ROBO DE IDENTIDAD

El robo de identidad se produce cuando alguien usa su nombre, número del Seguro Social, número de cuenta, información del seguro u otra información que lo identifique para cometer un fraude u otros delitos. En esta era electrónica, se ha convertido en un riesgo demasiado común. Afortunadamente, hay muchas medidas de prevención que puede tomar para reducir de manera sustancial la posibilidad de que se produzca un robo de identidad y acciones que puede realizar para minimizar los daños si es víctima de un delito de este tipo.

Resultados comunes

Los ladrones utilizan una variedad de técnicas ilegales para procurar la información de la identidad. Podrían hacer lo siguiente:

- robar estados de cuenta u otro tipo de correo que contenga información personal de su buzón;
- desviar su correo a otro lugar al completar un formulario de cambio de dirección;
- buscar en la basura o en la papelera de reciclaje documentos que contengan información personal o financiera;
- robar su billetera o un dispositivo electrónico;
- falsear su identidad ante una compañía con la cual usted opera o que tiene información sobre usted (por ejemplo, acceder a su informe de crédito al hacerse pasar por su arrendador);
- ingresar ilegalmente a su computadora o la de una compañía con la que usted opere;
- acceder a la información que ingresa por Internet o envía por correo electrónico;
- hacerse pasar por una compañía legítima o un organismo gubernamental y solicitar información personal por teléfono ("vishing"), por correo electrónico ("phishing") o por mensaje de texto ("smishing");
- colocar un dispositivo en un cajero automático para capturar el número de tarjeta y el PIN; o
- aprovecharse de una relación personal que tengan con usted. (Por ejemplo, un "amigo" podría tomar un estado de cuenta de su cómoda mientras está ocupado).

Evaluación de riesgo de robo de identidad

¿Cuán segura está su información personal frente al robo de identidad? Para descubrirlo, responda *verdadero* o *falso* a las siguientes afirmaciones.

1. Destruyo todas las ofertas de créditos preaprobados, estados de cuenta y documentos financieros antes de arrojarlos a la basura.
2. No llevo conmigo mi tarjeta de Seguro Social.
3. Nunca dejo mi billetera o mis dispositivos electrónicos accidentalmente.
4. Cuando me voy de vacaciones, suspendo el envío de mi correo o le pido a alguien en quien confío que lo recoja todos los días por mí.
5. Reviso cada uno de mis informes de crédito todos los años.
6. No descargo archivos ni hago clic en los enlaces que me envían personas que no conozco.
7. Reviso mis estados de cuenta una vez al mes.
8. Siempre me cercioro de que la página sea segura antes de ingresar mi información personal por Internet.
9. Estoy consciente de todas mis fechas de vencimiento y sé de inmediato si falta una factura.
10. No llevo mi chequera conmigo a menos que planee usarla ese día.
11. Nunca doy mi información personal a menos que yo haya iniciado el contacto y sepa exactamente con quién estoy tratando.
12. Tengo un software antispyware y antivirus actualizado instalado en mi computadora.
13. No guardo información personal o financiera confidencial en mi computadora portátil o en mi dispositivo electrónico portátil.
14. Me aseguro de que no haya nadie cerca de mí cuando ingreso mi PIN.
15. Todas las contraseñas de mi cuenta son demasiado complicadas para que alguien las adivine.

CLAVE DE PUNTUACIÓN:
15 afirmaciones verdaderas: está lo más seguro que se puede estar.
5 a 14 afirmaciones verdaderas: está tomando muchas medidas positivas para protegerse, pero trabaje para convertir esas afirmaciones falsas en verdaderas.
0 a 4 afirmaciones verdaderas: podría estar exponiéndose a un riesgo innecesario de robo de identidad.

