



Lo que debe saber sobre...

# Robo de identidad

- ▶ **CÓMO SUCEDE EL ROBO DE IDENTIDAD**
- ▶ **CÓMO PROTEGERSE**
- ▶ **CÓMO RECUPERARSE DE UN ROBO DE IDENTIDAD**



Usted puede haber escuchado de un crimen llamado robo de identidad, pero probablemente no esté seguro exactamente qué es, o cómo puede protegerse contra dicho crimen. Si bien el robo de identidad sucede mayormente en papel, es decir, alguien utiliza su información personal para obtener crédito en su nombre, engañar a la policía, cometer fraude con impuestos, etc., el impacto que tiene en su vida financiera es bastante real.

Hay una serie de cosas que usted puede hacer para protegerse contra el robo de identidad. Comprender el valor de su información personal, incluyendo el número de seguro social y la información de la cuenta de crédito, es el primer paso para protegerse a sí mismo. Y si, a pesar de todos sus esfuerzos, tiene un problema de robo de identidad, hay pasos que puede tomar para reparar el daño.

© 2005, HSBC Finance Corporation. Reservados todos los derechos.

Declaración informativa: Este contenido ha sido desarrollado y redactado exclusivamente como material educativo, y no pretende ser una solicitud de préstamo, producto financiero u otro servicio. Estos materiales no representan una recomendación por parte de HSBC para la compra de ningún producto, servicio o estrategia financiera y están sujetos a cambios sin previo aviso. Además, las sugerencias y recomendaciones incluidas en el material proporcionado no constituyen ninguna garantía de resultados en el futuro. Si usted necesita obtener asistencia adicional, HSBC le sugiere consultar a un abogado independiente, profesional en impuestos o asesor financiero.

# ¿Qué es el robo de identidad?

Si alguien le roba a usted su identidad, puede no darse cuenta que ha sucedido. Pero los efectos pueden ser serios. El robo de identidad ocurre cuando su información personal, tal como su nombre, número de cuenta, o número de seguro social (SSN, por sus siglas en inglés) se usan sin su conocimiento para cometer un fraude o robo. Armados con la información personal de usted, los ladrones pueden realizar compras no autorizadas utilizando sus tarjetas de crédito, solicitar nuevas tarjetas de crédito y préstamos, cobrar cheques sin fondos, arrendar automóviles, o engañar a la autoridad, causando serios daños a su historial de crédito.

Si bien usted probablemente no será responsable por cargos fraudulentos, el limpiar su nombre e historial de crédito puede ser un proceso largo, frustrante y que demanda tiempo. En los casos más serios, podría tomar meses o aún años completarlo, y durante dicho tiempo le será más difícil conseguir un préstamo, alquilar un departamento o ser contratado para un trabajo. Como con muchos crímenes, el impacto puede ser tanto emocional como financiero.

Existen dos métodos de robo de identidad:

1. El tipo más común de robo de identidad es cuando alguien utiliza tarjetas de crédito, tarjetas de débito, cheques o información de cuentas que ha robado para realizar compras o retiros de dinero de las cuentas. Probablemente usted detectará este tipo de robo cuando aparezcan cargos que no autorizó en su estado de cuenta de tarjeta de crédito o cuando se agoten las cuentas bancarias o de valores.
2. Con menos frecuencia, pero más peligroso, alguien puede abrir nuevas cuentas en su nombre utilizando su dirección, un número de seguro social robado, u otras formas de identificación personal, y realizar compras u obtener crédito en su nombre. Y si utilizan una dirección postal diferente, usted probablemente ni siquiera se percatará que existen las cuentas fraudulentas hasta que le rechacen crédito o revise su informe de crédito.



## ¿Quién es responsable?

La ley federal limita la responsabilidad a \$50 si alguien roba y utiliza su tarjeta de crédito. Algunos bancos ni siquiera lo hacen a usted responsable de compras fraudulentas utilizando su tarjeta, de manera que infórmese acerca de la política de su banco. Las reglas son un poco diferentes si un ladrón utiliza su tarjeta de débito o de cajero automático (ATM, por sus siglas en inglés). Usted puede limitar su pérdida a \$50, pero debe informar sobre las transacciones no autorizadas a su banco en un plazo de dos días después de descubrirlas. Si se demora más de dos días, puede perder hasta \$500, y posiblemente el monto total que fue debitado a su cuenta.

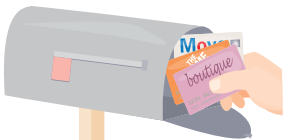
## ¿Cómo protegerse?

Una manera de reducir el riesgo de robo de identidad es aprendiendo algunos de los métodos que los ladrones utilizan para robar información personal.



