora? Cuando se conecta a Wi-Fi desde una computadora, una conexión de red insegura tendrá un símbolo de signo de exclamación negro y no requiriera una contraseña. Una red segura requiriere una contraseña.

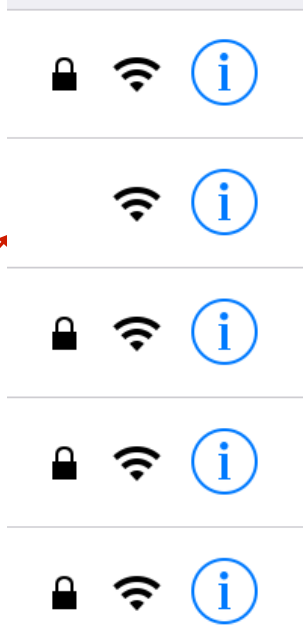
Al conectarse por medio de un aparato móvil, un símbolo de candado indica una red segura y requiriera una contraseña para conectarse. Si no ve un símbolo de candado y no se requiere entrar contraseña, es una red abierta o insegura.

Computadora

Segura

Insegura

Aparato Móvil



SUGERENCIA PARA EVITAR CONECTARSE A UNA RED INSEGURA:

Apague las configuraciones de su computadora y aparato móvil que lo conectará automaticamente a una red abierta.

DOCUMENTOS PERSONALES

Otra forma en que ocurre el robo de identidad es a través de la pérdida de información personal. Esto sucede cuando alguien, ya sea un amigo, pariente, empleado o desconocido roba sus datos o su información personal está comprometida de alguna manera. Los ladrones de identidad roban correo, buscan entre la basura, o sencillamente toman su billetera, cartera, o celular para acceder a su información personal. También pueden estar vigilándolo mientras está trabajando o tomar su información si se aleja de su computadora sin bloquearla.

SUGERENCIA PARA EVITAR LA PÉRDIDA DE INFORMACIÓN PERSONAL:
No escriba su número PIN ni lo guarde con sus tarjetas o donde otros puedan verlo facilmente.

Empezando en la página 11, encontrará otras maneras para proteger su información y documentos de forma proactiva.

ROBO DE ARCHIVO DE DATOS

Una violación de datos surge cuando su archivo personal es robado y luego usado/explotado del lugar donde realiza sus negocios. Por ejemplo, tal vez haya oído hablar de una tienda grande donde ha surgido una violación y se han robado archivos con números de crédito/débito.

SUGERENCIA PARA EVITAR SER IMPACTADO POR UN ROBO DE ARCHIVOS DE DATOS:

Sea proactivo. Si sabe de un robo de datos que le puede afectar, cambie las contraseñas asociadas con la cuenta comprometida inmediatamente.

Ejemplos de Robos de Archivos de Datos: Titulares

- "Robo de Datos de Delta 2018: ¿Se expuso su información?"
- "El Robo de datos de Target se está convirtiendo en pesadilla"
- "Yahoo! dice que tienen 500 millones de cuentas robadas"

Robo de Datos de EQUIFAX 2017

En el 2017, 144 millones de americanos se vieron afectados por el robo de datos de Equifax. Equifax es una de las 3 agencias mayores de crédito. Debido a este robo, Equifax ofreció 1 año de monitoreo de crédito gratis a cualquiera que fue afectado y lo solicite. Es muy importante que revise su reporte de crédito por precisión cada cuatro meses. Revíselo inmediatamente tras un robo de datos que le pudiera afectar. Para obtener su reporte de crédito gratis, vaya a ***annualcreditreport.com***.

PROTEJA SU IDENTIDAD

Ya que existe tanta información personal circulando, casi todos son vulnerables al robo de identidad. Está en riesgo si alguna vez solicito una tarjeta de crédito o un préstamo, asistió a la universidad o ha tenido un empleo, tiene una cuenta de ahorros o corriente, o ha tenido seguro médico con un empleador.

