Robo de identidad

Evite el robo de identidad

¿Qué es el robo de identidad?

El robo de identidad ocurre cuando alguien usa la información personal de otro para obtener tarjetas de crédito y préstamos o realizar otras transacciones financieras en su nombre. Estas transacciones fraudulentas afectan su calificación crediticia y sus financias si no se identifican y resuelven de inmediato.

¿Cómo se puede evitar el robo de identidad?

Cómo reducir el riesgo de robo de identidad

1. **Proteja su número del Seguro Social, números de tarjetas de crédito y débito, PIN (Número de Identificación Personal), contraseñas y otra información personal.**

Nunca proporcione esta información en respuesta a una llamada telefónica, fax, carta o correo electrónico no solicitado, sin importar lo amistosas u oficiales que parezcan las circunstancias.

Para reducir al mínimo el daño que provoca una billetera perdida o robada, lleve consigo sólo la identificación, cheques, tarjetas de crédito y tarjetas de débito que realmente necesita. El resto, incluso su tarjeta del Seguro Social, es mejor dejarlo en un lugar seguro en casa. Además, tenga mucho cuidado si tiene compañeros con quien comparte su casa o si deja entrar a otras personas a su casa, porque pueden apoderarse de la información personal y usarla sin su conocimiento.

Asimismo, no preimprima su número del Seguro Social, número de teléfono o número de licencia para conducir en sus cheques. Es muy fácil para alguien que ve sus cheques copiar esta información personal e incluso venderla a un ladrón de identidad. Recuerde que tiene derecho a negarse a dar su número del Seguro Social si se lo pide algún comerciante, ya que este tiene otras maneras de identificarlo. Si su número del Seguro Social aparece en su licencia para conducir, pida usar otro número.

2. **Proteja su correo entrante y saliente**

Es probable que el cartero le lleve una tarjeta de crédito o un estado de cuenta bancario, un sobre que contenga un cheque u otras cosa que puedan ser valiosas para un ladrón. O quizá deba enviar por correo un cheque o documentos que contienen números de cuenta u otra información financiera personal.

Para el correo entrante: Trate de usar un buzón cerrado con llave u otro lugar seguro, como un apartado postal. Si su buzón no está cerrado o en un lugar seguro, trate de recoger sin tardanza la correspondencia entregada o mude el buzón a un lugar más seguro. Cuando ordene cheques nuevos, pida que se los envíen a la sucursal de su banco en lugar de que se los envíen por correo a su casa corriendo el riesgo de que los dejen en la puerta.

Para correo saliente que contiene un cheque o información personal: Deposite el sobre en un buzón azul de recolección del Servicio Postal de Estados Unidos, entréguelo al cartero o llévelo a la oficina de correos en lugar de dejarlo en su puerta o en el buzón de su casa. Un buzón que contiene sus pagos salientes es un blanco excelente para los ladrones que deambulan por los vecindarios en busca de información de cuentas. Peor aún es colocar el banderín en el buzón para indicar que hay correspondencia saliente esperando.

3. **Inscríbase en el servicio de depósito directo**

Inscríbase en el servicio de depósito directo de su sueldo o de sus beneficios estatales o federales, como el Seguro Social. El depósito directo impide que alguien robe el cheque de su buzón y falsifique su firma para tener acceso al dinero.

4. **Conserve "limpia" su basura**

Los ladrones conocidos como "dumpster divers" hurgan en la basura para hallar pedazos de papel que contengan números del Seguro Social, información de cuentas bancarias y otros detalles que puedan usar para cometer fraudes. Son ejemplos de basura valiosa la información de seguros que contienen su número del Seguro Social, los cheques en blanco enviados por correo por instituciones financieras con ofertas para que usted mismo los llene y "escriba la cantidad que desea en préstamo", cheques cancelados y estados de cuenta bancarios.

¿Cuál es su mejor protección contra los hurgadores de basura? Antes de tirar estos documentos, destrúyalos, de preferencia con un triturador de papel que los convierte en confeti que no puede reconstruirse con facilidad.