Resultados típicos
Después de que el ladrón de identidad tiene su información personal, podría usarla en una variedad de formas ilegales. Entre las prácticas comunes se incluyen:

- Hacer cambios en la cuenta de una tarjeta de crédito existente. Si el cajero no solicita identificación, lo único que el ladrón necesita hacer es falsificar su firma. Es todavía más fácil que use su cuenta cuando realiza compras telefónicas o por Internet.
- Abrir una nueva cuenta de tarjeta de crédito. Una vez que el ladrón tiene su información personal, puede abrir una cuenta a su nombre, pero hacer que le envíen la tarjeta y las facturas a él. El ladrón realiza las compras, pero la factura nunca llega a su casa. (Y por supuesto, el ladrón no paga por ellas). Es probable que no se entere del crimen hasta que un cobrador lo rastree, hasta que solicite un crédito y se lo rechacen, o hasta que pida una copia de su informe de crédito y vea la actividad.
- Sacar un crédito para comprar un auto u otros artículos costosos. Como sucede con las tarjetas de crédito, a menudo no sabrá sobre la actividad hasta que experimente algún tipo de acción de cobranza o crédito negativo.
- Usar una cuenta de cheques existente. El ladrón podría preparar cheques fraudulentos o usar su tarjeta de débito. Tener el PIN hace que sea fácil sacar efectivo del cajero automático, pero incluso sin él, el ladrón puede igualmente hacer compras por Internet, por teléfono o en una tienda al seleccionar la opción “crédito”.
- Obtener beneficios del gobierno o usar su seguro de atención médica. El ladrón podría solicitar cosas como beneficios del Seguro Social o cupones para alimentos con su identidad o hacerse pasar por usted y proporcionar la información de su seguro para pagar la atención médica.

Prevenir el robo de identidad
Tomar medidas en la actualidad para reducir las probabilidades de convertirse en víctima es mucho más fácil o consume menos tiempo que reparar los daños que causa un robo de identidad.

Revise su informe de crédito
Revise su informe de crédito de cada una de las tres agencias de crédito (Equifax, Experian y TransUnion) en busca de actividad fraudulenta al menos una vez al año. Puede recibir una copia gratuita de los tres informes una vez al año a través del Servicio de solicitud de informes de crédito anual. Ver página 5 para acceder a la información de contacto. Puede obtener los tres informes a la vez o pedir por separado sus solicitudes a lo largo del año. Si cree que fue víctima de robo de identidad, tiene derecho a informes gratuitos adicionales. (Para esto, comuníquese directamente con las agencias de crédito). Si en la actualidad no cumple con los requisitos para solicitar los informes gratuitos, puede comprarlos en las agencias de crédito mediante el pago de un cargo. Cuando obtenga sus informes, revíselos minuciosamente en busca de saldos que no parezcan correctos, cuentas que nunca haya abierto o cualquier otra cosa que parezca sospechosa. Impugne de inmediato la información incorrecta ante las agencias y comuníquese con los acreedores involucrados (se abordan en mayor detalle más adelante).

Proteja su información personal
Cuando alguien le pida su información personal, nunca dude en hacer preguntas o decir que no si no se siente cómodo. Solo debería proporcionar sus datos personales si sabe cómo se usarán, si está seguro de que la persona o la compañía son legítimas y si usted es el que ha iniciado el contacto.

Verifique sus estados de cuenta
Conozca sus ciclos de facturación y asegúrese de revisar sus estados de cuenta para las tarjetas de crédito, los servicios públicos, las cuentas de ahorros y de cheques y otras cuentas cuando se emitan. Si ve algún cambio que no autorizó, comuníquese con la compañía de inmediato. También comuníquese con ellos si no recibe su estado de cuenta cuando debería.

Minimice y proteja su correo
Intente reducir la cantidad de correo que recibe que contenga información confidencial. Muchas compañías de tarjetas de crédito, bancos, cooperativas de crédito, proveedores de servicios públicos y otras instituciones le permiten elegir si desea recibir los estados de cuenta solo por Internet. No obstante, como es probable que no pueda detener por completo el flujo de correo que contenga información personal, asegúrese de vaciar rápido su buzón y no dejar que el correo permanezca allí durante un día o dos. Si se va a ir de vacaciones y no hay nadie disponible para recoger su correo, puede solicitar la suspensión del envío de este durante las vacaciones en la oficina del correo.

Evite una falsa sensación de seguridad
Es fácil tener una sensación de seguridad en su hogar, en el trabajo, en su lugar de culto o en otro lugar que le sea familiar, pero recuerde que muchas personas se convierten en víctimas de alguien que conocen. (Y por supuesto, también podría haber extraños que pasen). Nunca deje su billetera, sus estados de cuenta o sus dispositivos electrónicos portátiles a la vista de todos.