Puede minimizar su riesgo al administrar agresivamente su información personal y por medio mantenerse consciente del problema continuamente. Hay muchas maneras en las que puede protegerse del robo de identidad:

Número de Seguro Social (SSN)

- Suministre su SSN solamente cuando sea absolutamente necesario (p.ej. su empleador lo necesita para reportar impuestos y salario).
- NO CARGUE su tarjeta de seguro social consigo. Manténgala en un lugar seguro, como en una caja fuerte en casa.
- Nunca escriba su SSN en sus cheques.
- Si alguien le pide su SSN, haga las siguientes preguntas: (las respuestas le ayudarán a determinar si quiere continuar negociando con ellos).
  - ¿Por qué lo necesita?
  - ¿Cómo es protegido contra el robo?
  - ¿Cómo será utilizado?
  - ¿Qué pasa si no se lo doy?
- Revise sus ingresos y declaración de beneficios del Seguro Social cada año en busca de fraude.

Contraseñas

- Cree una contraseña compleja usando letras mayúsculas y minúsculas, números y caracteres especiales.
  - No utilice información fácil de identificar tal como: apellido de soltera de madre, dirección, fecha de nacimiento, o su número de teléfono.
  - Hágala significativamente diferente de contraseñas anteriores.
  - Si le cuesta recordar sus contraseñas, escriba pistas que le ayudarán con la memoria, pero que no son fáciles para otra persona. Mantenga las pistas en un lugar seguro.
- Use diferentes contraseñas para diferentes cuentas.
- No guarde sus contraseñas en una computadora portátil compartida o su celular.
- Si piensa que alguien más sabe su contraseña o ha conseguido acceso a su cuenta, cambie su contraseña inmediatamente.
- No comparta sus contraseñas con nadie y no las escriba y cargue con usted.

DOCUMENTOS PERSONALES/INFORMACIÓN

En Casa

- Destruya todo material confidencial, tal como facturas, ofertas de crédito pre-aprobadas, y otros documentos con información personal.
- No escriba su número clave ni lo cargue con usted.
- No deje su información personal a la vista donde parientes, compañeros de cuarto o la ayuda doméstica la pueda ver.
- Manténgase al tanto de sus finanzas, especialmente las fechas de vencimiento de las facturas.
- Si recibe una llamada, pida llamarle de regreso. No divulgue su información a menos que sepa con quién habla.
- Reporte cualquier cargo cuestionable en sus facturas.
- Cuando pague sus facturas por correo, no escriba su número de cuenta bancaria o de tarjeta de crédito en los cheques.
- Firme y active sus tarjetas nuevas inmediatamente. Corte y tire a la basura toda tarjeta de crédito expirada.
- Si puede, deposite todo correo directamente a la oficina de correos y mantenga sus contenedores de basura en un área segura.
- Haga copia de toda su información financiera, personal, y tarjetas de seguro e identificación que carga en su billetera. Guárdela en lugar seguro en casa.
- Solicite un reporte crediticio cada año de cada una de las tres agencias principales de crédito a través de *annualcreditreport.com*.

Cuando está fuera de casa

- Lleve solo los documentos que realmente necesita. Elimine toda información identificativa de su billetera.
- Siempre asegure su tarjeta de Cajero Automático (ATM), Número Clave de Identificación (PIN) y recibos del cajero automático.

En el trabajo– Practique la seguridad y cuestione todo

- Bloquee su computadora portátil cada vez que se aleje de ella. Si la usa en un cuarto de hotel, apáguela y asegúrela cuando salga del cuarto.
- No tire a la basura ninguna información personal
- Use una pantalla de privacidad con su computadora portátil para evitar que otros sentados a su lado lo espíen.
- Siempre apague el internet inalámbrico en su computadora cuando no la esté usando.

Tecnología

- Use un navegador seguro para proteger la seguridad de sus transacciones en línea.
- Habilite la opción de contraseña de acceso en su aparato móvil.
- Actualice regularmente el programa de protección contra virus en su computadora de casa.
- Pague sus facturas en línea. Hay menos probabilidades de robo de identidad al pagar en línea que pagarlos a través del correo.
- Lea las políticas de privacidad cuidadosamente.
- No descargue archivos de personas extrañas o haga clic en hiperenlaces enviados de personas desconocidas.
- Si recibe un correo electrónico de un amigo que solo contiene un enlace, o si algo no le parece bien comuníquese con su amigo antes de hacer clic.
- Evite el uso de inicio de sesión automática para los servicios en línea.

