



ParentPapers: Protege tu identidad

Última actualización: 17/08/2007

Última traducción: 20/09/2007

<http://www.secureparents.com>

Bienvenido a SecureParents, un sitio web gratuito dedicado a vosotros, los padres ocupados. Estamos dedicados a ayudaros, sin ningún coste, para protegeros a vosotros y a vuestra familia en la actual era de la información. Entendemos la tremenda presión y limitaciones de tiempo que tienen los padres, por eso nuestros recursos están creados por expertos para ser sencillos y proporcionar la información que necesitáis conocer. ParentPapers son una serie de documentos diseñados para proporcionaros esta información en menos de 15 minutos.

SINOPSIS:

En este artículo discutimos sobre cómo proteger uno de tus activos más íntimos y más importantes, tu identidad.

La información contenida en este documento aplica a cualquier país aunque contiene ejemplos que se refieren a los Estados Unidos.

Este documento es copyright de "SecureParents". Te animamos a distribuir libremente este documento a quién consideres oportuno. La única limitación es que este documento no puede ser modificado ni vendido con propósito comercial. Este documento se distribuye bajo la licencia "Creative Commons", "Attribution-NonCommercial-NoDerivs 3.0 Unported". Bajo ningún supuesto SecureParents será responsable de los daños, incluyendo pérdida de datos, pérdidas económicas, coberturas, o cualquier otro daño especial, fortuito, accidental, directo o indirecto, derivado de esta documentación o consecuencia de su uso, con independencia de cómo se produzca. Esta limitación aplicará incluso en el caso en el que SecureParents haya sido advertido de la posibilidad de dichos daños. Leyendo este documento aceptas la existencia de estos riesgos.

Tu identidad

La Comisión Federal de Comercio (Federal Trade Comision, FTC) de los Estados Unidos, como la agencia nacional de protección al consumidor, es una de las principales organizaciones del gobierno que luchan contra los robos de identidad. Ellos definen robo de identidad como

“un robo de identidad ocurre cuando alguien utiliza la información que te identifica personalmente, como tu nombre, número de la Seguridad Social o número de la tarjeta de crédito, sin tu permiso, para cometer fraude u otros crímenes.”

Son diversos los tipos de información que ayudan a componer tu identidad. Por ejemplo, tu identidad incluye tu nombre y dirección, el número de la Seguridad Social, el número del carné de conducir, el número de la tarjeta de crédito, el número de cuenta bancaria o incluso tus tarjetas de fidelización. Básicamente, cualquier información que ayude a identificarte. Cuanta más información recoja un criminal sobre ti, más cosas puede hacer con ella y más valor tiene.

La cantidad de formas en las que los criminales pueden utilizar tu información es enorme. Los ejemplos incluyen usar tu identidad robada para pedir una tarjeta de crédito nueva, copiar tu tarjeta de crédito, crear cheques falsificados, conseguir subvenciones estatales, alquilar una casa o cometer crímenes usando tu nombre. El resultado final es que el criminal se beneficia, pero tú pagas por él. Conozcamos algunas de las medidas que podemos tomar para proteger nuestra identidad.

La protección de tu identidad

En la era digital en la que vivimos tu información se recoge y se almacena en ordenadores distribuidos por el mundo. Se almacena en bases de datos en tu antiguo colegio, en las tiendas en las que compras, en recopilaciones de datos o incluso en la librería o el ayuntamiento. En cualquier caso no puedes proteger tu información porque simplemente no la controlas. Sin embargo, hay algunas medidas que puedes tomar para protegerte.

1. Proteger tu propio ordenador para que los criminales no puedan acceder ilegalmente ni robar la información de tus sistemas mientras que estás conectado a Internet. Para más información lee nuestro ParentPaper: “Diez pasos para proteger tus ordenadores de casa”.
2. No dar tu información. Darla solamente a las organizaciones o a los individuos que confías en y solamente cuando inicias comunicación con ellos. Si alguien te llama o se pone en contacto contigo por correo electrónico pidiéndote que le des información tuya, no se la des a menos que hayas iniciado tú la comunicación con esa persona. Si dudas, pide a la persona su nombre y número de teléfono y dile que le devuelves la llamada.
3. Destruir cualquier información impresa identificable antes de tirarla a la basura.
4. No envíes por correo electrónico tu información privada (como tu DNI o número de la Seguridad Social). Si una organización de confianza tiene una necesidad legítima de conseguir información tuya, dale estos datos

por teléfono. El correo electrónico es inseguro. No sólo podría interceptar alguien la comunicación, sino que después tus datos residen en el sistema de esa persona o de la organización, posiblemente durante años.