Solo lleve consigo lo que necesita
Si le roban la billetera o la cartera, cuanto menos tenga dentro, menos información tendrá el ladrón. Casi nunca es necesario que lleve consigo su tarjeta del Seguro Social. La mayoría de las personas no necesitan cargar con sus chequeras tampoco.

Tenga cuidado al momento de desechar sus cosas
Si va desechar una declaración u otra cosa que contenga información personal, tritúrela; no la arroje simplemente a la basura. Haga lo mismo con las ofertas preaprobadas. Mejor aún, solicite que no se las envíen. (La información de contacto para hacer esto se encuentra en la página 5).

Proteja su computadora y su teléfono inteligente
Use un cortafuego y un software antivirus y antispyware para reducir la vulnerabilidad de su computadora frente a los piratas informáticos. Use una combinación compleja de números y letras mayúsculas y minúsculas para procurar que todas las contraseñas sean difíciles de adivinar.
Cierre sesión cuando salga de la habitación y no deje dispositivos portátiles sin supervisión. Antes de desechar su computadora o su teléfono inteligente, asegúrese de borrar la información personal utilizando un programa de "limpieza" para sobreescribir todo el disco duro.
Cuando realice compras por Internet, asegúrese de que la página sea segura. Ingrese su información personal y financiera solamente cuando haya un icono con un candado en la barra de estado de su navegador y busque la URL que diga "https" en lugar de "http".
No envíe información personal confidencial por correo electrónico ni descargue archivos o abra enlaces que le envíen personas que no conoce.

Considere (detenidamente) tener protección adicional
Si le preocupa demasiado la posibilidad de sufrir un robo de identidad, podría considerar pagar un seguro de robo de identidad o monitoreo de crédito, pero solo hágalo después de leer cuidadosamente la letra chica y considerar el costo frente al beneficio. Algunas de las empresas que ofrecen estos servicios son estafas en sí mismas. Investigue el historial de la compañía y verifique el registro de quejas del Better Business Bureau antes de contratarla.

- **Monitoreo de crédito.** Un servicio de monitoreo de crédito por lo general proporciona actualizaciones regulares del informe de crédito acerca de nuevas consultas, nuevas cuentas, pagos retrasados, cambios repentinos en los saldos de sus tarjetas de crédito y otras actividades posiblemente sospechosas. También podría acceder a su informe de crédito cuando lo desee sin costo adicional.
- **Seguro contra robo de identidad.** Si se convierte en víctima de un robo de identidad, este tipo de seguro le reembolsa los gastos de bolsillo que tenga para reparar los daños (pero no el dinero que le hayan robado) y le ayuda a lo largo del proceso de comunicarse con los acreedores, redactar declaraciones juradas y presentar denuncias.

Recuperarse de un robo de identidad
Si es víctima de un robo de identidad, ser proactivo puede minimizar el impacto que tenga en usted. Es probable que deba comunicarse con diferentes partes, entre ellas:

- **Acreedores e instituciones financieras.** Si se ha utilizado o abierto una cuenta de cheques o una tarjeta de crédito de forma ilegal, comuníquese con su acreedor o con su institución financiera de inmediato. Si la cuenta no es suya, debería cerrarse. Si es suya, debería obtener un nuevo número de cuenta y una tarjeta nueva. Supervise todos los estados de cuenta futuros minuciosamente en busca de evidencia de un nuevo fraude.
- **Agencias gubernamentales y legales.** Siempre debería denunciar los robos de identidad a la policía. Asegúrese de solicitar una copia de la denuncia policial oficial.
  Una agencia de crédito o un acreedor podrían solicitársela como parte de su investigación del fraude. También puede presentar un reclamo ante la Comisión Federal de Comercio, aunque no asisten en los casos individuales. Debería comunicarse con el Servicio de Inspección Postal de los Estados Unidos si le han robado su correo o han utilizado su dirección de forma fraudulenta. (La información de contacto se encuentra en la página 5).
- **Agencias de informes de crédito.** Verifique su informe de crédito de las tres agencias. (Recuerde que tiene derecho a informes gratuitos adicionales si cree que es víctima de robo de identidad). Impugne todos los elementos fraudulentos mediante la presentación de un formulario por Internet o del envío por correo de una carta a las agencias de crédito. Tienen la obligación de investigar y responder dentro de los 30 días (45 días si el informe se obtuvo a través del Servicio de solicitud de informe de crédito anual).