Reduzca su riesgo en línea

Ya que mucho de lo que hacemos hoy es en línea, es importante que reduzcamos el riesgo lo más posible. Aquí tiene unas sugerencias adicionales para protegerse en línea.

- *Programa antivirus* – un programa antivirus detecta, impide, y remueve los virus de una computadora. Asegúrese de usar un programa de buena reputación en todos sus aparatos tecnológicos y actualícelos regularmente. Unas buenas opciones incluyen Bitdefender, Norton, and Kaspersky Lab.
- *Limpie los cookies* – Cookies de Internet son archivos específicos usados por los sitios web que registran varias actividades del usuario. Debe borrar los archivos de su navegador regularmente. Vaya a "configuraciones" y siga las instrucciones para borrar. La mayoría de las configuraciones de cookies de navegador se hayan en el menú de "configuraciones" u "opciones". Busque en línea para determinar cómo borrar las cookies de su navegador. También puede navegar en modo incognito o InPrivate. Para ello, haga clic con el botón derecho en el símbolo de internet y escoja navegar InPrivate o incognito. Esto le permite navegar sin adjuntar al historial o cookies.
- *Sea cuidadoso con lo que comparte en las redes sociales* – Los ladrones de identidad buscan su información en muchos lugares y las redes sociales pueden ser un lugar fácil para juntar su información personal si no tiene cuidado. No comparta documentos con fotos de identificación, facturas, confirmación de viaje o boletos para eventos.
- *Al usar Apps* – ¿qué tipo de acceso permite? – Sea cuidadoso al usar apps que le piden sus datos o localidad. El permitir acceso a sus contactos o "Dar inicio a través de Facebook" en aplicaciones de tercera parte da acceso a su información.

En resumen, asegúrese de proteger lo que pueda controlar lo mejor que pueda. La mejor ofensa es una buena defensa. Sea consciente del robo de identidad, sea vigilante con su información y reporte cualquier actividad sospechosa inmediatamente.

¿HA SIDO VÍCTIMA DE ROBO DE IDENTIDAD?

A veces, uno descubre que ha sido víctima de robo de identidad en el momento más inoportuno. Por ejemplo, la pérdida de empleo, una denegación de préstamos, incluso un arresto, puede ser la primer indicación de que ha sido una víctima.

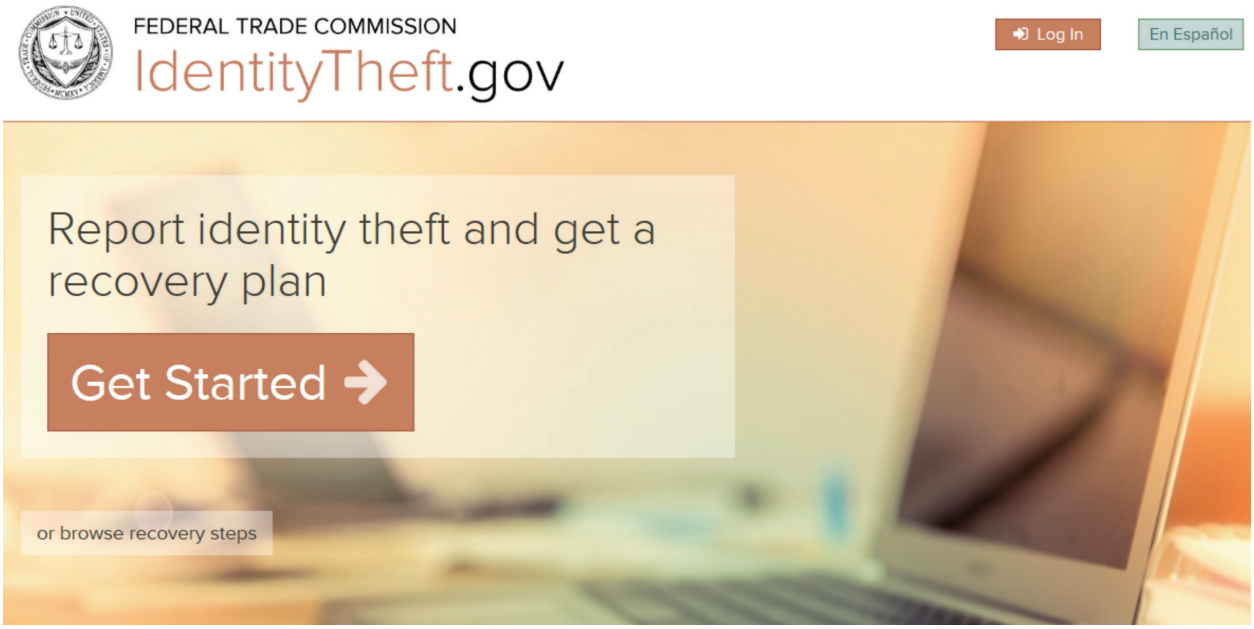
Algunas de las maneras más comunes para saber si ha sido víctima incluyen:

