



Consejos para Prevenir el Robo de Identidad y Comentario

El Robo de Identidad, también conocido como *Fraude de Identidad*, es un delito que se ha expandido y que está creciendo a pasos agigantados. Aunque potencialmente cualquier persona puede ser un blanco, existen un sinnúmero de cosas que pueden hacerse para reducir el riesgo de convertirse en una víctima del robo de identidad. Las recientes y muy comentadas brechas en los sistemas de seguridad, la ruina de la reputación financiera, la pérdida de un trabajo e incluso arrestos hechos por error a muchas víctimas, han motivado a individuos, empresas y gobierno a ponerse en acción.

Este informe está dirigido a individuos y organizaciones, y sugiere medidas importantes para ayudar a reducir el riesgo del robo de identidad. Los temas cubiertos incluyen el manejo de documentos de papel, asuntos relacionados con el teléfono y la computadora, y los métodos de implementación del robo de identidad con el uso de la nueva tecnología. También se proporcionan referencias de agencias gubernamentales que brindan información y asistencia, y se discuten algunas leyes actuales y otras que todavía son propuestas. Este reporte incluye información específica para los Estados Unidos y para Canadá.

Es importante mencionar que este informe de Demartek se ofrece en forma gratuita a nuestros clientes y amigos debido a la enorme atención generada por el robo de identidad. Este documento es una versión actualizada del publicado en el año 2009.

Copyright © 2015 Demartek. Todos los Derechos Reservados. Demartek es una marca registrada de Demartek, LLC.

Dennis Martin, Presidente de Demartek, está disponible para hablar sobre este tema a grupos cívicos u otras organizaciones o individuos interesados. Por favor llame a la oficina de Demartek al (303) 940-7575 si desea concertar una visita.

La versión actualizada: La versión actual de este documento está disponible en:

http://www.demartek.com/Demartek_Identity_Theft_Prevention_Tips_and_Commentary.html

Lineamientos para la Reproducción de este Documento: Usted puede hacer copias de este documento en su totalidad para ser distribuido en forma totalmente gratuita, a menos que se especifique otra cosa. Si usted cita o hace referencia a este documento, deberá atribuir en forma apropiada los contenidos y la autoría a Demartek e incluir el sitio web de Demartek: www.demartek.com en la atribución.

Las opiniones presentadas en este documento reflejan los criterios actuales al momento de su publicación y están sujetos a cambio.

LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SE PROPORCIONA ÚNICAMENTE CON FINES INFORMATIVOS. AUNQUE SE HAN HECHO ESFUERZOS PARA VERIFICAR LA EXHAUSTIVIDAD Y VERACIDAD DE LA INFORMACIÓN CONTENIDA EN EL MISMO, ÉSTE SE SUMINISTRA “COMO ESTÁ” SIN GARANTÍA DE NINGÚN TIPO, EXPRESA O IMPLÍCITA, INCLUYENDO, PERO NO LIMITADA A LAS GARANTÍAS DE NO VIOLACIÓN Y LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN Y ADAPTABILIDAD PARA UN PROPÓSITO PARTICULAR. NADA DE LO CONTENIDO EN ESTE DOCUMENTO PRETENDE, NI TENDRÁ EL PROPOSITO DE CREAR NINGUNA GARANTÍA O REPRESENTACIÓN POR PARTE DE DEMARTEK.

Los productos, nombres de marcas o nombres de empresas mencionados en este documento, pueden ser nombres comerciales, marcas de servicio, marcas comerciales o marcas registradas de sus respectivas compañías.

Contenido

Introducción	4
Manejo de Documentos de Papel	6
Adquiera una buena trituradora de papel.....	6
Correo Saliente.....	7
SOLICITE QUE NO LE ENVIEN INFORMACION POR CORREO	8
Cheques Bancarios.....	10
Tarjetas de Crédito y Débito.....	12
Fraude en Cajeros Automáticos o Lectores de Tarjetas	13
Tarjetas y Números del Programa de Jubilación.....	14
Licencias de Manejar	16
Registros de Separación del Servicio Militar (US DD 214)	16
Privacidad Telefónica	17
Números no enlistados y números no publicados	18
NO LLAME	18
Seguridad Informática	20
Software Antivirus	20
Anti-spyware	20
Firewalls.....	21
Las "Cookies" de su Navegador	22
Actualizaciones.....	23
Computadoras Antiguas	23
Fraudes electrónicos (Phishing)	24
Contraseñas.....	25
Dispositivos Móviles.....	27
Sitios Web de Redes Sociales.....	27
Intentos de Fraude Comunes.....	28
Hijos.....	32
Otras fuentes de información y asistencia	32
Organizaciones	33
Historias de Robo de Identidad.....	33
Leyes y Reglamentos.....	34
Congelamientos de Crédito y Alertas de Fraude	35
Burós de Crédito	36
Pasaportes de Robo de Identidad.....	36
Seguro contra el Robo de Identidad	38
Agencias Gubernamentales.....	38
Comentarios adicionales.....	48

Introducción

El *Robo de Identidad*, también conocido como *Fraude de Identidad*, sigue siendo uno de los delitos de más rápido crecimiento y de constante cambio. Entre sus víctimas se encuentra gente de todas las edades, niveles económicos, razas, género, etc. En muchos casos las víctimas y sus victimarios nunca se han conocido entre sí, sin embargo, el robo perpetrado por amigos, familiares o compañeros de trabajo está en aumento. En algunos casos pueden pasar semanas o meses antes de que las víctimas se den cuenta de que un fraude se ha cometido en su contra y para entonces el daño ya estará hecho.

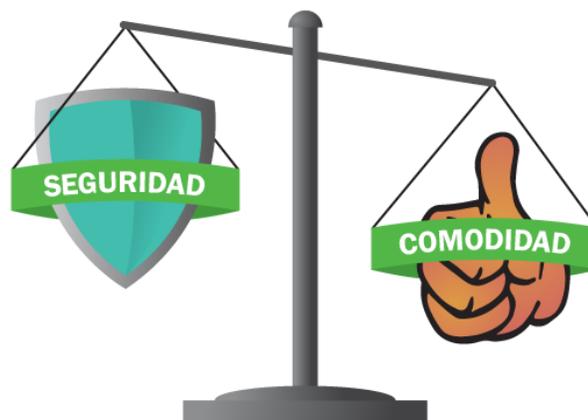
Tanto las empresas como los individuos enfrentan por igual a un sofisticado sistema de fraude en todo el mundo dirigido por la delincuencia organizada. Estos criminales están constantemente modernizando sus tácticas en un esfuerzo por robar tanto identidades como dinero. Aunque los criminales cibernéticos dirigen sus esfuerzos más hacia empresas y su propiedad intelectual, todavía existen amenazas reales para los individuos. Alguna de la información proporcionada en este reporte es específica para una región geográfica en particular, sin embargo los delincuentes están dirigiendo esfuerzos para tratar de operar en muchas diferentes jurisdicciones y marcos geográficos. Esto hace que este delito sea más difícil de combatir y perseguir.

Una de las formas más comunes en que los ladrones de identidad obtienen información, es a través de carteras y bolsas robadas o perdidas y de correo robado de los buzones. Algunas veces aun el correo tirado en los botes de basura puede proporcionar información muy valiosa para un ladrón de identidad. La práctica de los “Pepenadores” por parte de un ladrón de identidad, consiste en buscar en la basura documentos que contengan información útil. Un método creciente para cometer robos de identidad se presenta a través de diversas tácticas de estafa con las que se engaña o manipula a la persona para que entregue dinero o información a un desconocido, o en otras palabras a un ladrón. Dichos métodos le permiten a este último tener acceso a cuentas bancarias o a áreas con información que, combinada con información de otras páginas personales, puede utilizarse para cometer fraudes.

Tal parece que las empresas y otras organizaciones han sido muy eficientes (tal vez demasiado eficientes) en la distribución de información acerca de sus clientes y clientes potenciales. En sus esfuerzos por incrementar las ventas y el consumo en general, no se han puesto a pensar lo suficiente en los “efectos secundarios” de esta distribución masiva de datos personales. Muchas organizaciones han dado poca importancia a las formas en

que la información puede ser robada, y a métodos para proteger información vital de sus clientes.

Aunque algunas agencias gubernamentales promulgan leyes para castigar a los delincuentes y ayudar a las víctimas, y algunas empresas establecen procedimientos para reducir el potencial de un robo de identidad, los individuos pueden y deben tomar medidas para prevenir el mismo. De otra manera, la persona es la que pagará las consecuencias no sólo teniendo que recuperar lo perdido, sino también debiendo sobreponerse al desgaste emocional que provoca un robo de identidad. El grave efecto de éste es subestimado con frecuencia, ya que en la mayoría de los casos, esto lleva años de trabajo. Las víctimas son sometidas a situaciones vergonzosas, donde se les exige explicar las circunstancias del delito en contra de ellas, y en algunos casos, las personas han sido erróneamente arrestadas y encarceladas.



La seguridad y la comodidad son dos factores que contribuyen al nivel de amenaza de un individuo. ¿Está usted dispuesto a sacrificar la una por la otra?