Aunque la información fraudulenta no haya aparecido en sus informes, sea proactivo y denuncie ahora el delito ante las agencias de crédito. Es buena idea hacer que se eleve una alerta de fraude sobre sus informes de crédito. Cuando alguien solicita un crédito con su nombre, al acreedor se le exige que verifique que la persona que lo solicita es usted. La alerta inicial de fraude solo dura 90 días. No obstante, si presenta una denuncia policial, puede ampliar la alerta hasta siete años. También puede elevar una alerta de un año en su registro si presta servicio activo en el ejército.

Si cree que una alerta de fraude no le proporcionará suficiente protección, puede realizar un congelamiento de seguridad de su informe de crédito. Cuando se realiza un congelamiento en su informe, ningún acreedor u otra empresa que no tenga una relación preexistente con usted podrán acceder a su informe sin su permiso. Dado que la mayoría de los acreedores no otorgarán un crédito sin verificar su informe primero, esto hace que para el ladrón sea extremadamente difícil obtener un crédito a su nombre. Si desea solicitar un crédito usted mismo (o alquilar un apartamento o hacer otra cosa que requiera una verificación de crédito) puede levantar el congelamiento, ya sea de forma temporal o permanente. Recuerde que esto podría demorar el proceso de solicitud. Dado que es probable que hable con muchas personas durante el proceso de recuperación, es vital que se organice.

Guarde copias de todas las cartas, presente la documentación con prontitud y guarde todo en un lugar seguro y accesible. Puede usar el Registro de acciones ante robo de identidad (en las páginas 6 a 9) como ayuda para realizar un seguimiento de lo que ha hecho.

Leyes federales
Hay muchas leyes federales que son de ayuda en la lucha contra el robo de identidad.

Ley de Informe Imparcial de Crédito (FCRA, por su sigla en inglés)

- Si se le deniega un crédito, seguro o empleo debido al contenido de su informe de crédito, puede obtener un informe gratuito de la agencia que lo proporcionó dentro de los 60 días siguientes a la denegación.
- Tiene derecho a impugnar la información incorrecta de su informe de crédito. Las agencias de crédito deben investigar la validez de los elementos impugnados dentro de los 30 días (a menos que, como se indicó anteriormente, el informe se obtenga a través del Servicio de solicitud de informe de crédito anual).
- La información negativa que esté desactualizada o que no se pueda verificar no se puede informar.
- Solo aquellos con una necesidad reconocida por la FCRA (por lo general, acreedor, aseguradora, empleador, arrendador u otra empresa que esté evaluando una solicitud suya) pueden acceder a su registro.

Ley de Transacciones de Crédito Imparciales y Exactas (FACT, por su sigla en inglés)

- Puede recibir una copia gratuita de su informe de crédito de cada una de las tres agencias de crédito una vez por año.
- Puede recibir informes gratuitos adicionales si hay sospechas de robo de identidad.
- Puede bloquear la información fraudulenta para que no aparezca en su informe de crédito.
- Tiene derecho a acceder a los registros de negocio, tales como las solicitudes de crédito, que documentan las transacciones fraudulentas del ladrón de identidad.
- Tiene derecho a elevar una alerta de fraude en su informe de crédito si cree que ha sido víctima de robo de identidad. Los acreedores deben asegurarse de que todas las solicitudes de crédito sean legítimas después de que se haya elevado una alerta sobre un informe de crédito.
- El personal en servicio militar activo puede elevar una alerta especial en sus registros cuando estén desplegados en el exterior.
- Los recibos de las tiendas solo pueden contener hasta cinco dígitos del número de la tarjeta de crédito. La fecha de vencimiento de la tarjeta tampoco se puede indicar.
- Los acreedores deben implementar programas de prevención de robo de identidad.
- Los cobradores de deudas deben informar a los acreedores acerca de la información fraudulenta.