- Cargos o retiros inexplicables en su cuenta corriente o de ahorros
- No recibe facturas mensuales
- Recibo de tarjetas de crédito que no se solicitaron
- Denegación de Crédito sin razón aparente
- Llamadas de acreedores y cobradores de deudas para facturas que no son suyas
- Inexactitudes en sus reportes de crédito que no son el resultado de errores humanos

¿CÓMO RECUPERARSE?

Si ha sido víctima de robo de identidad, debe averiguar cuantos de sus registros han sido afectados. Es posible que deba presentar un informe policial. Algunas de las ubicaciones de sus registros son más comunes que otras. Las bases de datos más comunes incluyen: agencias de crédito, policía local y estatal y el Departamento de Vehículos. También es posible que su información personal aparezca en las listas de vigilancia federales debido a la actividad criminal del ladrón de identidad, listas de actividades bancarias fraudulentas, y o direcciones desconocidas afiliadas con su número de seguro social.

Si se convierte en víctima de robo de identidad, actúe rápidamente para restaurar su buen nombre. Un buen recurso que suministra instrucciones paso a paso para ayudarle a través del proceso de recuperación se puede hallar en *IdentityTheft.gov*.



Dependiendo en el tipo de robo de identidad que ocurrió, puede haber diferentes pasos a seguir y el sitio lo guiara a tomar los pasos apropiados. Generalmente, debe considerar lo siguiente:

PASO 1: Llame a las empresas donde sabe que ocurrió el fraude.	• Pida hablar con el departamento de fraude • Cierre o congele sus cuentas • Siga los procedimientos para disputar los errores • Cree nuevos PINS, contraseñas, etc.
PASO 2: Comuníquese con las Agencias de Crédito para colocar una alerta de fraude y obtener sus reportes de crédito.	• Coloque un alerta de fraude en su reporte de crédito con las tres agencias - Equifax, Experian y Transunion • Revise sus reportes de crédito cuidadosamente (puede ordenar su reporte de crédito gratuito d *Annualcreditreport.com*).
PASO 3: Reporte robo de identidad al FTC y otras autoridades apropiadas.	• Presente una queja con el FTC en www.ftc.gov • Tiene la opción de presentar un informe policial con el departamento de policía local donde ocurrió el robo. Se requiere un informe policial para congelar sus cuentas. • Si parece que alguien está utilizando su número de Seguro Social, comuníquese con la Administración del Seguro Social (SSA) en *www.ssa.gov*. • Contáctese con el Servicio de Correo para reportar si su correo está siendo manipulado o alterado.
Qué hacer a continuación: Haga un seguimiento para reparar el daño y mantenga buenos registros. (Documente sus acciones y adquiera toda confirmación por escrito).	• Cierre las cuentas que se han abierto. Pida la confirmación por escrito. • Pida que se remueva todo cargo fraudulento. • Haga un seguimiento con la Agencia de Reporte de Crédito para corregir errores en su reporte de crédito. Obtenga una copia de su reporte de nuevo en unos meses para verificar que se haya efectuado toda corrección. • Considere agregar una alerta de fraude extendida a los 90 días o considere un congelamiento de crédito.