### Obtener información acerca de usted sin su conocimiento

- Robar del correo, o buscar en la basura, estados de cuenta bancarios o resúmenes de cuentas de correaje, nuevos cheques u

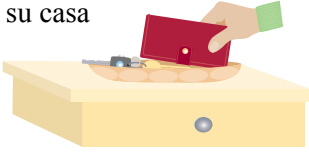


ofertas de tarjetas de crédito aprobadas por anticipado (“dumpster diving” en inglés)

- Robar archivos de personal y clientes en oficinas comerciales, incluyendo las de su empleador



- Robar la billetera o cartera, o los documentos personales de su casa



- Robar los números de tarjeta de crédito y débito cuando la tarjeta se pasa por la máquina procesadora (“skimming” en inglés)
- Mirar por encima de su hombro cuando está en el cajero automático para obtener el número de identificación personal (PIN, por sus siglas en inglés)



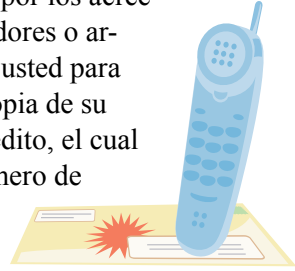
Por estas y otras razones, es una buena idea guardar los documentos financieros en un lugar seguro en la casa, y proteger los recibos y estados de cuenta. También es conveniente comprar una trituradora de papel para destruir documentos importantes cuando ya no los necesite.

## Obtener información acerca de usted de otras fuentes

- Llenar un formulario de cambio de dirección para que

ellos reciban correo dirigido a usted, incluyendo estados de cuenta de tarjeta de crédito para cuentas que ellos abrieron pero que no tienen ninguna intención de pagar

- Hacerse pasar por los acreedores, empleadores o arrendadores de usted para obtener una copia de su informe de crédito, el cual incluye su número de seguro social



- Obtener la información personal de usted a través de esquemas falsos de mercadeo por teléfono, correo, o correo electrónico (“phishing” en inglés)

- Utilizar tecnología avanzada para romper la seguridad en línea y robar la información de la cuenta



Usted debería ser muy cauteloso al dar su información personal a menos que esté seguro que la situación es legítima. Ninguna institución financiera legítima le pedirá que confirme su número de cuenta o dé su número de seguro social por teléfono o en línea durante una llamada o comunicación que usted no inició.

# Medidas preventivas

Puede sorprenderle de cuántas maneras las personas tratan de robar la información personal. La buena noticia es que hay maneras de protegerse. Si bien seguir estas sugerencias no garantizarán que pueda evitar el robo de identidad, le ayudarán a minimizar la probabilidad de convertirse en una víctima o evitar el daño ocasionado en caso suceda.

## Tarjetas de crédito y cuentas de crédito

1. Nunca coloque su número de identificación personal (PIN, por sus siglas en inglés) en las tarjetas de crédito o tarjetas de débito.
2. Sólo lleve consigo las tarjetas, cheques y formas de identificación que sean absolutamente necesarias. Mantenga las otras, como la tarjeta del seguro social y tarjetas de crédito poco utilizadas, en un lugar seguro en la casa.
3. Mantenga una lista de todas las tarjetas de crédito y sus números de telé-

## Documentar registros

Usted puede pensar que la mayoría de los crímenes de identidad se cometen en línea. Pero la FTC reporta que sólo alrededor del 20% de los casos tienen que ver con telecomunicaciones y la Internet. Según el Informe de la Encuesta sobre Fraude de Identidad del 2005 de la Better Business Bureau (Agencia de Buenas Prácticas de Negocios), el 68% de los casos de robo de identidad se cometieron con información obtenida fuera de línea. Aún más sorprendente es que en la mitad de los casos en que el ladrón de identidad fue capturado, el crimen fue cometido contra una persona que el ladrón conocía o con la cual estaba relacionado

fono de servicio al cliente en un lugar seguro en la casa. De esa manera, puede comunicarse con las compañías de la tarjeta u otros prestamistas inmediatamente con la información



necesaria si le roban o se pierde la tarjeta.

4. Revise las cuentas bancarias y los estados de la tarjetas de crédito cuidadosamente y con regularidad para ver si hay señales de transacciones que usted no hizo. Es una buena idea guardar todos los recibos y compararlos con el estado de cuenta mensual impreso o en línea.

### **Documentos de identidad, estados de cuenta e informe de crédito**

1. Guarde la identificación personal, el certificado de nacimiento, la tarjeta de seguro social y el pasaporte, en un lugar seguro en casa, especialmente si tiene personas que hacen trabajo de servicio en la casa. Considere guardar los documentos en un lugar con llave y candado.
2. Revise el informe de crédito por lo menos dos veces al año o más frecuentemente.
3. Triture los recibos y documentos financieros antes de arrojarlos a la basura. La ley FACT requiere que para el año 2007, los comerciantes impriman

en los recibos sólo los últimos cinco dígitos del número de cuenta del cliente en lugar del número completo de la cuenta.