Ley de Facturación Imparcial de Crédito (FCBA, por su sigla en inglés)

- La responsabilidad por la pérdida o el robo de una tarjeta de crédito se limita a $50 si notifica al emisor de la tarjeta dentro de los 30 días posteriores.
- Si hay un error en una factura de tarjeta de crédito, el prestamista debe corregirlo o explicar por qué se cree que el monto es correcto dentro de los 90 días posteriores a la recepción de la notificación. (Debe enviar la notificación dentro de los 60 días posteriores a la fecha en la cual se le envió la factura que incluía el error).

Ley de Transferencias Electrónicas de Fondos

- La responsabilidad máxima por la pérdida o el robo de una tarjeta de débito o de cajero automático es:
  - $50 si lo denuncia dentro de los dos días hábiles posteriores al momento en que tomó conocimiento de la pérdida o el robo de la tarjeta.
  - $500 si lo denuncia después de dos días hábiles pero dentro de los siguientes 60 días.
  - No hay límite si espera más de 60 días. Puede perder todo el dinero en su cuenta además de su línea de crédito con protección contra sobregiro máximo, si corresponde.
  - Muchas instituciones financieras proporcionan protecciones mayores a las que exige la ley.
- Tiene 60 días para impugnar un error en un estado de cuenta de ahorros o de cheques. La institución financiera debe responder dentro de los 45 días (en la mayoría de los casos). Todos los fondos impugnados deben devolverse a su cuenta dentro de los 10 días hábiles siguientes.

Si un acreedor o una agencia de crédito infringen alguna de estas leyes, puede presentar un reclamo ante la oficina del fiscal general de su estado y ante la Comisión Federal de Comercio. Las infracciones que involucren una cuenta de ahorro o cheques se pueden denunciar ante la Oficina del Contralor de la Moneda para los bancos nacionales, el Directorio de la Reserva Federal para los bancos estatales que responden a esta, la Corporación Federal de Seguros de Depósito para otros bancos, la Administración Nacional de Cooperativas de Crédito para las cooperativas de crédito federales y la junta estatal de supervisión financiera para las cooperativas de crédito estatales.

RECURSOS ÚTILES

Dado que la información de contacto puede cambiar cada cierto tiempo, confirme las direcciones antes de enviar una carta que contenga información personal.

Agencias de informes de crédito

- Equifax
  Para solicitar un informe de crédito: 800.685.1111
  Para denunciar un fraude: 800.525.6285
  PO Box 740241, Atlanta, GA 30374
  www.equifax.com

- Experian
  888.397.3742
  PO Box 2104, Allen, TX 75013
  www.experian.com

- TransUnion
  Para solicitar un informe de crédito: 800.888.4213
  Para denunciar un fraude: 800.680.7289
  PO Box 2000, Chester, PA 19022
  www.transunion.com

- Servicio de solicitud de informe de crédito anual (Annual Credit Report Request Service)
  877.322.8228
  PO Box 105281, Atlanta, GA 30348
  www.annualcreditreport.com

Agencias gubernamentales

- Asociación Nacional de Fiscales Generales
  www.naag.org

- Comisión Federal de Comercio
  877.438.4338
  600 Pennsylvania Avenue NW
  Washington, DC 20580
  www.ftccomplaintassistant.gov

- Servicio de Inspección Postal de los Estados Unidos
  877.876.2455
  Centro de Servicio de Investigaciones Criminales (Criminal Investigations Service Center)
  Dirigido a: Mail Fraud
  222 S Riverside Plaza, Ste 1250
  Chicago, IL 60606
  www.postalinspectors.uspis.gov

Organismos de control bancario

- Oficina del Contralor de la Moneda (bancos nacionales)
  800.613.6743
  1301 McKinney St., Ste 3450, Houston, TX 77010
  www.occ.treas.gov

- Directorio de la Reserva Federal (bancos estatales)
  888.851.1920
  PO Box 1200
  Minneapolis, MN 55480
  www.federalreserve.gov