SUGERENCIAS:

El robo de identidad no se resuelve de la noche a la mañana. Como promedio, toma 6 meses o 200 horas para reparar el robo de identidad. Puede tener un impacto negativo en su puntaje de credito y impactar su capacidad de hacer cosas como comprar una casa, alquilar un apartamento, obtener un préstamo u otro tipo de crédito. Incluso puede dificultar la apertura de nuevas cuentas de utilidades o cuentas corrientes. Así que es muy importante actuar rápidamente y tomar las medidas adecuadas para corregirlo.

EL ROBO DE IDENTIDAD Y LAS LEYES QUE LO PROTEGEN

Resolver problemas de crédito causados por el robo de identidad puede llevar mucho tiempo y ser frustrante. Existen protecciones bajo la ley federal para corregir reportes de crédito y errores de facturación. También hay una ley federal que lo protege de ser contactado por cobradores sobre deudas que no son suyas.

Además, se han emitido leyes Federales que específicamente aplican al robo de identidad.

Ley de Transacción de Crédito Justa y Precisa (FACT Act) del 2003

- Le da al consumidor el derecho a obtener su reporte de crédito gratis cada año.
- Requiere que los vendedores omitan todos los números de la cuenta de su tarjeta de crédito excepto los últimos cinco números, en los recibos de tienda.
- Crea y establece un sistema nacional de detección y alerta de fraude para consumidores.
- Crea una Regla de Eliminación que establece que cualquier persona que mantenga o posea información del consumidor para propósitos de negocios, debe destruir la información adecuadamente antes de desecharla.

Ley de Disuasión y Asunción de Robo de Identidad de 1998

- Convierte en un crimen federal cuando alguien usa o transfiera los medios de identificación de una persona, sin una razón legal para hacerlo y con la intención de cometer un crimen.

Ley de Ampliación de Penalidad para Robo de Identidad

- Establece mayores sanciones para ladrones de identidad.
- Crea el crimen de "robo de identidad agravado" sancionado con hasta dos años de prisión cuando se comete en conexión con otras felonías.

Ley de Facturación de Crédito Justo

- Otorga a los consumidores derechos particulares cuando están tratando con errores de facturación.

Ley de Transferencia de Fondos Electrónicos

- Establece procedimientos para resolver errores en los estados de cuentas para transferencia de fondos electrónicos.

Ley de Reporte Justo de Crédito

- Diseñado para promover la precisión, equidad (¿) y privacidad de la información en los expedientes de cada Agencia de Reportes de Consumidor, la más común de las cuales es una agencia de crédito.

SUGERENCIAS:

Si tiene problemas con su crédito tras un robo de identidad y quiere consultar con alguien sobre su situación, hay agencias de consejería de crédito sin fines lucro que le pueden ayudar. Para una discusión más profunda sobre estos temas, se puede comunicar con GreenPath Financial Wellness, una organización de bienestar financiero sin fines de lucro. Sin costo a usted, su situación puede ser revisada llamando al *866-692-2659* o visitando *www.greenpath.org*.

VIGILE SU CRÉDITO PARA PROTEGERSE DE SER UNA VÍCTIMA

Monitoreo de su crédito debe ser un componente clave de su plan de finanzas.

Es importante que entienda la información en su reporte de crédito independientemente de su situación financiera. Esta información tiene un impacto directo en su capacidad de obtener una tarjeta de crédito, comprar un auto o casa, alquilar un apartamento, o hasta obtener nuevo empleo. Dos de las mejores razones para revisar su crédito hoy son 1) asegurarse de que su reporte de crédito esté acertado 2) para protegerse de fraude o robo de identidad.

Puede crear su propio sistema de monitoreo continuo obteniendo uno de sus reportes de crédito gratuitos cada cuatro meses de annualcreditreport.com.

Por ejemplo:

1. En Enero, solicite su reporte de Experian.
2. Luego en Mayo, solicite su reporte de TransUnion.
3. Y finalmente, en Septiembre, solicite su reporte de Equifax. Comience el proceso de nuevo en Enero.