La seguridad, incluida la seguridad física y la electrónica, está inversamente relacionada con la comodidad, es decir, el tomar medidas para aumentar la seguridad reducirá la comodidad. Por el contrario, el aumento de la comodidad resultará en una reducción de la seguridad. La prevención del robo de identidad se ha convertido en un debate acerca de la seguridad que es básicamente una evaluación de riesgo y el balance entre las prácticas, los procedimientos, el tiempo, el dinero y la comodidad. Usted no puede eliminar todas las amenazas de un robo de identidad, ya que siempre habrá nuevas amenazas que emergerán,

pero sí puede tomar medidas específicas para reducir su vulnerabilidad a las mismas. Las sugerencias proporcionadas en este documento pueden parecer inconvenientes o quizás extremas. Cada situación es diferente, por lo tanto usted debe analizar los riesgos y determinar qué pasos son apropiados dar en su situación.

Aunque las agencias de gobierno y las empresas encontrarán muy útil la información contenida en este reporte, éste ha sido elaborado pensando principalmente en el beneficio del ciudadano que desea aprender más sobre este importante tema.

Manejo de Documentos de Papel

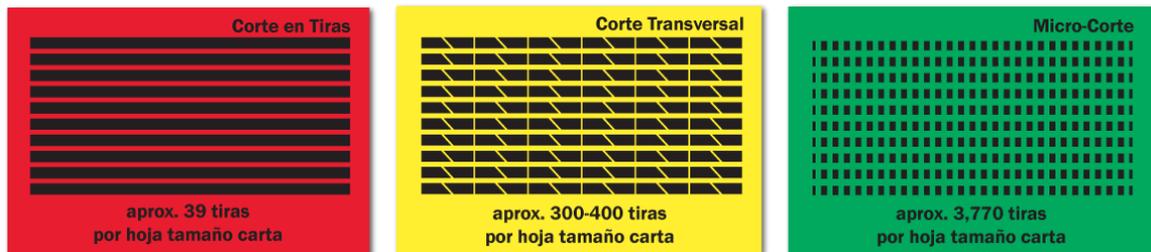
Aunque el robo de identidad tiene una cierta connotación de alta tecnología, muchos de los esfuerzos de prevención y de recuperación son relativamente de baja tecnología. Los ladrones de identidad están buscando información personal que ellos puedan usar y mucha de ésta, está bastante disponible. Uno de los fines de estos robos es la oportunidad de crear “crédito instantáneo,” comprar mercancía con este crédito y hacer que otro pague por ella. Existen varias medidas que pueden tomarse para reducir o eliminar la información acerca de usted que pudiera ser rentable para los ladrones de identidad:

Adquiera una buena trituradora de papel

Para prevenir que una persona utilice técnicas como el hurgar en la basura, entre otras que se usan para obtener información impresa, compre y use una buena trituradora de oficina. La trituradora debe ser de la variedad de corte-en-cruz las cuales producen pedazos de papel muy pequeños. Algunas trituradoras son lo suficientemente fuertes como para triturar plástico delgado, como el de las tarjetas de crédito viejas. La variedad más antigua que simplemente corta el papel en tiras largas, no proporciona una protección adecuada ya que las tiras pueden ser pegadas nuevamente. Algunos centros de reciclado no aceptan papel triturado, así que éste debe tirarse a la basura.

Todos los documentos financieros antiguos deben ser triturados. Éstos incluyen los estados de cuenta de banco y de tarjetas de crédito, documentos de compañías aseguradoras y cualquier otro documento que tenga su nombre, dirección, número de cuenta u otra información personal que pudiera identificarlo. Esto también incluye los sobres en los que se envían los anteriores documentos, si acaso contienen su nombre o número de cuenta impresos. Los documentos tales como cheques viejos o fichas de depósito de cuentas ya cerradas, también deben ser triturados. Algunos documentos se

consideran “viejos” antes que otros. Ciertos documentos relacionados con los impuestos sobre la renta deben conservarse por siete años, sin embargo otros documentos financieros pueden ser destruidos antes de siete años. Consulte a su asesor de impuestos, legal o financiero en cuanto a los períodos de retención de documentos específicos.



Adicionalmente, toda la correspondencia de correo basura o propaganda que contenga su nombre, dirección, u otra información específica suya, debe ser triturada. Esto incluiría también los sobres si tienen su nombre impreso en ellos.

Si usted no posee una trituradora de papel o si usted encuentra que lo que le proponemos le va a quitar mucho tiempo, busque algún evento público en su área en el que se triture papel. Algunas ciudades y estados organizan periódicamente “eventos de triturado” abiertos a los miembros de la comunidad.

En resumen, la basura impresa o el papel reciclado que incluya su nombre u otra información personal legible, no debe salir de su residencia. Si usted tiene dudas respecto a si debe triturar algo o no, a menudo lo mejor es hacerlo.

Correo Saliente

Llevar su correo saliente y sus paquetes a la oficina postal, oficina de paquetería, etc., es una práctica excelente para evitar la alteración en la correspondencia. No deje su correo saliente ni sus paquetes en su buzón particular ni en su puerta de entrada para que sean recogidos. Los ladrones de identidad buscan cheques que usted haya escrito o cualquier cosa con su nombre o número de cuenta impreso dentro de éstos. Los ladrones de identidad también andan en busca de buzones localizados en lugares oscuros o que están llenos de correo. Estos delincuentes se llevarán correo de estos buzones y una vez en posesión de él, podrán alterar los cheques o copiar el número de cuenta de usted y reproducir cheques usando su número de cuenta u otra información personal pre-impresa en sus cheques originales.

Si usted va a estar fuera de su casa por más de un día, es buena idea que alguien de su confianza revise y asegure su correo diariamente. La oficina postal también puede retener su correspondencia desde un mínimo de tres días y hasta un máximo de treinta. Cuando regrese a su casa puede reprogramar la entrega de la correspondencia incluida la acumulada, o bien puede recogerla en la oficina postal. El servicio postal de Canadá ofrece un servicio similar de retención de correspondencia en vacaciones el cual tiene costo y retiene hasta un máximo de quince días.

SOLICITE QUE NO LE ENVIEN INFORMACION POR CORREO

Una manera de ayudar a prevenir el robo de información personal a través del correo es solicitando a sus proveedores que no le envíen información por correo. Existen muchas organizaciones que desean venderle a usted sus productos, probablemente mucho más de lo que usted realísticamente puede usar o puede pagar. Hay muchas empresas que generan ingresos simplemente vendiendo listas, tanto de clientes como de clientes potenciales, a otras empresas. Hay algunas cosas que usted puede hacer para frenar la distribución de su nombre e información personal. Usted puede solicitar que su nombre sea removido de las listas de correo de varias maneras, las cuales le recomendamos aquí; algunas de estas son listas generales y algunas son más específicas:

- ◆ **Asociación de Mercadeo Directo de los Estados Unidos (DMA) Servicio de Correo**

Preferente (MPS) – Este servicio le permitirá a usted reducir significativamente, a nivel nacional, la cantidad de publicidad no solicitada que usted recibe en su hogar. Cuando usted se registra con MPS, a usted se le da la opción de administrar los tipos de correo que usted recibe. Las ofertas de correo son divididas en cuatro categorías – las ofertas de crédito, catálogos, ofertas de revista y otras ofertas. Usted puede escoger cuáles ofertas, si alguna, le gustaría recibir de cada categoría. Puede tomar hasta 90 días para que su selección tenga efecto, y su información solo permanecerá en el MPS por un período de tres años. Para registrarse con el Servicio de Correo Preferente, visite el sitio: <http://www.DMAchoice.org>

- ◆ **Asociación de Mercadeo Canadiense (CMA) Servicio de No Contactar** – Este es un servicio que le permite a usted remover su nombre y dirección de las listas de correo en Canadá. Este servicio puede tomar hasta seis semanas para llevarse a efecto, y los nombres permanecerán en la lista por sólo tres años. A

diferencia de la Asociación de Mercadeo Directo de los Estados Unidos (MPS), este servicio no requiere que usted administre sus ofertas de correo, simplemente agrega su información a una lista de: “No enviar correo a...” Para agregar su nombre y dirección vaya a:

http://www.cmaconsumersense.org/marketing_lists.cfm.

