ROBO DE IDENTIDAD

Robo de identidad

Algunos datos sobre el robo de identidad:

- Según el informe del FBI sobre crímenes en Internet, las víctimas de robo de identidad perdieron $160,305,789 en 2019.
- Sólo 3 de cada 5 personas han revisado su reporte de crédito.
- 2 de cada 3 personas que han revisado su puntaje de crédito han tenido que tomar medidas para corregir las inexactitudes.
- El número promedio de correcciones a sus reportes de crédito para aquellos que notaron inexactitudes fue 13.
- 60% de las personas reportan que ellos o un miembro de su familia inmediata han sido alguna vez víctimas de fraude. Esto incluye cartas, correos electrónicos o llamadas telefónicas haciéndose pasar por el IRS, robo de un número de tarjeta de crédito existente, nuevas líneas de crédito abiertas en su nombre o fraude en la declaración de impuestos.
- 62 por ciento de los padres de menores no saben que sus niños están en riesgo. En 2018, casi 1 de cada 4 niños había sido víctima de robo de identidad. Esto afectó a más de 13 millones de personas.

Cómo ayudarse a sí mismo para protegerse del robo de identidad

No hay una forma segura de protegerse del robo de identidad. Pero hay muchos pasos que puede tomar para reducir las posibilidades de que alguien le robe la identidad.

La primera parte de este folleto explica las mejores prácticas para proteger su identidad.

La segunda parte de este folleto contiene los pasos que puede tomar si es una víctima de robo de identidad.

Lo básico:

Nunca dé o escriba su número de seguro social

Asegúrese de que su número de seguro social no aparezca en sus cheques o identificaciones. Si se lo piden, siempre solicite proporcionar una forma diferente de identificación.

Lleve sólo las tarjetas que necesite en su cartera

Esto incluye las tarjetas médicas que puedan tener su información confidencial. Deje las tarjetas de crédito adicionales y su tarjeta de seguro social bajo llave en su casa.

En caso de duda, opte por no participar

Lea los avisos de privacidad de sus instituciones financieras. Luego, siga las instrucciones para optar por no compartir su información. Detenga las ofertas de tarjetas de crédito no solicitadas llamando al 888-5OPT-OUT o visite www.optoutprescreen.com.

En el trabajo:

Mantenga su bolso bajo llave en el trabajo

El robo en el lugar de trabajo es más frecuente de lo que la mayoría de la gente cree. Pídale a su empleador un lugar seguro para guardar bajo llave su bolso o su cartera si no le han proporcionado ya uno.

Pregunte a su empleador sobre los protocolos de seguridad para los archivos de personal

Asegúrese de que su empleador guarde los archivos bajo llave

y que exista una política para evitar el robo. Muchos casos de robo de identidad comenzaron en el trabajo porque los compañeros de trabajo robaron datos personales.

No acceda a las cuentas financieras personales desde el trabajo

Además, no configure los ordenadores del trabajo para que recuerden automáticamente las contraseñas personales. Finalmente, no almacene información personal en su escritorio o en las computadoras del trabajo.

En casa:

Utilice un buzón seguro, si es posible, para recibir el correo

Los ladrones pueden desvalijar las facturas u otro correo de su buzón y usar esa información para cometer un fraude. Envíe cualquier correo sensible desde la oficina de correo o usando un buzón oficial del USPS.

Evite que le envíen cheques nuevos a su casa

Sólo debe recibir cheques si su buzón es seguro. Si no, pida a su banco que se los guarde en su sucursal local y recójalos allí.

Compre una trituradora de papel barata

Triture cualquier correo o documento con información confidencial antes de tirarlo.

Lleve un registro de la fecha en que normalmente llegan las facturas de sus tarjetas de crédito

Si falta alguna, comuníquese con su prestamista inmediatamente. No asuma que puede saltarse un mes de pago o que su acreedor olvidó enviarlo.