Dado que las tres agencias tienen casi la misma información, podrá monitorear la actividad en sus reportes de crédito e identificar los puntos en cuestión. Si encuentra errores o inexactitudes, puede presentar una disputa con cada una de las tres agencias. La información de contacto se encuentra abajo.

OFICINAS DE CRÉDITO		
Contacto:	Teléfono:	Sitio de internet:
Experian	888-EXPERIAN	www.experian.com
TransUnion	800-916-8800	www.transunion.com
Equifax	800-685-1111	www.equifax.com

Los niños también pueden ser víctimas de robo de identidad. Si usted tiene un niño y sospecha que ha sido víctima de robo de identidad, puede verificar si existe un informe de crédito para su niño. Cada sitio de las agencias de crédito tiene instrucciones sobre cómo hacer esto.

Cuando tiene que ver con su información personal precaución y prudencia son la orden del día.

CONCLUSIÓN

El robo de identidad es un crimen. Afecta a muchas personas cada año. Aunque no hay garantía para evitarlo, sí hay pasos que puede seguir para protegerse. Proteger su número de seguro social, revisar su reporte de crédito, estar al tanto de su entorno al hacer compras, especialmente si se requiere información delicada, son pasos que puede tomar para protegerse. Y recuerde, si usted es una víctima de robo de identidad, no te asustes. Comuníquese con las autoridades apropiadas y use los pasos descritos en este cuaderno.

RECURSO: GreenPath Financial Wellness es una organización sin fines lucros que suministra consejería de finanzas, educación, y productos para capacitar a las personas a llevar vidas financieras saludables. Por medio de trabajar directamente con individuos, y a través de asociación con otras organizaciones, GreenPath tiene como objetivo redefinir el sueño americano para que funcione para todos. Con su sede en Farmington Hills, Mich., GreenPath tiene casi 500 empleados y opera unas 60 sucursales en 19 estados. GreenPath es miembro de la Fundación Nacional de Consejería de Crédito (NFCC, por sus siglas en ingles), y es acreditada por Concilio de Acreditación (COA, siglas en ingles). Para más información, visite greenpath.org o para hablar uno a uno con un experto certificado de finanzas, llame al 866-692-2659.

¿CUALES SON LOS PRÓXIMOS PASOS?

Es importante el tomar lo que ha aprendido y actuar. Sea proactivo para defenderse contra el robo de identidad. Complete el plan de acción y use la lista de verificación para asegurarse que sigue moviéndose hacia sus metas. Fije una fecha para completar la meta y marque la caja cada vez que complete una acción.

PLAN DE ACCIÓN:

- ☐ 1 **Voy a:** ser cuidadoso en el internet y con correos electrónicos desconocidos.
- ☐ 2 **Voy a:** estar al tanto de los skimmers en los ATM's y otros lugares cuando uso mi tarjeta.
- ☐ 3 **Voy a:** usar solo redes seguras y desactivare las opciones de conexión automática en mi computadora y aparatos móviles.
- ☐ 4 **Voy a:** proteger mis documentos personales incluyendo mi número de seguro social, contraseñas, PINS, y materiales delicados. Crearé contraseñas complicadas, trituraré los documentos confidenciales y usaré la tecnología con cuidado para proteger mi información personal.
- ☐ 5 **Voy a:** ser consciente de las violaciones de datos en las noticias y seré proactivo si me entero de que una de estas me afecta.
- ☐ 6 **Voy a:** reducir mi riesgo en línea usando y actualizando programas de antivirus, borrando cookies cuando estoy en el internet, no compartiendo información personal en las redes sociales y siendo cuidadoso usar apps para no permitir acceso a mi información personal.
- ☐ 7 **Voy a:** seguir los pasos de recuperación encontrados en identitytheft.gov, si soy víctima de robo de identidad. Monitorearé mi reporte de crédito cada año para verificar su precisión y me comunicaré con GreenPath Financial Wellness al 866-692-2659 si necesito guía adicional de un experto.

Notas o metas adicionales: _____

_____

¡Estaré preparado!

TÉRMINOS CLAVES

Programa antivirus – Un programa que detecta, previene, y remueve los virus de la computadora.