- ◆ **Servicio Opt-out (de la pre-selección)** – Este servicio le permitirá a usted reducir el número de ofertas de crédito “pre-aprobadas” que usted recibe. Actualmente, este servicio está solamente disponible en los Estados Unidos. Sus derechos como consumidor incluyen la posibilidad de “Opt-out de la pre-selección” o “Solicitar Excluirse de la pre-selección” lo cual impide que las compañías de información de crédito al consumidor usen su información de crédito para enviarle ofertas “pre-aprobadas” de crédito o de seguros. Usted puede solicitar "Opt-out" o "Excluirse" de listas de ofertas 'pre-aprobadas' por un período de cinco años o en forma permanente. Asegúrese de especificar su preferencia. Para registrarse a este servicio de Exclusión “Opt-out”, visite su website en: <https://www.optoutprescreen.com> o llame al 888-5-OPT-OUT (888-567-8688).
- ◆ **Otras ofertas de crédito de Bancos** – Esto requiere un poco más de acción de parte suya que los primeros tres puntos anteriores. Cuando usted recibe ofertas no solicitadas de tarjetas de crédito de bancos, aerolíneas u otros negocios, la solicitud incluirá un número telefónico al cual usted puede llamar para registrarse. Si usted no desea solicitar esa tarjeta de crédito, llame al número de teléfono y solicite ser registrado en la lista de “NO ENVIAR CORREO” de tarjetas de crédito. Ellos deberán respetar esta solicitud y el representante de servicio al cliente generalmente le leerá a usted el “script” que ellos usan para este proceso. Usted tendrá que repetir estos pasos para cada oferta de tarjeta de crédito que usted reciba, sin embargo después de un muy corto tiempo, usted no recibirá más ofertas de este tipo. Una vez que la compañía ha confirmado que su nombre y domicilio están en su lista de “NO ENVIAR CORREO” usted deberá triturar la solicitud, así como está descrito en la sección de “Adquiera una buena trituradora...” anterior.
- ◆ **Cheques pre-impresos respaldados por su tarjeta de crédito** – Tal vez usted reciba cheques pre-impresos de su compañía de tarjetas de crédito, los cuales pueden ser usados como cheques regulares pero con cargo a su tarjeta de

crédito. Estos son un favorito de los ladrones de identidad, porque una vez en su posesión, son especialmente fáciles de usar. Los ladrones buscan cheques respaldados por tarjetas de crédito dentro de su correo y gustan de robarlos antes de que usted recoja su correspondencia. Usted puede llamar a su compañía de tarjetas de crédito y solicitarles que no le envíen cheques respaldados por tarjetas de crédito en el futuro. Si usted ya ha recibido estos, y planea usarlos, deberá mantenerlos en un lugar seguro. Si usted no planea usar estos cheques respaldados por su tarjeta de crédito, usted debe triturarlos y discontinuarlos.

- ◆ **Cualquier otra oferta de correo** – Usted puede hacer uso del mismo procedimiento que usted seguiría para ofertas de bancos o de tarjetas de crédito que usted no solicitó. Llame a la compañía telefónica o visite el sitio web de la compañía y solicite ser removido de sus listas de correo. En el caso de los paquetes con hojas sueltas o volantes de tiendas, llame a la agencia de publicidad que aparece en la etiqueta de dicho correo. Como el empleado postal deja este tipo de publicidad en cada casa en forma rutinaria, pudiera también necesitar notificarle a él de su decisión.

Cheques Bancarios

Ante la implementación y aceptación difundida de otras formas de pago como las tarjetas de crédito y débito, y los métodos de pago en línea, el uso de cheques bancarios va cayendo en desuso. Sin embargo, esto no significa que deban pasarse por alto las prácticas de manejo seguro de los cheques; estos pueden proporcionar a los ladrones una buena parte de su información bancaria. Sus cheques de banco regulares deben estar siempre en un lugar seguro. Adicionalmente sus cheques pre-impresos deben ser del tipo de cheques de “alta-seguridad” con por lo menos 8 elementos de seguridad incluidos. Algunos de estos elementos de seguridad son visibles y otros son invisibles. Estos cheques de alta-seguridad son más difíciles de falsificar o adulterar. Evite llevar cheques con usted, a menos que usted planea girar un cheque para un propósito específico.

NO imprima en sus cheques su número de Seguro Social, número de Licencia de Manejar o cualquier otro número de identificación oficial.

Algunas personas prefieren no imprimir su nombre completo en sus cheques, sino sólo las iniciales de su nombre y su apellido. Si un ladrón de identidad no conoce su nombre completo y ha robado sus cheques, no sabrá a ciencia cierta cómo firmar el cheque. En lugares donde usted decida proporcionar su información personal, lo mejor es brindar solamente la necesaria o requerida. También es importante no escribir ni firmar de antemano los cheques antes de que se realice la transacción de pago. Si éstos son robados o se pierde una chequera con una firma ya escrita, es fácil para un ladrón llenar los otros espacios y cobrar el dinero del cheque.

DEBE

- ✓ Mantenerlos en un sitio seguro
- ✓ Utilizar alta seguridad (al menos ocho medidas de seguridad)
- ✓ Envolver en papel los cheques enviados correo
- ✓ Si va a enviar cheques por correo, llévelos a la oficina postal
- ✓ Enviar por correo al banco las solicitudes de cheques
- ✓ Registrarse para la banca electrónica o para pagar facturas electrónicamente

NO DEBE

- ✗ Prestar su chequera
- ✗ Llevarla con usted a menos que planea utilizarla
- ✗ Endosar cheques en su casa
- ✗ Imprimir el número de Seguro Social en sus cheques
- ✗ Imprimir el número de la Licencia de Manejar en sus cheques
- ✗ Pre-escribir/pre-firmar los cheques

El Lavado de Cheques es el proceso mediante el cual se utilizan productos de limpieza para borrar la tinta en ciertas porciones de los cheques, pudiendo cambiar el nombre del beneficiario o modificar el monto del cheque. Algunos ladrones de identidad se han vuelto muy diestros en el empleo de esta técnica. Cuando usted escriba un cheque, utilice una pluma de tinta permanente del tipo de las de gel, cuya tinta penetra en las fibras de papel, ya que éstas son más difíciles de borrar.

Cuando envíe cheques por correo, envuelva el cheque y otros artículos en una hoja blanca de papel o utilice un sobre de seguridad, ya que la mayoría de los sobres que los bancos u otras compañías proveen para enviarlos a vuelta de correo son relativamente baratos y, por ende, transparentes. Si usted envía cheques por correo, asegúrese de llevarlos directamente a la oficina postal.

Al solicitar nuevos cheques de su entidad financiera, opte porque los mismos sean entregados a su sucursal de banco. Es común también, que el banco le envíe a su residencia los cheques

que usted solicitó, sin embargo es mejor que usted los recoja ya que es una forma de mantener información confidencial lejos de su buzón. Si usted sospecha que su buzón no es seguro, que ha sido forzado en el pasado o si éste forma parte de un conjunto de buzones (es decir, una estación postal en un complejo de apartamentos), informe a su banco y haga que no se los envíen y que le avisen para que usted los recoja.

Frank Abagnale es un antiguo estafador que se convirtió en consultor de seguridad y cuya vida inspiró la película *Atrápame si Puedes*. Él escribió un documento que provee un extenso asesoramiento sobre la forma de estar protegido contra la falsificación de cheques. Usted puede leer este documento en: http://www.abagnale.com/pdf/protection_b.pdf.

Mucha gente está cambiando a la banca electrónica y al sistema de pagos de facturas en forma electrónica para evitar algunos de los problemas que se tienen con los cheques de papel.

Tarjetas de Crédito y Débito

Usted debe siempre saber en dónde están sus tarjetas de crédito y débito. Nunca deje su tarjeta sin vigilancia en su trabajo o en la guantera de su automóvil. Estos son dos de los lugares más frecuentes en donde ocurren los robos de tarjetas de crédito. Si usted está utilizando su tarjeta en una tienda o un restaurante, asegúrese de que se la devuelvan. Es muy fácil olvidar su tarjeta, o que ésta se pierda cuando los comerciantes están manejando diversas transacciones al mismo tiempo.

Apenas reciba su tarjeta, fírmela por la parte de atrás utilizando tinta permanente. Las tarjetas sin firma no son válidas. Si usted quiere que el vendedor o comerciante solicite además una identificación con foto, usted debe entonces firmar su tarjeta, y escribir junto a su firma: "Solicite ID". Nunca escriba su Número de Identificación Personal (NIP) en su tarjeta; es mejor memorizarlo.

Es extremadamente importante que usted no dé su número de tarjeta de crédito en el teléfono, a menos que usted haya iniciado la llamada o esté completamente seguro de quién está al otro lado de la línea. Muchos estafadores engañan a la gente haciéndose pasar por empresas legítimas. No preste su tarjeta a amigos o familiares. Las compañías de tarjetas de crédito y los bancos considerarán que ese usuario tiene el permiso de usted, y usted será responsable de todos los cargos incurridos. En muchos casos, por razones de seguridad, los bancos cerrarán las cuentas de aquellos que permiten a otros utilizar sus tarjetas de débito o crédito. Si usted ha permitido que alguien más utilice su tarjeta en el pasado y ya no desea

que dicha persona tenga la información, la única manera de garantizar que no tenga acceso es solicitar una nueva tarjeta con un número y NIP nuevos.

Es una buena idea sacar copias fotostáticas de sus tarjetas y guardar esas copias en un lugar seguro como un archivero con llave. Si su tarjeta se pierde o es robada, usted tendrá el número de teléfono a dónde llamar, al igual que toda la información pertinente. Siempre revise sus estados de cuenta bancarios o su cuenta bancaria en línea para asegurarse que todos los cargos han sido realmente hechos por usted. Si usted observa alguna actividad sospechosa o si usted pierde su tarjeta, informe a su compañía de tarjetas de crédito o a su banco de inmediato e infórmeles que se le perdió o se la robaron. Ellos cancelarán la tarjeta y le emitirán otra con información nueva. Lo mejor es informar a su entidad financiera todas las razones por las que solicita tarjetas nuevas para que puedan ayudarle mejor y rastrear potencialmente cualquier uso no autorizado de las tarjetas robadas o extraviadas.