5. Si vives en los Estados Unidos y no deseas recibir ofertas de crédito preaprobadas, la llamada 1-888-5-OPT-OUT (1-888-567-8688) para quitarte de las listas de las principales entidades de crédito.

Detectar los robos de identidad

Puesto que de muchas maneras no controlas tu propia información, la mejor manera de protegerse contra los robos de identidad es detectarla cuanto antes. Si detectas el robo de identidad justo después de que suceda, tienes más probabilidades de suavizar el daño. Sin embargo, si lo detectas meses después de que suceda el robo de identidad, el daño será mucho mayor y requerirá mucho más trabajo e implicará más coste el conseguir recuperarse. A continuación hay seis formas simples para detectar si te han robado tu identidad. Esta lista está basada en la del sitio web de la FTC.

1. Cargos en tus tarjetas de crédito o los apuntes en los extractos de tus cuentas bancarias que no puedas explicar. La manera más fácil de detectar esta actividad es comprobar tus informes de la tarjeta de crédito y de la cuenta cada mes.
2. Presencia de información fraudulenta o inexacta en tus informes de riesgo crediticio, incluyendo cuentas e información personal, como tu número de Seguridad Social, dirección, nombre o iniciales y empresas para las que trabajas. La manera más fácil de detectar esto es mediante la supervisión del informe de crédito. Para más información sobre informes de crédito puedes leer el ParentPaper: "Protege tu crédito".
3. El dejar de recibir facturas, extractos o el resto del correo. Comunica a tus proveedores que tus facturas no te llegan a tiempo. Una factura que falta podría significar que un ladrón de identidad ha asumido el control tu cuenta y que ha cambiado tu dirección de facturación para no dejar pistas.
4. El recibir tarjetas de crédito que no hayas solicitado.
5. La denegación de un préstamo o que te ofrezcan condiciones de crédito menos favorables, como un interés más alto, sin razón aparente. Si sucede esto, tu calificación de crédito pudo haber sido afectada negativamente y deberías comprobarlo. Para más información sobre calificaciones de crédito puedes leer el PapersPaper: Protege tu crédito.
6. El recibir llamadas o cartas de proveedores sobre productos o servicios que no compraste.

Responder al robo de identidad

Vale, crees que puedes haber sido víctima de un robo de identidad y ¿ahora qué? A continuación hay cinco medidas que puedes tomar. Esta lista está basada en la del sitio web de la FTC.

1. Poner una alarma de fraude en tu crédito, que explicamos en mayor detalle más abajo.

2. Revisa y vigila tus informes de riesgo crediticio. Explicamos más sobre eso en el PapersPaper: Protege tu crédito.
3. Bloquear las cuentas que piensas que han sido afectadas. Si piensas eres víctima de un robo de identidad financiero, por ejemplo si perdiste tu talonario de cheques, tarjeta de crédito o tu cartilla del banco o te las robaron, ponte en contacto con la oficina de tu banco. Pídeles que cancelen tu tarjeta o cheques, que te envíen nuevos y que tomen nota para que estén al tanto de la situación. Esto es conveniente para cualquier posible continuación del asunto.
4. Si se ha perdido alguna identificación personal reconocida oficialmente, como tu DNI, Denuncia la desaparición y pide una nueva. Conserva copia de la denuncia sellada.
5. En cualquier caso deberías denunciar el robo de identidad. Esta denuncia será crítico para probar a las distintas organizaciones (tales como tu banco) que has sido víctima de un robo de identidad. Para hacer esto, acude a la comisaría más cercana y explícales los hechos, lleva contigo toda la documentación que tengas sobre el incidente.
6. Para responder a un robo de identidad, asegúrate de mantener un registro de cada conversación que tengas con las fuerzas de seguridad, funcionarios, representantes de las entidades financieras o cualquier otra persona que participe en tu caso. Incluye la fecha y hora de la conversación, qué se discutió y con quién hablaste. Esta información podía ser importante al procurar resolver asuntos posteriores o determinar quién dijo qué.

Para más información sobre la protección, detección y respuesta a robos de identidad, recomendamos fervientemente sitio web de la FTC. Además de contener una gran cantidad de información, ofrecen un vídeo de 10 minutos sobre los robos de identidad (en inglés). Véa la información del cuadro 1.