Guarde su información personal en su casa, en una habitación cerrada con llave o en un archivo seguro

Esto es especialmente importante si tiene visitas frecuentes, un ama de llaves u otras personas que puedan estar en su casa.

Revise su reporte de crédito por lo menos una vez al año

Considere un servicio de monitoreo de crédito si desea mantener un seguimiento cercano de su reporte de crédito. La detección temprana del fraude puede ahorrarle horas de tiempo y molestias más adelante.

Cuando reciba un estado de cuenta de beneficios de la SSA, revíselo cuidadosamente para detectar errores o posibles fraudes

Si ve signos de alguno de ellos, llame a la Administración del Seguro Social (SSA, por sus siglas en inglés) lo antes posible.

En Internet:

Utilice una red privada virtual

Asegúrese de usar una VPN si usa Wi-Fi público. Esta tecnología oculta su identidad, actividad en línea y comunicaciones no deseadas. Instale una VPN en su teléfono también.

Use un firewall en el ordenador de su casa

A menudo son baratos y bien valen la pena. Si está constantemente conectado a Internet a través de un módem de cable o una conexión de fibra, es especialmente importante que se proteja.

Elija buenas contraseñas y nombres de usuario

No utilice su número de seguro social, dirección o fechas de nacimiento suyas o de sus hijos. Las mejores contraseñas usan letras, números y caracteres especiales. Los mejores nombres de usuario no dan información valiosa.

Tenga cuidado con el phishing

Los estafadores pueden usar el correo electrónico o sitios web falsos para recopilar información personal de los consumidores. Miles de consumidores han sido víctimas de la estafa del correo electrónico de "PayPal", donde los consumidores reciben correos electrónicos que parecen ser de la empresa. Los correos electrónicos les piden que actualicen su información personal, pero esa información va directamente a los estafadores. Los estafadores operan sitios falsos, pero parecen reales. Siempre inicie sesión en los sitios financieros desde la página de inicio que suele utilizar.

Piénselo dos veces antes de proporcionar información personal sensible en línea

Los consumidores han sido engañados para que soliciten préstamos en sitios web falsos diseñados sólo para recopilar información sobre los consumidores. En otros casos, las empresas venden información de los consumidores a empresas externas sin su permiso. Asegúrese de que un sitio web tenga buena reputación antes de ingresar su número de seguro social u otros datos personales.

Compre con cuidado

Sólo trate con comerciantes de buena reputación que tengan sitios web seguros. Para obtener la máxima protección, utilice siempre una tarjeta de crédito en lugar de una tarjeta de débito o de cheques cuando trate con un nuevo comerciante en línea.

Enseñe a sus hijos sobre la privacidad en línea

Asegúrese de que entiendan que no deben dar ninguna información personal sin su permiso.

Antes de tirar un ordenador a la basura, vacíe el disco duro

Asegúrese de que su información ya no esté disponible para alguien que pueda recogerla de la basura o de una organización benéfica. Limpie su computadora o destruya físicamente el disco duro. Puede que no sea suficiente con borrar los archivos.

Qué hacer si le sucede a usted

Si usted es víctima de un robo de identidad, deberá tomar estas medidas inmediatamente:

Presente un informe policial

Necesitará esto para denunciar el robo. Guarde el original y haga copias para otros que lo necesiten.

Notifique a las agencias de crédito

Reporte el fraude inmediatamente a las tres principales agencias de crédito: Equifax, Experian y TransUnion. Una compañía debería notificar a las otras dos, pero asegúrese de preguntar. Pídales que pongan una alerta de fraude en su expediente.

Obtenga un plan de recuperación de la Comisión Federal de Comercio

Visite www.identitytheft.gov para obtener los formularios, declaraciones juradas y cartas que necesitará para iniciar el proceso de recuperación.