Además, al viajar dentro o fuera de su país, informe a su entidad financiera y/o a su compañía de tarjetas de crédito/débito el lugar donde usted estará y las fechas.

Así como el uso de cheques va en descenso y el de tarjetas de crédito y débito va en aumento, así también aumentan los métodos en los que los ladrones pueden poner en riesgo sus cuentas y su seguridad. Es importante tener siempre precauciones generales al comprar o realizar transacciones bancarias con una tarjeta de crédito o débito.

Fraude en Cajeros Automáticos o Lectores de Tarjetas

Los cajeros automáticos son una herramienta ampliamente utilizada por las entidades financieras para entregar dinero a sus clientes de manera rápida y cómoda. Los ladrones están empezando a atacar las transacciones realizadas en estos lugares debido precisamente a la comodidad y rapidez de las mismas, así como a la falta de atención de las personas al momento de realizarlas.

Al utilizar un cajero automático y antes de insertar su tarjeta, realice una inspección visual de la máquina y de las áreas a su alrededor para detectar cualquier cosa inusual. Una nueva práctica utilizada por los ladrones consiste en colocar una ranura "falsa" de inserción de tarjeta sobre la ranura original puesta por el banco. A primera vista parecen normales pero están instaladas en la máquina para leer los números de su tarjeta y su banda magnética con el fin de enviar y almacenar información en un dispositivo exterior. Estando en el cajero automático, asegúrese de revisar el teclado de la máquina para detectar teclados falsos que

puedan haberse sobrepuesto al existente y que puedan grabar las teclas que usted oprime, como su NIP, para enviarlas a un dispositivo exterior. Tenga cuidado también con las cámaras utilizadas que puedan no formar parte de la máquina. Por último, tome nota mentalmente de las personas a su alrededor mientras utilice un cajero automático. Si en algún momento se siente incómodo con la situación en el cajero, no inserte su tarjeta, informe a la entidad financiera inmediatamente y utilice otro cajero. Siempre será más rápido ir a otro cajero que utilizar uno intervenido e intentar recuperar el dinero perdido a manos de un ladrón.

Las prácticas mencionadas también deben observarse al utilizar lectores de tarjeta en las bombas de las gasolineras, pues se están convirtiendo rápidamente en sitios donde los ladrones pueden colocar lectores de tarjetas para leer y almacenar información importante. Como se dijo anteriormente, inspeccione visualmente todo dispositivo de lectura de tarjetas antes de insertar su tarjeta de débito o crédito.

Tarjetas y Números del Programa de Jubilación

Muchos países tienen programas nacionales de jubilación con un número de cuenta para cada persona que es elegible. En los Estados Unidos y en Canadá, esto se conoce como el Número de Seguro Social (SSN en Estados Unidos, SIN en Canadá). Aunque los programas no son idénticos, los usos básicos de estos números son muy similares. Ellos se usan principalmente para asuntos fiscales y programas de jubilación y deben ser guardados en forma confidencial. Sin embargo, con el tiempo, especialmente en los Estados Unidos, estos números han sido usados como una forma de identificarse para muchos propósitos, sin tomar en cuenta los posibles problemas que esto puede representar para la privacidad de la información.

Los números aparecen en una tarjeta oficial expedida por el gobierno. Es posible que usted tenga que mostrar su tarjeta a su empleador cuando usted empiece en un trabajo, aunque algunas veces los empleadores únicamente desean asegurarse de que tienen el número correcto. De lo contrario, estas tarjetas deben mantenerse en un lugar seguro y no llevarse en su bolsa o en su cartera. Si estas tarjetas son encontradas o robadas, estos números son de valor incalculable en las manos de un ladrón de identidad. Usted no debe escribir su Número de Seguro Social en sus cheques. No debe aparecer tampoco en su Licencia de Manejo. No lo publique en Internet. Por otro lado es importante saber que es ilegal utilizar números de Seguro Social falsos, alterados o robados para obtener un empleo, un préstamo, un crédito u otros bienes y servicios. Las sanciones incluyen multas y penas de cárcel, y cuando el número es utilizado por gente no-ciudadana, puede incluso resultar en deportación.

No divulgue los números de sus tarjetas y manténgalas en un sitio seguro cuando no las esté usando. Si alguien le pide información confidencial, haga preguntas antes de contestar.

En los Estados Unidos, la Administración del Seguro Social proporciona una declaración anual a los trabajadores y ex-trabajadores de 25 años o más, y a trabajadores de cualquier edad que la soliciten. Es una buena idea comparar la información incluida en esta declaración a la cantidad de dinero que usted reporta en su declaración de impuestos. Si la cantidad para un cierto año es mayor en la declaración del Seguro Social que en la declaración de impuestos, es posible que alguien haya estado usando su Número de Seguro Social para propósitos de nómina, y también para solicitar algún tipo de crédito.

El gobierno de Canadá ofrece un servicio en línea llamado “My Service Canada Account” el cual le permite ver, actualizar e imprimir los registros de su Plan de Pensión Canadiense (CPP), Seguro de Empleo (EI) y Seguro para la Vejez (OAS). Los nuevos usuarios de este servicio deberán solicitar un Código de Acceso Personal (Personal Access Code) antes de poder aplicar para una cuenta. La cuenta requiere un Nombre de Usuario y una Contraseña llamada “epass”. En el futuro, un “epass” será todo lo que usted necesitará para tener acceso a la “My Service Canada Account”. Revise su cuenta en forma periódica para asegurarse que su información es correcta y que refleja su historial de trabajo.

Estos números no deben darse a cualquier persona. Si alguien le pide su Número de Seguro Social (SSN o SIN), usted debe hacer varias preguntas:

- ◆ ¿Es esto requerido por ley?
- ◆ ¿En qué se va a usar mi número?
- ◆ ¿Puede usted o la organización que lo está solicitando aceptar otra identificación que no sea mi número de Seguro Social?

Para obtener más información acerca del Seguro Social en los Estados Unidos visite: <http://www.ssa.gov> o en Español en: <http://www.ssa.gov/espanol>. Para obtener más

información acerca del Seguro Social en Canadá vaya a:

<http://www.servicecanada.gc.ca/eng/sc/sin/index.shtml>.

Licencias de Manejar

En los Estados Unidos usted está obligado por ley a proporcionar prueba de su Número de Seguro Social a los funcionarios encargados de la Licencias de Manejar, pero éste no debe aparecer impreso en su licencia. El Acta de la Reforma de Inteligencia y Prevención del Terrorismo del año 2004 impide a los estados mostrar el Número de Seguro Social en licencias de manejar, tarjetas de identificación del estado o registros de vehículos de motor. Los residentes Canadienses no están obligados a proporcionar el Número de Seguro Social para obtener una licencia de manejar, pero éste puede ser usado como una forma secundaria de identificación. El Número de Seguro Social tampoco aparecerá impreso en las licencias de manejo Canadienses.

Rehúcese a proporcionar su licencia de manejar o su número de licencia de manejar a nadie, a excepción de funcionarios que muestren ser legítimos servidores de la ley. Ha habido casos de robo de identidad que comienzan con empresas sin escrúpulos que solicitan la información de la licencia de manejar con "fines de seguridad", quienes luego venden la información de estas licencias a ladrones de identidad.

En algunas jurisdicciones se puede obtener un informe de multas pendientes relacionadas con una licencia de manejar en particular. Vale la pena pagar una pequeña cuota para ver si alguien, utilizando el nombre de usted, ha cometido alguna infracción o recibido multas de tránsito.

Registros de Separación del Servicio Militar (US DD 214)

En los Estados Unidos el Reporte de Separación, Forma DD 214, también conocido como "Documento de Baja del Servicio Militar" es expedido a los miembros del servicio militar cuando dejan el Servicio Militar. La Forma DD 214 contiene información personal que podría ser utilizada por un ladrón de identidad. Como una opción, muchos estados permiten el archivo de estas formas en la corte del condado local para que las copias puedan ser más fáciles de obtener en lugar de tener que solicitar copias del Centro Nacional de Registros Personales (NPRC). Estas formas, ya sea las originales o copias certificadas, se requieren en ocasiones para poder obtener beneficios de Veteranos. La desventaja de archivar copias del DD 214 en la corte del condado es que la información se convierte en un

registro público, disponible para cualquiera. En los últimos años, muchos estados han cambiado sus leyes para proporcionar una cierta medida de confidencialidad a la DD 214. Algunos estados todavía consideran a la DD 214 como un registro público sin ningún grado de confidencialidad, mientras que otros estados no registran la Forma DD 214 en absoluto.

Los estados han adoptado diferentes enfoques con respecto a la Forma DD 214. Para ayudar a disminuir el robo de identidad, algunos estados permiten que cierta información contenida en la Forma DD 214 sea removida de las cortes locales. Algunas jurisdicciones permiten la *Solicitud de Exención de Revelación Pública de los Documentos de Baja* (*Request for Exemption from Public Disclosure of Discharge Papers*) para que sólo los Veteranos, su pariente más cercano, u otro representante específicamente designado, pueda tener acceso a estos registros. Algunas jurisdicciones automáticamente restringen el acceso a la DD 214. Otras permiten la investigación histórica y genealógica en los registros de la DD 214 después de 75 años u otros períodos de tiempo similares después de la fecha de registro.