4. Solicite que el número de seguro social no se utilice como número de cuenta ni para tarjetas de identidad de cliente, empleado o estudiante.
5. No deje el correo en el buzón para que lo recoja el cartero, ya que pueden robarlo. En lugar de ello, lleve las cartas a la oficina postal o colóquelas en los buzones oficiales. Por la misma razón, asegúrese también de recoger oportunamente el correo del buzón.
6. No hable sobre asuntos privados y financieros que requieran divulgar el número de seguro social, números de cuentas o contraseñas cuando esté utilizando el teléfono celular o inalámbrico, ya que tales llamadas pueden ser interceptadas o escuchadas por potenciales ladrones. En lugar de ello, utilice un teléfono con línea de tierra.
7. Si está considerando hacer una donación a una institución de caridad, solicite documentación por escrito primero y verifique las credenciales de la organización.



# La protección de su persona cuando está en línea

Puede no percatarse, pero su información personal probablemente está almacenada en la computadora de la casa y del trabajo. Y si paga las cuentas o compra en línea, algunas veces necesita proporcionar información personal. Si bien algunos expertos piensan que la información está más segura en línea que en ningún otro lugar, sigue siendo una buena idea tomar algunas precauciones.

- 1 Nunca proporcione su información de contacto, código de ingreso, contraseña o información importante a través del correo electrónico. Puede recibir correo electrónico falso que se presenta como negocio legítimo, quizás su propio banco, y solicitar dicha información. Este engaño se conoce como “phishing” en inglés.
- 2 Considere utilizar una tarjeta de crédito con la característica de seguridad llamada Número de Cuenta Virtual que genera un número de cuenta diferente cada vez que usted realiza una compra en línea.



3. Busque el icono de un candado o una llave en la parte inferior derecha de la ventana del buscador para asegurarse que está en una página segura, lo cual significa que cualquier información personal que proporcione será codificada durante la transacción. Algunos ladrones sofisticados han podido reproducir dichas imágenes, pero haciendo doble clic en el icono del candado, puede asegurarse que el URL en el certificado es igual al URL de la página en la que se encuen-



## La ley FACT

La Ley de Transacciones de Crédito Equitativas y Precisas (Ley FACT, por sus siglas en inglés), le otorga el derecho de solicitar un informe de crédito gratis de cada una de las tres agencias de informes crediticios, Equifax, Experian y TransUnion, una vez al año. Para solicitar el informe en línea, visite: [www.annualcreditreport.com](http://www.annualcreditreport.com), o llame al 1-877-322-8228.

tra. Si los URL no son iguales, probablemente sea un engaño.

4. Asegúrese de tener software antivirus actualizado instalado en la computadora así como una “firewall” (barrera protectora), especialmente si tiene conexión de Internet de alta velocidad que se mantiene conectada a la Internet las 24 horas del día. La mayoría de programas le notificarán si hay actualizaciones disponibles, pero usted mismo

## Lo que dice la FTC

Para conocer más acerca de “phishing”, revise este artículo de la Federal Trade Commission (Comisión Federal de Comercio)  
[www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.pdf](http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.pdf)

también puede revisar si están disponibles visitando el sitio web de la compañía.

## Qué hacer si usted es una víctima

Aun si ha tenido cuidado especial para proteger su información personal, usted puede ser víctima del robo de identidad. Si ello sucede, hay cuatros pasos que debería seguir inmediatamente para reparar su nombre y crédito. Recuerde, mientras más rápido responda mayor es la probabilidad de minimizar el daño.

**Paso 1:** Comuníquese con una de las tres agencias de informes crediticios y coloque una **alerta de fraude** en su informe. Esta agencia luego está obligada a notificar a las otras dos agencias para que también

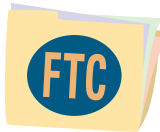
marquen el informe. Esta alerta de fraude es efectiva por 90 días. Puede extenderse hasta 7 años si usted proporciona un informe de robo de identidad, siempre que haya sido registrado en la estación de policía local. Los acreedores potenciales podrán de esta manera confirmar con usted las solicitudes de crédito antes de otorgarlas. Si usted piensa que su correo ha sido violado, proporcione también su número de teléfono. Después que la agencia de informes crediticios confirma la alerta de fraude, las otras dos agencias serán notificadas automáticamente y también colocarán alertas en el informe. Usted puede solicitar una copia gratis del informe reciente de cada agencia. Revise cuidadosamente el informe para ver si se abrieron cuentas no autorizadas y qué cargos no fueron pagados.





**Paso 2:** Presente un informe policial. La mayoría de acreedores requerirá uno cuando usted se comunique con ellos para limpiar su crédito. Si usted no puede obtener una copia del informe, consiga el número del informe.