Solicite su reporte de crédito e investigue nuevas cuentas

Por ley, las víctimas de fraude tienen derecho a una copia

gratuita de su reporte de crédito. Revise sus reportes de crédito, preferiblemente de las tres agencias principales. Contacte a todos los acreedores desconocidos que aparecen en la lista de "Cuentas nuevas" o "Indagaciones". Explique que es una víctima de robo de identidad y pregúnteles cómo puede presentar una denuncia. Probablemente querrán una declaración jurada de fraude, prueba de su identidad y una copia del informe policial.

Póngase en contacto con sus acreedores

Si sospecha que alguien usó sus cuentas corrientes (especialmente las tarjetas de crédito) o robó su información, póngase en contacto con sus acreedores y pídales que cancelen esas cuentas. Esto también se aplica a su tarjeta de cajero automático o a sus tarjetas de débito.

Póngase en contacto con la Administración del Seguro Social si cree que alguien utilizó su número de seguro social de manera fraudulenta

Incluso si no está seguro, revise su declaración anual de beneficios y ganancias para asegurarse de que es correcta. Piénselo dos veces antes de solicitar un nuevo número de Seguro Social. Hacerlo puede crear más problemas de los que resuelve. Puede reportar el fraude a la SSA al 1-800-772-1213 o visite www.ssa.gov.

Verifique su dirección

Verifique con el Servicio de Inspección Postal de los Estados Unidos (www.uspis.gov) para ver si alguien presentó un cambio de dirección. También notifíqueles si sospecha que el impostor utilizó el correo de los Estados Unidos en su delito. (Por ejemplo, si han enviado por correo avisos de cambio de dirección o solicitudes de crédito).

Revise sus cheques

Si sospecha que un ladrón utilizó sus cheques de manera fraudulenta, comuníquese con las principales agencias de verificación de crédito para presentar una alerta de fraude.

- ChexSystems es la compañía de cheques más grande que provee este tipo de servicio. Contáctelos en www.chexsystems.com y haga clic en "Alerta de Seguridad" bajo el menú "Robo de Identidad" o llame al 1-800-428-9623.
- Telecheck es más pequeña pero también puede ser útil contactarlos en www.getassistance.telecheck.com/index.html o 1-800-366-2425.

Haga una doble revisión de su licencia de conducir

Si sospecha que alguien la ha usado indebidamente, póngase en contacto con el Departamento de Vehículos Motorizados de su estado para colocar una alerta de fraude en su licencia de conducir. Reportes de investigación recientes muestran que es muy fácil para los impostores obtener nuevas licencias de conducir usando la información de otras personas.

Revise su pasaporte

Alerte a la oficina de pasaportes para asegurarse de que nadie pida un pasaporte con su información (ya sea un reemplazo o uno nuevo). Visite www.travel.state.gov/content/travel.html o llame al 1-877-4USA-PPT (1-877-487-2778).

Hable con un abogado

Según la ley actual de reportes de crédito, sólo tiene dos años para presentar una demanda después de que descubra el uso indebido de su reporte de crédito. Es posible que desee hablar con un abogado si se encuentra con obstáculos en las agencias de reportes de crédito o con los acreedores. Comuníquese con

la Asociación Nacional de Defensores del Consumidor en www.consumeradvocates.org para localizar un abogado en su área. Ellos deben tener experiencia con la Ley de informes de crédito justos y los casos de robo de identidad.

¿Qué pasa si conoce al ladrón?

Muchas veces, los consumidores conocen al ladrón que robó su información. Puede ser un compañero de trabajo, un amigo, o incluso un pariente o un ser querido. Esto puede crear problemas adicionales ya que la víctima tiene miedo de que el ladrón tenga problemas con la ley. El robo de identidad es un delito grave, y si no se maneja la situación apropiadamente, puede quedar atrapado enfrentando las consecuencias en los años venideros. Para obtener guías útiles sobre qué hacer cuando conoce al delincuente, visite el Centro de Recursos sobre Robo de Identidad en www.idtheftcenter.org.