Se han dado casos de robo de identidad donde el ladrón obtuvo información concerniente a muchos Veteranos utilizando los archivos DD 214 de una cierta área. Cada estado tiene políticas de confidencialidad diferentes; es mejor contactar al Oficial de Servicios al Veterano en su condado quien le explicará el alcance, significado y aplicación de las leyes donde usted vive. Para encontrar un oficial de servicios visite NACVSO.org.

Privacidad Telefónica

En ocasiones los ladrones de identidad intentan obtener su información personal vía telefónica. Hay algunas cosas que usted puede hacer para hacer que su información telefónica sea menos visible. Como cada día son más las comunicaciones que se realizan vía internet, las estafas telefónicas están disminuyendo, aunque todavía existen. Cuando usted hable por teléfono con una persona o empresa, verifique que conoce a la persona con quien está hablando. Igualmente, si una empresa lo está contactando, asegúrese de que la razón por la que lo llaman y por la que potencialmente le están solicitando información, es lógica. Con mucha frecuencia un ladrón o grupo de ladrones se presentará como una empresa legítima, o como una empresa relacionada con un servicio que usted usa a menudo. En muchas ocasiones, cuando usted confronta o pregunta al que llama, éste dará vueltas al tema y seguirá intentando obtener información. Si usted no conoce a la persona o compañía, no dé ninguna información y cuelgue. Si parece un ladrón que se hace pasar por una empresa legal, cuelgue y contacte directamente a la empresa y discuta el suceso. Ellos podrán informarle si la llamada era válida y también le advertirán si hay alguien que está

afirmando falsamente tener relación con ellos para sacar provecho monetario o informativo. Demartek informó recientemente de un engaño telefónico que se ha vuelto muy común, incluyendo una grabación de la conversación telefónica, en el "Reporte de Engaño Telefónico relacionado con el IRS" de Demartek ([Demartek IRS Telephone Scam Report](#)).

Números no enlistados y números no publicados

Existen 3 categorías básicas de números de teléfono. Estas son: La lista principal de teléfonos, los teléfonos no enlistados y los teléfonos no publicados. De los 3 tipos, la lista de los teléfonos no publicados es la más segura.

- ◆ **Lista Principal** – Su nombre, dirección y número de teléfono están incluidos en los directorios telefónicos impresos y están disponibles a través del Servicio de Asistencia Telefónica. Su nombre y número de teléfono también están incluidos en las listas que la compañía telefónica vende a otras compañías con propósitos de mercadotecnia.
- ◆ **No enlistados** – Su nombre, dirección y número de teléfono no están incluidos en los directorios telefónicos impresos, pero sí están disponibles a través del Servicio de Asistencia Telefónica. A esto también se le conoce como un "Número no enlistado".
- ◆ **No publicados** – Su nombre, dirección y número de teléfono no están incluidos en los directorios telefónicos impresos ni tampoco están disponibles a través del Servicio de Asistencia Telefónica. Su nombre y número telefónico no están incluidos en las listas que la compañía de telefónica vende a otras compañías con propósitos de mercadotecnia.

Los "servicios" para solicitar que los teléfonos no aparezcan enlistados o que no sean publicados están disponibles por una cuota mensual. Usted debe pedir por uno de los dos servicios, el de teléfonos no enlistados o el de teléfonos no publicados.

NO LLAME

Existen registros disponibles del gobierno nacional y local, de los conocidos como: "NO LLAME". También existen los registros comerciales voluntarios. El agregar su número de teléfono a estos registros ayudará a reducir la cantidad de llamadas telefónicas no deseadas, y disminuirá la publicación y distribución de su número de telefónico.

- ◆ **Registro NO LLAME (Estados Unidos)** – En los Estados Unidos, el Registro Nacional Federal "NO LLAME" está disponible en <https://www.donotcall.gov> o en español en: https://www.donotcall.gov/default_es.aspx . También puede llamar al 1-888-382-1222. En Febrero de 2008, El Acta de Mejoramiento del Registro No Llame del 2007 se convirtió en Ley. Esto quiere decir que una vez registrado, un número telefónico permanecerá en la lista en forma permanente. La colocación de su número en el "Registro Nacional No Llame" detendrá la mayoría de las llamadas de telemarketing, pero no todas. Debido a las limitaciones en la jurisdicción del FTC y FCC, las llamadas de, o en nombre de organizaciones políticas, organizaciones de beneficencia y encuestadores telefónicos sí están autorizadas, así como las llamadas de empresas con las que usted mantiene una relación de negocios, o aquellos de quienes usted ha proporcionado el nombre en un documento por escrito solicitando recibir sus llamadas. Aunque el registro nacional existe, algunas compañías han decidido ignorarlo y se han hecho acreedoras a citatorios o han sido sancionadas. Usted puede encontrar un listado de estas compañías en: <http://www.fcc.gov/eb/tcd/DNCall.html>.
- ◆ **Registros Estatales de NO LLAME** – Adicionalmente, muchos estados en la Unión Americana tienen sus propios registros estatales. Usted puede encontrarlos por medio de su Motor de Búsqueda favorito de Internet escribiendo la frase "Do not call" (No llame) y el nombre de su Estado, o contactándose con la agencia de Protección al Consumidor de su Estado.
- ◆ **Registro Canadiense de NO LLAME** – En el año 2006, el gobierno Canadiense aprobó una ley permitiendo la creación de una lista nacional de números "NO LLAME". Este registro está disponible en: <https://www.lnnte-dncl.gc.ca>. También puede marcar al 1-866-580-3625. Una vez que su número está en la lista, permanecerá registrado durante 5 años. Los Telemarketers están obligados por ley a suscribirse a la lista y deben actualizar sus registros cada mes. Similar a la lista de "NO LLAME" en los Estados Unidos, su registro a ella no impide la entrada de llamadas de entidades de beneficencia, organizaciones que realizan encuestas o sondeos, de partidos políticos, o de periódicos en busca de suscripciones.

Seguridad Informática

Mucho se ha escrito acerca de la seguridad informática, así que nos enfocaremos en algunos conceptos básicos con el objetivo de reducir su vulnerabilidad al robo de identidad a través de la computadora. La mejor defensa es una de multi-capas, varias de las cuales se discutirán aquí. Existen muchos temas avanzados respecto a este tema, por lo cual usted puede muy fácilmente encontrar información adicional.

Software Antivirus

Algunos virus y gusanos de computadoras están diseñados para buscar información personal en su computadora y enviarla a una ubicación externa. Existen muchas variantes conocidas de este tipo de software malicioso y la información acerca de estos está disponible en los sitios web de las compañías líderes en software antivirus. Una amenaza que se está volviendo cada vez más común es el software de seguridad falso o "scareware". Estos programas ofrecen falsos antivirus para eliminar el software malicioso de las computadoras, pero lo que en realidad hacen es que instalan virus Troyanos y con frecuencia aconsejan al usuario comprar protección que es falsa. Tenga cuidado de las ventanas que se abren de repente o de los anuncios que aparentan tener productos legítimos, ya que estos son métodos comunes utilizados por los delincuentes cibernéticos. Algunos anuncios pueden incluso afirmar ser parte de una empresa conocida especializada en antivirus. En lugar de hacer click en ese tipo de vínculos, mejor consulte el sitio de internet de la empresa en cuestión.

Consiga un buen paquete antivirus de algún fabricante conocido por tener experiencia en esta área y asegúrese de estar al tanto de las actualizaciones de las variantes de virus. Con el fin de mantenerse al día con el volumen de actividad criminal en Internet, algunos de los fabricantes líderes en antivirus ponen a disposición varias actualizaciones de estos durante el día.

Anti-spyware

El Spyware ha generado mucha atención de los medios recientemente: Su propósito es recopilar información de su computadora y ponerla a disposición de una entidad externa. Algunos de ellos están relacionados a propósitos publicitarios y otros están buscando por información personal o datos clave (como Nombres de Usuario y Contraseñas). Existen varias soluciones anti-spyware, y algunas de las compañías de software antivirus incluyen

tecnología anti-spyware con sus soluciones antivirus. Haga una relativamente pequeña inversión para protegerse del spyware.

Firewalls

Los Firewalls también llamados Cortafuegos, ayudan a proporcionar protección contra usuarios maliciosos en Internet y en redes internas y no debe ser una opción. Los firewalls inspeccionan el tráfico de red entrante y saliente y desechan el tráfico entrante que no está entrando en respuesta directa a alguna solicitud hecha por usted. Opcionalmente, las firewalls pueden también bloquear tráfico saliente. Este documento le proporciona un entendimiento básico de la tecnología de firewall para redes informáticas, pero no pretende ser un tutorial completo sobre el tema.

***Cuando se trata de información importante,
siempre es mejor estar sobre-protegido que
desprotegido.***

Existen 2 tipos básicos de firewalls para redes informáticas: hardware y software. Le recomendamos que utilice ambos tipos de firewalls juntos, como parte de una estrategia de defensa multi-capa. Ambos tipos de firewalls pueden configurarse para ignorar ("stealth") solicitudes entrantes. Esta es una muy buena estrategia ya que existen delincuentes en todas partes del mundo quienes constantemente escanean el Internet buscando computadoras con puertos abiertos.