**Paso 3:** Comuníquese con todas las compañías con las que tiene cuentas de crédito y cierre aquellas que fueron usadas indebidamente o abiertas sin su autorización. Las cuentas de crédito incluyen aquellas con compañías de tarjeta de crédito, bancos, compañías de teléfonos, compañías de teléfonos celulares, proveedores de servicio de Internet (ISP, siglas en inglés), compañías de servicios públicos y otros proveedores de servicios.



**Paso 4:** Presente una queja a la FTC. Una vez que lo haya hecho, la información de usted se ingresará en la base de datos segura de la FTC y ayudará a los agentes a rastrear a los ladrones. Además, si no pudo obtener una copia del informe policial, puede utilizar el Affidávit de Robo de Identidad de la FTC, el cual es un formulario estándar de cinco páginas aceptado por la mayoría de compañías en el que se describen incidentes de robo de identidad.

## Dónde informar sobre un fraude

Ya que es importante actuar rápidamente, es una buena idea tener toda la información de contacto necesaria para el momento que usted la necesite.

### Las tres agencias de informes crediticios más importantes

#### Equifax

Para informar sobre fraude, llame al 1-800-525-6285, y escriba a: P.O. Box 740241  
Atlanta, GA 30374-0241  
[www.equifax.com](http://www.equifax.com)

#### Experian

Para informar sobre fraude, llame al 1-800-EXPERIAN (397-3742), y escriba a: P.O. Box 9532  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

#### TransUnion

Para informar sobre fraude, llame al 1-800-680-7289, y escriba a: Fraud Victim Assistance Division  
P.O. Box 6790  
Fullerton, CA 92834-6790  
[www.transunion.com](http://www.transunion.com)

### Federal Trade Commission (Comisión Federal de Comercio)

Para llamar a la línea directa de Robo de Identidad de la FTC, llame al 1-877-IDTHEFT (438-4338), y escriba a: Identity Theft Clearinghouse  
Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

Para presentar un informe en línea a la FTC, visite:  
<http://www.consumer.gov/idtheft/>

Para obtener una copia del Affidávit de Robo de Identidad de la FTC visite:  
[www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf](http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf)

### **Administración del Seguro Social**

Para informar sobre un número de seguro social robado o utilizado indebidamente, llame al 1-800-269-0271  
[www.ssa.gov](http://www.ssa.gov)

### **Compañías de verificación de cheques**

Si le han robado los cheques, es una buena idea notificarlo a las principales compañías de verificación de cheques siguientes:

TeleCheck  
1-800-710-9898

Certegy, Inc.  
1-800-437-5120

International Check Services  
1-800-366-5010

ChexSystems  
1-800-428-9623

### **Engaños y alertas**

Para obtener actualizaciones recientes sobre engaños y alertas al consumidor, visite los siguientes sitios web:

La página de Robo de Identidad de la FTC: <http://www.consumer.gov/idtheft/index.html>

El Centro de Recursos para Robo de Identidad: <http://www.idtheft-center.org/index.shtml>

### **Haga clic aquí para obtener consejos sobre cómo organizar su caso de robo de identidad**

- Después de llamar por teléfono, comuníquese por escrito. Al enviar las cartas, utilice correo certificado y solicite confirmación de recepción. También tome notas detalladas de todas las conversaciones, incluyendo fechas, horas, nombre de la persona con la que habló, etc.
- Guarde copias de todas las cartas y formularios que envió por correo. Si es posible, guarde los originales de la documentación de apoyo, tales como el informe policial y cartas enviadas a los acreedores y recibidas de ellos. Envíe solamente copias.
- Cree un sistema de archivo para guardar toda la documentación.
- Guarde todos los archivos, aun hasta después de resolver el caso. Pueden surgir problemas nuevamente y, de ser así, usted estará preparado.

**C**omo una de las principales compañías de servicios financieros del mundo, HSBC es un comprometido defensor de la educación financiera. Nuestro objetivo es ayudar a que los consumidores conozcan los conceptos financieros, así como las herramientas necesarias para tomar decisiones financieras inteligentes. El programa **YourMoneyCounts**<sup>®</sup>, administrado por el Center for Consumer Advocacy (Centro para el Apoyo del Consumidor) de HSBC, promueve nuestro antiguo compromiso de proporcionar educación financiera, el cual se inició el año 1929 con la fundación del Money Management Institute (Instituto para la Administración del Dinero). Ya que sabemos que las personas escogen distintos medios para aprender, le ofrecemos el programa **YourMoneyCounts** a través de múltiples canales: en línea, en material impreso y mediante talleres de educación financiera.

Visítenos en [YourMoneyCounts.com](http://YourMoneyCounts.com)

HSBC - North America patrocina y administra **YourMoneyCounts**  
**YourMoneyCounts** ha sido creado en conjunción con Lightbulb Press<sup>®</sup>