5. **Examine atentamente sus estados de cuenta bancarios y de tarjetas de crédito**

Examine los estados de cuenta cada mes y comuníquese de inmediato con su institución financiera si hay alguna discrepancia con sus registros o si nota algo sospechoso, como un pago omitido o un retiro no autorizado. Aunque las leyes federales y estatales pueden limitar sus pérdidas si usted es víctima de fraude o robo, las protecciones pueden ser más eficaces si usted denuncia el problema oportunamente y por escrito. Póngase en contacto con su institución si un estado de cuenta bancario o de tarjeta de crédito no llega a tiempo. Esta correspondencia faltante puede ser indicio de que alguien ha robado su correspondencia o información de su cuenta y quizá cambió su dirección postal para realizar gastos cuantiosos en su nombre desde otro lugar.

6. **Evite el robo de identidad en Internet**

Los "piratas informáticos" y estafadores buscan maneras de robar la información privada que se transmite por Internet o se almacena en sistemas de cómputo. Protéjase cuando compre, realice operaciones bancarias, envíe correo electrónicos o navegue por la Web. Por ejemplo, nunca proporcione su cuenta bancaria u otra información personal en respuesta a un correo electrónico no solicitado o cuando visite un sitio web que no explica cómo protegerán su información personal.

Las estafas de "phishing" que llegan por correo electrónico por lo general le piden que "actualice" la información de su cuenta. Sin embargo, las organizaciones legítimas no le pedirían esos detalles, porque ya cuentan con la información necesaria o pueden obtenerla de otras maneras. No responda a estos correos electrónicos y no abra los datos adjuntos a menos que se comunique con la organización legítima de la manera acostumbrada y confirme de manera independiente la validez de la petición; *no* use la dirección de correo electrónico, sitio web o número de teléfono proporcionado en el correo electrónico. Si usted cree que el correo electrónico es fraudulento, considere la posibilidad de denunciarlo ante la Comisión Federal de Comercio (FTC). Si abre y responde un correo electrónico fraudulento, póngase en contacto de inmediato con su institución financiera.

Para obtener más información sobre seguridad informática y cómo proteger su información personal, visite el sitio web de la Comisión Federal de Comercio en www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm. Para más información sobre cómo evitar estafas de phishing, o para obtener un folleto con sugerencias sobre cómo evitar el robo de identidad, visite www.fdic.gov/consumers/theft/.

7. **Ejerza los derechos que le otorga la Ley de Transacciones de Crédito Justas y Precisas (Fair and Accurate Credit Transactions Act, FACTA) para revisar su informe crediticio y denunciar actividad fraudulenta.**

Su informe crediticio, que prepara una agencia de crédito, resume su historial de pago de deudas y otras facturas. Los informes de crédito son utilizados por prestamistas, empleadores y otras entidades que tienen la necesidad legal y legítima de la información. La ley FACTA le permite obtener un informe crediticio gratis cada año de cada una de las tres agencias de crédito más importantes que operan en todo el país – Equifax, Experian y TransUnion – con una sola llamada telefónica, carta o solicitud electrónica. Esto representa un cambio respecto a la ley anterior, porque puede obtener una copia aunque no sospeche de robo de identidad ni de ningún otro problema en su informe crediticio. (Vea más detalles en www.annualcreditreport.com, o llame al 877-322-8228.)

Después de obtener su informe crediticio, busque señales de advertencia de robo de identidad, real o potencial. Estas incluyen la mención de una tarjeta de crédito, préstamo o arrendamiento que usted nunca pidió y solicitudes de una copia de su informe crediticio de alguien que no reconoce (que podrían ser una señal de que un estafador está buscando información personal).

8. **Obtenga más información**

Visite el sitio web de la Comisión Federal de Comercio: www.ftc.gov/idtheft/, o llame al 877-IDTHEFT (438-4338)

¿Qué hacer si sospecha que es víctima del robo de identidad?

La FTC recomienda las siguientes medidas si usted cree que es víctima del robo de identidad. También puede llamar a la línea de robo de identidad de la FTC al 877-IDTHEFT (438-4338) o visite http://www.ftc.gov/idtheft/.