La mayoría de los sistemas operativos de las computadoras proporcionan un firewall de software. Para el entorno Windows, los firewalls de software que fueron introducidos con el Windows XP Service Pack 2 (SP2) fueron mejorados en versiones posteriores de Windows 8 y 8.1. Apple Macintosh y muchos sistemas Linux incluyen un firewall de software, además de que se pueden encontrar firewalls de software a través de terceros. Es importante usar un firewall en cada computadora que esté conectada a una red, ya sea la que viene con su sistema operativo o una versión adquirida con un tercero. Además, se recomienda que el firewall de hardware se despliegue también en hogares y oficinas pequeñas que tengan conexiones a Internet.

Los firewalls de hardware proporcionan una protección constante a todas las computadoras conectadas en una red doméstica o de pequeña empresa, incluso si una de esas computadoras no tiene sus defensas encendidas o si está de alguna manera comprometida. Los firewalls de hardware también proporcionan otra capa de defensa y ayudan a retrasar o prevenir algunos ataques entrantes. Los firewalls de hardware están generalmente pre-configurados para ignorar (stealth) puertos TCP/IP para el tráfico procedente del exterior. Si una computadora detrás de un firewall de hardware se viera comprometida de tal manera que abriera algunos de sus propios puertos TCP/IP y "escuchara" los comandos de una fuente externa, el firewall de hardware bloqueará el tráfico antes de que llegue al equipo en la red interna. Existen varias marcas reconocidas de firewalls o *routers* de firewalls disponibles. Los modelos diseñados para uso en el hogar son relativamente sencillos y de bajo costo. Estos firewalls están disponibles para redes alámbricas e inalámbricas.

Las "Cookies" de su Navegador

Muchos sitios de Internet utilizan "cookies". Estos son archivos pequeños con información acerca de usted o su sesión de Internet actual. Algunas de estas cookies son útiles para algunos sitios que usted visita con frecuencia, pero muchas son solamente útiles para compañías que gustan de llevar un seguimiento del uso suyo en Internet. Usted se sorprendería de saber cuántas cookies tiene usted, incluso para sitios que usted no visitó específicamente. Periódicamente, usted debe deshacerse de estas cookies de sitios de los que usted no desea que exista la posibilidad de un seguimiento.

Muchos navegadores ofrecen ahora el modo de privacidad. Esta característica evita que el navegador almacene datos como cookies, archivos temporales de internet e historial. Los usuarios necesitan iniciar la navegación privada desde el menú del navegador. La sesión de navegación privada continuará entonces en el navegador actual o abrirá una ventana nueva del navegador.

Adicionalmente la mayoría de los navegadores le permite a usted "bloquear siempre" las cookies de ciertos sitios. Le recomendamos agregar a su categoría de "bloquear siempre" todo tipo de publicidad y otros sitios de los cuales usted no desea que exista un seguimiento.

Actualizaciones

Todos los sistemas operativos informáticos tienen brechas de seguridad en ellos, y la mayoría tiene un procedimiento para la obtención de 'parches' y actualizaciones de seguridad a través de Internet. Algunos también ofrecen actualizaciones de seguridad que pueden ser ordenadas en un CD-ROM. Las buenas prácticas de seguridad requieren diligencia, y mantenerse al día con las actualizaciones es parte de esa buena práctica de seguridad.

Computadoras Antiguas

Si usted está en condiciones de donar una computadora a una organización benéfica, a un pariente, amigo, etc., asegúrese que usted ha quitado correctamente toda la información personal de esa computadora y de sus componentes de almacenamiento (dispositivos de disco, cintas de respaldo, unidades USB, tarjetas de memoria, etc.) antes de que salga de su control. Usted necesita hacer más que simplemente eliminar los archivos. Cuando usted elimina un archivo, la computadora simplemente elimina la entrada en el "Contenido" pero en realidad no elimina la información donde reside el archivo. Cada dispositivo de almacenamiento de información (disco, cinta, tarjeta de memoria, etc.) debe, por lo menos, ser reformateada antes de que usted se deshaga de ella. También puede obtener programas que escribirán patrones de información aleatorios (varias veces) en los medios de transmisión para que cualquier dato que pudiera existir, sea borrado. Estos programas se conocen a veces como Servicios de "Borrado" ("Wipe" Utilities). Algunos de estos Servicios de Borrado cumplen con las normas de seguridad de datos del Departamento de Defensa de los Estados Unidos (DOD). Algunos sistemas informáticos de almacenamiento cuentan con sus propias características de "borrado seguro." Para obtener instrucciones respecto a la forma de eliminar por completo datos de su computadora personal, Demartek ha producido una guía llamada: "Cómo eliminar por completo datos de una unidad de disco" ([How to Fully Delete Data from a Disk Drive](#)).

Para aquellos que necesitan de seguridad adicional debido a que tienen información altamente confidencial, existen empresas más profesionales y procedimientos de tipo militar para borrar información, disponibles a un costo significativamente más alto. Estos métodos de borrado de datos requieren de un equipo especializado y, en algunos casos, ambientes especiales contenidos. Estos métodos pueden incluso evitar que los hackers u organizaciones más sofisticadas puedan obtener información que pudiera ser posible encontrar aun después de que se hubieren realizado procedimientos "ligeros" de borrado de datos. Estos métodos incluyen el uso de potentes imanes para desmagnetizar la superficie

de los medios magnéticos, el desensamblado de las unidades de disco y el lijado del material de óxido magnético; la aplicación de ácidos y otros químicos a la superficie de los medios y la trituración, fusión o destrucción de los medios de una manera física. Algunas variaciones de estos métodos pueden ser aplicados a discos, cintas, medios ópticos, medios tales como las unidades flash USB, tarjetas de memoria, etc.

Fraudes electrónicos (Phishing)

Muchos delincuentes intentan que usted les proporcione su información personal por correo electrónico (e-mail), utilizando una técnica conocida como "phishing." Ellos le envían una solicitud para recopilar información de usted, haciéndose pasar como un correo electrónico de un banco, un proveedor de servicios de Internet, un sitio de redes sociales, u otra institución en la que regularmente usted confiaría. El texto del correo generalmente hace referencia a una actualización del sistema, a posibles actividades fraudulentas con algunas cuentas, o a cualquier otra razón donde la información necesita ser "confirmada." Algunas veces estos correos le aconsejan suspender algunas cuentas hasta que la información haya sido confirmada. En muchos casos, estos intentos de fraude incluyen algún tipo de "formulario para clientes" adjunto al correo electrónico. Otros intentos dirigen a las personas a sitios web falsos que tienen nombres muy similares a los sitios web auténticos. Preste atención a la apariencia de los correos electrónicos de su banco y de otros sitios seguros. Muy a menudo, un correo fraudulento lucirá muy similar pero con algo que tiende a ser un tanto diferente.

El "Spear Phishing" es una forma de phishing más específica, que puede venir en forma de correos electrónicos que parecieran venir de un jefe, compañero de trabajo, proveedor, etc. Éstas pueden incluir solicitudes de nombres de usuario y contraseñas. Algunos delincuentes sofisticados hacen una investigación de su víctima con el fin de seleccionar una línea de asunto que sería más probable que la víctima abriera y así evitar los filtros de spam.

El mejor curso de acción es considerar este tipo de mensajes como correo basura y simplemente eliminarlos. El banco u otra organización legítima seguramente ya tienen su información y no necesitan que usted confirme nada. Cuando tenga alguna duda, llame a la persona u organización marcando un número de teléfono conocido para confirmar que el correo electrónico sí sea de ellos. Si usted siente la necesidad de adoptar medidas adicionales, usted puede reenviar el correo electrónico a la dirección de correo electrónico del departamento de Fraudes de esa organización. Regularmente los bancos proporcionan

información acerca de intentos de fraude en su sitio web. Los bancos trabajan con los departamentos de policía y algunos proveedores de servicios de Internet para detener la fuente de estos correos electrónicos lo antes posible.

También es un buen hábito bloquear su computadora con una contraseña cuando usted se aleje de su puesto de trabajo, especialmente si contiene información confidencial. Esto disuadirá al ojo entrometido o a personas que pudieran acceder a su información sin su conocimiento.

Se está haciendo cada vez más popular el recibir correos electrónicos de compañías después de haber creado una cuenta (generalmente cuentas de consumidor o de compras). Al proporcionar información bancaria a una compañía, asegúrese de leer la letra pequeña. Donde antes había que “seleccionar” las casillas para suscribirse a los servicios, ahora es común que estas casillas ya estén seleccionadas. En estos casos, desactívelas para excluir productos adicionales o servicios. También se está convirtiendo en práctica habitual de las empresas tener “Términos y Condiciones” o una “Política de Privacidad” al realizar negocios que requieran su aceptación. No pase esto por alto y no acepte sin leer lo que está aceptando. Esta es un área en la que no leer la letra fina puede conllevar cargos o tarifas adicionales que no pueden revertirse porque usted las ha aceptado previamente.