Cómo las leyes y los derechos del consumidor pueden ayudarle

En 2003, el Congreso aprobó una ley que actualizaba la Ley federal de Informe Justo de Crédito. Contiene toda una sección de requisitos que facilitan la resolución de los casos de fraude. La siguiente información resume algunos de los puntos más destacados:

Alertas de fraude por robo de identidad

Si cree que puede haber sido, o está a punto de ser víctima de un robo de identidad, las agencias de reportes crediticios deben colocar una alerta de fraude en su reporte de crédito

si usted lo solicita. Existe un sistema, por lo que sólo debe hacer una llamada telefónica para iniciar la activación de una alerta. Tendrá que llenar una declaración jurada de fraude y proporcionar una prueba de su identidad.

Los miembros de las fuerzas armadas en servicio activo pueden solicitar que las agencias coloquen una alerta en su expediente indicando que están en servicio activo. En el caso de quienes tengan alertas de fraude en sus archivos crediticios, los acreedores tendrán que tomar medidas razonables para asegurarse de que verifican la identidad del consumidor antes de abrir una nueva cuenta.

Prevención del robo de identidad

Las agencias bancarias federales, la Administración Nacional de Cooperativas de Crédito y la Comisión Federal de Comercio trabajaron conjuntamente para desarrollar directrices para cualquier persona que utilice la información de los reportes de crédito para evitar el robo de identidad. También exigen a las instituciones financieras u otros usuarios de reportes de crédito que notifiquen a la Comisión Federal de Comercio si se ha producido alguna violación de seguridad de la información de los consumidores.

Además, establecieron normas para que, si un emisor de crédito recibe una solicitud de una tarjeta nueva o de reemplazo de un consumidor en menos de 30 días después de recibir un cambio de dirección, el emisor debe tomar medidas adicionales para verificar que la solicitud sea válida.

También puede solicitar a las agencias de crédito que no revelen los primeros cinco dígitos de su número de seguro social cuando suministren su reporte de crédito a cualquier solicitante.

Si le han robado su identidad

Si usted es víctima de un robo de identidad, puede solicitar una copia de cualquier solicitud y registro de transacciones que haya hecho el impostor. Por ejemplo, puede solicitar copias del formulario de solicitud a una compañía de tarjetas de crédito que haya abierto una cuenta para el ladrón en su nombre. Deberá presentar una prueba de su identidad y, si la empresa lo solicita, una copia de un informe policial y una declaración jurada de robo de identidad. La empresa debe suministrar la información dentro de los 20 días.

Dentro de los cuatro días hábiles de haber notificado a una agencia de reportes de crédito sobre el robo de identidad, la agencia debe bloquear la información que el consumidor reporta y notificar al acreedor que reporta la información que el consumidor cree que es fraudulenta.

Las víctimas de robo de identidad tienen derecho a dos reportes de crédito gratuitos en ese año, así como a bloquear su archivo de ofertas de crédito preseleccionadas. Los acreedores también deben seguir ciertos procedimientos para asegurarse de que la información que ha sido bloqueada o eliminada no pueda volver a presentarse a la agencia de crédito. El objetivo es mantener la información legítimamente relacionada con el robo de identidad fuera del reporte del consumidor. Por lo general, los acreedores no pueden vender o transferir cuentas que los consumidores afirman que se deben al robo de identidad, especialmente a las agencias de cobro.

Los cobradores de deudas que son notificados de que una deuda puede estar relacionada con el robo de identidad deben

notificar al acreedor de quien recibieron la deuda de que ésta puede ser fraudulenta.

Recursos adicionales

Varios sitios web ofrecen información adicional útil para prevenir y afrontar el robo de identidad:
Comisión Federal de Comercio (Sitio de Robo de Identidad):
www.identitytheft.gov
Centro de Recursos para el Robo de Identidad:
www.idtheftcenter.org
Centro de Derechos de Privacidad:
www.privacyrights.org