App – Una aplicación o programa diseñado para ser descargado en un aparato móvil.

Cookies – Archivos especiales utilizados por sitios de internet que llevan un registro de varias actividades de los usuarios. Debe borrarlos de su navegador de internet regularmente yendo a configuraciones y siguiendo las instrucciones para borrar.

Congelación de crédito – Un consumidor puede colocar una congelación de crédito en su reporte que lo bloquea para que no se puedan abrir cuentas nuevas. La congelación se mantiene en lugar hasta que usted la remueva. (En ciertos estados, expira después de 7 años.) Dependiendo de la ley del estado, las congelaciones de crédito pueden tener tarifas. En la mayoría de los estados son gratis para las víctimas de robo de identidad. Para otros, cuestan alrededor de $5 a $10 cada vez que el consumidor congela o descongela su cuenta con cada agencia de reporte de crédito

Reporte de Crédito – Un reporte financiero utilizado para evaluar su valor crediticio y calcular su puntaje crediticio. Contiene información detallada sobre el historial de crédito incluyendo su información identificadora personal, información sobre cuentas de crédito y préstamos (incluyendo historial de pagos), registró público, y solicitudes.

Robo de Archivo de Datos – Archivos de datos personales son robados de un negocio y utilizados/explotados.

Alerta de Fraude – Un consumidor puede colocar una alerta de fraude en su reporte de crédito que dificulta a un ladrón abrir más cuentas a su nombre, y requiere que el prestamista/negocio intente verificar la identidad del consumidor antes de extender crédito nuevo. Es gratis y generalmente permanece en su reporte por 90 días, a menos que se reanude.

Robo de identidad – El crimen de utilizar la información personal, historial de crédito u otras características identificativas de otra persona para hacer comprar o conseguir préstamo sin su permiso.

Contraseña – Una palabra o frase secreta que se puede utilizar para tener admisión a algo. Una contraseña fuerte debe ser compleja y contener tanto letras mayúsculas, minúsculas, números, y caracteres especiales.

Número de Identificación Personal (PIN) – Un código alfanumérico usado en muchas transacciones financieras electrónicas para autenticar un usuario en un sistema. Por ejemplo, debe introducir su PIN para tener acceso a su cuenta bancaria desde un ATM.

Información Personal /Documentos – Documentos que contienen información personal identificadora como número de seguro social, fecha de nacimiento, dirección, etc., que los ladrones pueden robar y utilizar para cometer fraude sin que usted lo sepa.

Pharming – Una forma de robo de identidad que ocurre por internet cuando una persona (Pharmer) dirige a los usuarios a sitios de internet comerciales fraudulentos y captura la información personal introducida por los usuarios.

Phishing – Una práctica donde los ladrones de identidad intentan "pescar" contraseñas confidenciales y datos financieros usando correo electrónico. Estafadores construyen un sitio falso y mandan miles de emails falsos con un enlace al sitio falso. Las víctimas hacen clic en el enlace, pensando que es legítimo. El sitio los insta a introducir su información personal. Los estafadores recopilan la información personal robada y la venden en línea o la usan ellos mismos.

Conexión de Red Segura – Una conexión que está codificada por uno o más protocolos de seguridad para asegurar la seguridad de la información que fluye. Se necesita una contraseña para establecer una conexión segura.

Skimmer – Un aparato pequeño utilizado para robar información de crédito o débito en durante una transacción legítima. Cuando una tarjeta de crédito o débito se pasa por el skimmer, el aparato captura y guarda la información y los detalles de la banda magnética de la tarjeta.

SMShing – MShing o SMiShing es el equivalente Phishing a través de un dispositivo móvil. Ocurre cuando recibe un mensaje de SMS (texto) en su teléfono que afirma venir de un lugar de buena reputación y le pide su información personal.

Conexión de Red Insegura – Una conexión de red a la que puede tener acceso sin contraseña y no está codificada. Estas redes están abiertas al público.

Vishing – "Vishing" o phishing por voz es un tipo de ataque efectuado por teléfono. Estafadores llaman e intentan manipular a las personas a tomar cierta acción o suministrar información.

NOTAS