Contraseñas

Existen por lo menos 5 categorías de malas contraseñas. Usted debe escoger contraseñas que no caigan en ninguna de estas 5 categorías. Las contraseñas seguras utilizan una mezcla de letras, números, y caracteres especiales. Elija una contraseña que usted pueda recordar, pero que sea lo suficientemente segura como para proteger la información detrás de ella. También debe usted memorizar sus contraseñas y no debe intentar escribirlas. Para una mayor protección, cambie sus contraseñas periódicamente, especialmente en los sitios web que contengan información financiera.

A continuación encontrará sugerencias para tener en cuenta a la hora de elegir una contraseña:

- ◆ **Contraseña en blanco** – No tener contraseña es totalmente inseguro y simplemente invita al robo.
- ◆ **Contraseña sencilla** – Las contraseñas sencillas son aquellas a las que usted le tomó poco tiempo elegir y que a los ladrones les tomará poco tiempo adivinar.

La palabra contraseña y la palabra secreta son 2 ejemplos. Existen herramientas automatizadas de ataque que intentarán adivinar las contraseñas. Entre otros ejemplos de este tipo de contraseñas (tomados de algunas de estas herramientas automatizadas de ataque) se encuentran: abc, admin, administrator, debug, diag, god, guest, home, owner, pass, root, server, sexy, test, user, xyz, 111, 123, 321, 1234, 4321, 111111, abcdefg, abc123, asdfgh, entre otras. Existen un sinnúmero de ejemplos en Internet de este tipo de contraseñas deficientes las cuales un hacker puede encontrar con una simple búsqueda.

- ◆ **Contraseña predeterminada** – Se trata de cualquier contraseña predeterminada suministrada por algún proveedor. Estas son muy fáciles de obtener a través de Internet en pocos minutos. Usted debe cambiar la contraseña predeterminada por alguna bajo su solo control tan pronto como sea posible.
- ◆ **Contraseña con Información Personal** – Es cualquier contraseña basada en información personal tal como nombres de su cónyuge, hijos, mascotas, equipo deportivo favorito, cantante o grupo favorito, cumpleaños, número de placas de carro, etc. Si un ladrón sabe algo acerca de usted (y muchas veces lo sabe), eso podría ser una pista para adivinar su contraseña.
- ◆ **Contraseñas Repetidas** – Esto es utilizar la misma contraseña para todo. Si un ladrón logra 'hacker' una de sus cuentas, esa persona podrá acceder a todos sus movimientos y robar toda su información sensible. Es una buena idea tener múltiples contraseñas e idear una contraseña especial para sus cuentas de banco en línea, completamente diferente de las que usted utiliza en su correo electrónico o en sitios de redes sociales.



Dispositivos Móviles

A pesar de que muchos consumidores están conscientes de los peligros que el Internet representa para las computadoras personales, es importante recordar que muchas de estas mismas amenazas se aplican a los dispositivos móviles que utilizan Internet. Aunque algunos dispositivos móviles proporcionan protección básica contra sitios "phishing", resulta imposible bloquear todo, así que no introduzca información confidencial en sitios cuestionables. Asegúrese que las contraseñas no sean almacenadas en su dispositivo móvil— esto facilitaría a los ladrones el acceso a toda su información personal. Si es necesario que usted guarde contraseñas en su dispositivo móvil, asegúrese de utilizar un algoritmo de encriptado fuerte y conocido. Como regla general, los usuarios de dispositivos móviles deben ejercer la misma cautela que se tiene al usar una computadora.

Sitios Web de Redes Sociales

Con la popularidad de los sitios de redes sociales como Facebook, LinkedIn, My Space, Twitter, etc., hay algunas "prácticas" de sentido común que se deben seguir para reducir la posibilidad del robo de identidad. Lo fundamental es recordar que las cosas publicadas en Internet tienden a tener una larga vida, y una vez publicadas, se copian a múltiples locaciones y son extremadamente difíciles de remover. Una vez "en la luz" los muchos motores de búsqueda hacen un índice y una lista de toda esta información para que cualquier persona alrededor del mundo, incluyendo criminales, puedan encontrarla.

A medida que surgen más y más sitios de redes sociales y los usuarios tienen cuentas en muchos de ellos, empezamos a enfrentar problemas relacionados con la cantidad de información potencialmente perjudicial que las personas hacen pública. Sea cauteloso con la cantidad de información personal que ingresa en estos sitios de redes sociales y mantenga un perfil relativamente bajo en todos ellos. Es mejor omitir información como dirección, números telefónicos, fechas de cumpleaños, múltiples direcciones de correo, etc. Cuanta más información haga pública, más información tendrá el ladrón para hacerse una imagen de usted, facilitando la obtención de información confidencial.

Entre más información personal usted haga pública, más fácil será que usted se convierta en una víctima del robo de identidad.

Además de limitar la cantidad de información que usted hace pública, es sabio familiarizarse de manera regular con las configuraciones de privacidad de su cuenta. A menos que una persona sea amiga o familiar, es mejor dificultar a los extraños el acceso a su información e imágenes. Igualmente, antes de permitir que alguien vea su perfil o cuenta completa (aceptar una “solicitud para hacerse amigo”), asegúrese de conocer a la persona. Los ladrones pueden fácilmente incluirse dentro de sus amigos para obtener información y luego utilizarla en otras partes para acceder a sus datos privados.

Además de estos consejos, algunos medios de comunicación social (como Twitter) han aumentado los niveles de seguridad para sus usuarios con un sistema de autenticación doble. Esto exige que el usuario tenga dos contraseñas: La primera es a menudo un código que se le envía como mensaje de texto al teléfono móvil. Aunque esto aumenta el nivel de seguridad, también disminuye el nivel de comodidad del usuario.

Con esta premisa básica en mente, considere cuidadosamente la información personal que usted publica en los sitios de redes sociales. Revise detalladamente las políticas de confidencialidad en estos sitios y personalice la configuración de privacidad de su cuenta para que su información personal permanezca tan segura como sea posible.

Intentos de Fraude Comunes

La siguiente lista contiene algunos de los fraudes prevalentes que se encuentran en circulación. Existen numerosas variaciones de cada esquema, pero los elementos básicos son los mismos. Es esencial que las personas sean escépticas y recuerden que, si parece muy bueno para ser verdad, ¡probablemente lo es!

Cuando se trate de ofertas de productos o servicios recuerde que, si parece muy bueno para ser verdad, ¡probablemente lo es!

- ◆ **Fraudes Nigerianos 419/Lotería Extranjera** – Un fraude de correo regular y correo electrónico es el de alguien que dice ser extranjero y que necesita ayuda para transferir una gran cantidad de dinero fuera del país. El número "419" se refiere al Código Penal Nigeriano que se ocupa de estos crímenes. Como incentivo, el estafador ofrece al destinatario un porcentaje del dinero a cambio de su ayuda. El

estafador solicita al destinatario cubrir algunos de los costos iniciales con la promesa de reembolsarlos, y luego elabora razones por las cuales "la transferencia de la fortuna" está siendo aplazada. La mejor forma de protegerse es eliminar este tipo de correos inmediatamente.

Un fraude similar involucra a un representante de una falsa lotería extranjera que dice que usted ha ganado una fortuna y que sólo necesitan su número de cuenta para transferir el dinero a su banco. Como con todos los fraudes de este tipo, no responda.

- ◆ **Estafas en Craigslist** – Cuando realice compras en Craigslist o sitios de internet similares, especialmente compras significativas como vehículos o propiedades de alquiler, asegúrese de conocer a la parte involucrada. En muchas ocasiones los negocios en Craigslist parecen demasiado buenos para ser verdad ¡y a menudo lo son! Con frecuencia, los vendedores solicitarán que se les envíe dinero por diversas razones, una de ellas tal vez porque vivan fuera del estado. Siempre dude en enviar dinero a alguien por vía electrónica. Muchas veces los estafadores solicitarán que se les envíe dinero por los productos o servicios prometidos y luego dejarán de comunicarse una vez que lo hayan recibido. Igualmente, evite aceptar cheques como método de pago, ya que pueden rebotar cuando los lleve al banco para cambiarlos. Lo mejor es realizar transacciones personalmente y, de ser necesario, ambas partes involucradas deberán asegurarse conjuntamente de que se disponga de los fondos (es decir, cobrar los cheques o pagos). Esto garantizará que la transacción se realice sin perder dinero ni posesiones.
- ◆ **Estafas involucrando obras de beneficencia** – Después de un desastre natural o de una crisis, muchas personas sienten el deseo irresistible de ayudar, a menudo ofreciendo donativos en efectivo a obras benéficas. Desafortunadamente, después de este tipo de eventos surgen muchas organizaciones fraudulentas que falsamente afirman estar recaudando dinero para las víctimas. Algunas incluso utilizan esquemas *phishing*, y envían correos electrónicos para intentar obtener información personal y bancaria de las personas. Es mejor donar a organizaciones conocidas tipo la Cruz Roja.
- ◆ **Fraudes a Abuelos** – Un estafador llama a una persona de la tercera edad, casi siempre a mitad de la noche, fingiendo ser un hijo o un nieto. El estafador dirá que se encuentra en algún tipo de problema, generalmente en otro país o lugar

distante, y le pedirá a la víctima que le envíe algo de dinero. El estafador dirá también que no desean que el resto de la familia sepa sobre la situación, como para convencer a la víctima de no hacer llamadas para verificar la situación. Si usted se encuentra en esta situación, no proporcione ningún número de cuenta de banco o de tarjeta de crédito. Haga preguntas específicas que sólo sus verdaderos familiares podrían contestar. Si la persona en el teléfono sigue pareciendo legítima, dígame que usted le devolverá la llamada, y aun si la persona le diera otro número de teléfono diferente al de la persona que supuestamente llama, marque el número que usted tiene registrado para esa persona o el número de los padres de ella o su cónyuge. Lo más probable es que usted se dé cuenta que su familiar está realmente a salvo y en su casa. Finalmente, notifique a las autoridades.