- Corporación Federal de Seguros de Depósito (Federal Deposit Insurance Corporation) (otros bancos)
  703.812.1020
  2345 Grand Blvd., Suite 100
  Kansas City, MO 64108
  www.fdic.gov

- Administración Nacional de Cooperativas de Crédito (National Credit Union Administration)
  800.755.1030
  1775 Duke Street, Alexandria, VA 22314-3428
  www.ncua.gov

Servicios de monitoreo y verificación de cuentas de cheques

- ChexSystems
  800.428.9623
  7805 Hudson Rd, Suite 100, Woodbury, MN 55125
  www.consumerdebit.com

- TeleCheck
  800.710.9898
  PO Box 4451, Houston, TX 77210
  www.telecheck.com

Otros

- Better Business Bureau
  www.bbb.org

- Para solicitar que no le envíen ofertas de créditos preaprobados:
  888.567.8688
  www.optoutprescreen.com

Institución financiera n.º 1

Acción	Sí/No	Fecha	Persona de contacto	Notas (teléfono, correo electrónico, extensión, etc.)
Detener los pagos				
Denunciar fraude de cheques				
Cancelar cuentas				
Cambiar números de cuentas y contraseñas				

Institución financiera n.º 2

Acción	Sí/No	Fecha	Persona de contacto	Notas (teléfono, correo electrónico, extensión, etc.)
Detener los pagos				
Denunciar fraude de cheques				
Cancelar cuentas				
Cambiar números de cuentas y contraseñas				

Institución financiera n.º 3

Acción	Sí/No	Fecha	Persona de contacto	Notas (teléfono, correo electrónico, extensión, etc.)
Detener los pagos				
Denunciar fraude de cheques				
Cancelar cuentas				
Cambiar números de cuentas y contraseñas				

Cuenta de crédito n.º 1

Acción	Sí/No	Fecha	Persona de contacto	Notas (teléfono, correo electrónico, extensión, etc.)
Denunciar fraude				
Enviar declaración jurada				
Cambiar números de cuentas y contraseñas				

Cuenta de crédito n.º 2

Acción	Sí/No	Fecha	Persona de contacto	Notas (teléfono, correo electrónico, extensión, etc.)
Denunciar fraude				
Enviar declaración jurada				
Cambiar números de cuentas y contraseñas				

Cuenta de crédito n.º 3

Acción	Sí/No	Fecha	Persona de contacto	Notas (teléfono, correo electrónico, extensión, etc.)
Denunciar fraude				
Enviar declaración jurada				
Cambiar números de cuentas y contraseñas				

Cuenta de crédito n.º 4

Acción	Sí/No	Fecha	Persona de contacto	Notas (teléfono, correo electrónico, extensión, etc.)
Denunciar fraude				
Enviar declaración jurada				
Cambiar números de cuentas y contraseñas				

Cuenta de crédito n.º 5

Acción	Sí/No	Fecha	Persona de contacto	Notas (teléfono, correo electrónico, extensión, etc.)
Denunciar fraude				
Enviar declaración jurada				
Cambiar números de cuentas y contraseñas				

Cuenta de crédito n.º 6

Acción	Sí/No	Fecha	Persona de contacto	Notas (teléfono, correo electrónico, extensión, etc.)
Denunciar fraude				
Enviar declaración jurada				
Cambiar números de cuentas y contraseñas				

Agencias de crédito

Agencia	Acción	Sí/No	Fecha	Persona de contacto	Notas (teléfono, correo electrónico, extensión, etc.)
Equifax	Obtener informe				
	Alerta de fraude				
Experian	Obtener informe				
	Alerta de fraude				
TransUnion	Obtener informe				
	Alerta de fraude				

Agencias gubernamentales

Agencia	Acción	Sí/No	Fecha	Persona de contacto	Notas (teléfono, correo electrónico, extensión, etc.)
Departamento de policía	Denunciar delito				
	Presentar denuncia				
Fiscal general del estado	Presentar denuncia				
USPIS	Denunciar delito				
	Presentar denuncia				
DMV	Denunciar delito				
	Presentar denuncia				

Otros contactos

Organización	Persona de contacto	Fecha	Notas (teléfono, correo electrónico, extensión, etc.)

Notas adicionales