Avisos de fraude

Un aviso de fraude es un aviso realizado a las tres agencias de crédito. En los Estados Unidos hay tres agencias nacionales dedicadas a mantener información sobre tu riesgo crediticio y responsables de tu crédito; Equifax, Experian y TransUnion. Estas tres compañías recopilan grandes cantidades de información sobre ti, por ejemplo la apertura de cuentas bancarias, los pagos de tarjeta de crédito, la petición de préstamos o los impagos de tus facturas. Estas organizaciones están constituidas conforme a lo establecido en el Fair Credit Reporting Act (La ley de las calificaciones de crédito justa, FCRA, 15 U.S.C. 1681 et seq.) y Fair Debt Collection Practices Act (Ley de las prácticas justas de reembolso de la deuda o FDCPA) y deben cumplir con lo impuesto en estas leyes. Entonces, estas agencias toman tu información y la procesan usando varios algoritmos avanzados, determinando tu calificación de crédito. Para más información sobre las agencias de crédito, lee el ParentPaper: "Protege tu crédito".

Un aviso de fraude notifica a las tres agencias de crédito que crees ser víctima de un robo de identidad. Siempre que un comerciante o una organización pida un informe de crédito sobre ti, la agencia de crédito le notifica de que tienes un aviso de fraude. Esto les fuerza a seguir pasos adicionales antes de que puedan conseguir tu calificación de crédito. Por ejemplo, supongamos que tienes un

aviso de fraude y pides una hipoteca a tu banco. Normalmente, tu banco haría simplemente una comprobación de crédito, averiguaría cuál es tu calificación y determinaría tu hipoteca basándose en la información. Sin embargo, si tienes una alarma del fraude en tu cuenta del crédito el banco tendrá que tomar medidas adicionales. Por ejemplo, muy probablemente tendrán que ponerse en contacto contigo más tarde (al día siguiente por teléfono) para confirmar que eras tú el que querías la hipoteca y si pueden proceder con comprobación de crédito. Los pasos adicionales como éste ayudan a protegerte si tu identidad ha sido comprometida.

Hay dos tipos de avisos de fraude: inicial y extendido. Un aviso inicial de fraude es muy fácil de solicitar, simplemente llamas a una de las tres agencias de crédito y pones el aviso. Sin embargo, la alarma inicial de fraude sólo dura 90 días. El aviso extendido de fraude es cuando tienes una situación más grave y has realizado una denuncia ante las fuerzas de seguridad por robo de identidad. Un aviso extendido del fraude dura por siete años. Puedes aprender más sobre avisos de fraude y cómo poner uno en

<https://www.annualcreditreport.com/cra/helpfaq#fraudalert>

Resumen

Proteger tu identidad es una tarea difícil. Uno de los problemas más grandes a los que haces frente es que tú no controlas la mayor parte de tu información. En consecuencia, la mejor manera para proteger tu identidad es supervisarla, especialmente las actividades económicas y financieras y reaccionar inmediatamente si sucediera algo sospechoso.

Sitios web

En este artículo hemos mencionado varios sitios web para proteger tu identidad. Aquí puedes encontrar la lista de ellos. Si tuvieras dudas sobre la validez de alguno de ellos, empieza por el de la Comisión Federal de Comercio (FTC) que termina con .gov.

- Comisión comercial federal www.ftc.gov/bcp/edu/microsites/idtheft/
- AnnualCreditReport www.annualcreditreport.com
- Experian (institución de crédito) www.experian.com
- TransUnion (institución de crédito) www.transunion.com
- Equifax (institución de crédito) www.equifax.com
- ParentPapers:
 - [Protege tu crédito](#)
 - [Diez pasos para proteger tus ordenadores de casa](#)

Acerca de nosotros

¿Preocupados por proteger vuestras finanzas online? ¿Os preguntáis quién está obteniendo información de vuestros hijos? ¿Confundidos sobre cómo proteger vuestro ordenador de casa? SecureParents está diseñado para vosotros – unos padres responsables y ocupados. SecureParents es un punto único donde

conocer todos los pasos necesarios para protegeros a vosotros y a vuestra familia en la era de la información actual, compleja y cambiante. El sitio web es gratuito, creado por padres para padres. Si tenéis comentarios o sugerencias sobre este documento, nuestro sitio web, o tenéis una historia que querráis compartir, ¡no dudéis en poneros en contacto con nosotros! Enviadnos vuestras sugerencias o preguntas a informacion@secureparents.com.