- ◆ **Fraudes a través de Redes Sociales** – En esta versión moderna de los Fraudes a Abuelos que acabamos de hablar, un 'hacker' obtendrá la contraseña de algún sitio web de redes sociales, tal como Facebook, LinkedIn, MySpace, Twitter, etc., y enviará un mensaje que parezca ser enviado por usted a muchos o todos sus amigos en línea, diciéndoles que usted se encuentra en problemas y necesita dinero. El 'hacker' puede también cambiar la contraseña de usted para que usted no pueda tener acceso a su propia cuenta de red social. Es importante tener una contraseña segura para los sitios de redes sociales y mantenerla separada del resto de sus contraseñas. Si usted se da cuenta de que alguien que usted conoce parece estar comportándose de manera extraña en una red social, envíele un correo personal para decirle que su cuenta pudo haber sido intervenida.
- ◆ **Fraudes con Seguros médicos** - Las personas a veces se dan cuenta de que son víctimas de un fraude de identidad cuando reciben una factura médica o un aviso de su compañía de seguros sobre una atención médica que no recibieron. Aunque algunos hospitales están utilizando escaneos de iris del ojo y de palma digitales para verificar la identidad de sus pacientes, ninguna tecnología es cien por ciento segura. Estos casos de robo de identidad surgen en menor grado por tarjetas de seguro perdidas y más a menudo por "trabajos internos". Las víctimas de fraude con seguros médicos deben presentar un reporte policiaco y contactar al proveedor médico y a la compañía de seguros médicos indicando por escrito los detalles del fraude, asegurándose de incluir el reporte policiaco.
- ◆ **Fraudes en el Censo de los Estados Unidos** – La Oficina del Censo de los Estados Unidos alerta sobre posibles fraudes en torno al Censo. Aunque probablemente

usted reciba un correo electrónico o una llamada telefónica en relación al Censo, es importante que usted sepa que la Oficina del Censo no pedirá su Número de Seguro Social, ni su Número de Identificación Personal (NIP), o números de Cuentas de Bancos o de Tarjetas de Crédito. Para denunciar cualquier fraude de correo electrónico visite:

http://www.census.gov/survey_participants/related_information/phishing_email_scams_bogus_census_web_sites.html.

Un trabajador del Censo probablemente lo visitará en su casa, pero le mostrará una tarjeta de identificación del Censo y usted puede, además, solicitar ver otra forma de identificación con fotografía. Si usted se siente incómodo, debe saber que usted no está legalmente obligado a permitir a tal persona del Censo que entre a su casa.

- ◆ **Fraudes en los citatorios a servir como Jurado** – Muchos estados han emitido advertencias acerca de fraudes que involucran personas que se hacen pasar como funcionarios de la Corte. Los falsos oficiales pueden decirle que existe una orden de arresto en su contra después de que usted falló al no presentarse a servir como jurado. Si usted dice que no recibió un Citatorio para servir como jurado, ellos le preguntarán por su Número de Seguro Social y fecha de nacimiento prometiéndole aclarar el asunto. Pueden inclusive pedirle información de su tarjeta de crédito para cobrarle una multa. Si usted recibe una llamada de éstas, no proporcione ningún tipo de información personal y contacte a sus autoridades locales. Los oficiales de la corte jamás solicitarán de usted información confidencial a través del teléfono y la mayoría de la comunicación entre los tribunales y los jurados se lleva a cabo a través del correo. Para mayor información acerca de los Citatorios para servir como Jurado, contáctese con las oficinas de las cortes locales.
- ◆ **Estafas laborales** – Antes de proporcionar información personal en respuesta a un anuncio sobre trabajo, asegúrese de saber quién es la persona o compañía con la que está tratando. Es mejor dar esta información solo en persona y no por teléfono o por correo electrónico.
- ◆ **Fraudes de Pornografía Infantil** – Los usuarios desprevenidos pueden ser bombardeados por virus que depositan pornografía infantil en sus computadoras personales. Los pedófilos pueden usar el equipo de usted para acumular este tipo de imágenes sin preocuparse de que lo atrapen. Sin embargo, no sólo las imágenes se quedan en su computadora con el peligro de que algún familiar o amigo las vea, sino que, si esto llegara a manos de las autoridades, podría llevarlo a usted a la

cárcel, causarle la pérdida de su trabajo y costarle miles de dólares para limpiar su nombre. La mejor manera de evitar esta horrible situación es proteger su computadora de los virus, utilizando un buen firewall, un programa antivirus y siendo siempre cuidadoso de los sitios web que usted visita.

Hijos

Además de proteger la propia identidad, mucha gente necesita considerar proteger la identidad de sus hijos. Muchos casos de robo de identidad han sucedido con bebés o niños muy pequeños porque su información personal fue robada. En algunos casos de divorcio, un padre que tenga una mala reputación puede tratar de utilizar la identidad del niño para obtener servicios como teléfono, servicios públicos, etc. También se está volviendo muy común obtener el número de Seguro Social de un niño y utilizarlo para solicitar préstamos, tarjetas de crédito, empleos, etc. Esto va en aumento debido a la falta de supervisión en la información personal de los niños. Muchas personas no piensan que la información personal de su hijo pueda ser utilizada para cometer un fraude, por eso éste puede continuar durante mucho tiempo o en muchas formas, antes de que el afectado se dé cuenta.

Es una buena idea tomar las mismas medidas provistas en los apartados anteriores cuando se trata de sus niños pequeños, y es importante enseñarles a ellos a hacerlo por sí mismos cuando ya han crecido. También resulta una buena práctica informar a sus hijos de la importancia de mantener segura la información privada. Si sus hijos tienen acceso a su información confidencial o si estuvieron presentes cuando usted estableció alguna información confidencial, es mejor recordarles la importancia de no permitir que los demás la conozcan. Si sospecha que puede haber problemas con alguno de sus hijos y con el uso no autorizado de cualquier información confidencial, usted puede tomar medidas para cambiar esta información e impedir cualquier violación futura.

Es una buena práctica el informar a sus hijos de la importancia de mantener segura la información privada.

Otras fuentes de información y asistencia

Existen numerosas fuentes de información en relación al robo de identidad, incluyendo qué hacer si usted es una víctima de robo de identidad. A continuación proporcionamos varias de

estas fuentes, las cuales han sido víctimas ellos mismos y describen el tipo de problemas que experimentaron en el camino a limpiar el desorden que produjo el robo de identidad.

Algunas son organizaciones que promueven los derechos de confidencialidad las cuales ofrecen excelente información. Otras son agencias gubernamentales que brindan ayuda.

Otras fuentes proporcionan antecedentes sobre leyes que han sido aprobadas o proyectos de ley que se han propuesto para hacer frente al robo de identidad.

Organizaciones

Las organizaciones mencionadas a continuación poseen información excelente en el tema del robo de identidad y explican qué hacer en cuanto a él. También proporcionan información en temas relacionados como el de la confidencialidad. Sus vínculos de Internet se muestran aquí simplemente para su referencia. Algunas son organizaciones sin fines de lucro:

- ◆ <http://www.privacyrights.org/identity.htm>
- ◆ <http://www.idtheftcenter.org>
- ◆ <http://www.pirg.org/consumer/credit>
- ◆ <http://www.identitytheft.org>
- ◆ <http://www.vaonline.org/fraud.html>
- ◆ <http://www.identity-theft-help.us>
- ◆ <http://www.fraudcast.ca>
- ◆ <http://www.abcfraud.ca>

Historias de Robo de Identidad

Existen un sinnúmero de historias sobre víctimas del robo de identidad. Los problemas enfrentados por estas víctimas incluyen cheques que no son aceptados, cartas de agencias de recolección o cobro por cosas compradas por el ladrón de identidad; pérdida de trabajos, arrestos hechos por error, cateos a casas y muchos otros. Consulte su fuente de noticias preferida y seguramente encontrará muchas historias sobre robos de identidad. Es siempre una buena idea mantenerse al día en cuanto a las nuevas formas de engaño que los estafadores están utilizando.

Leyes y Reglamentos

Se han promulgado leyes y se han aprobado reglamentos que son un intento de llamar la atención sobre el problema de las violaciones a la seguridad de datos. Estos son una respuesta a una actitud de descuido por parte de algunas empresas, universidades y agencias gubernamentales con respecto a proteger la confidencialidad de cierta información. Varias personas han acusado a estas organizaciones de irresponsabilidad y negligencia. Este tipo de brechas de seguridad informática son perfectas para una demanda colectiva, ya que un buen número de organizaciones han encabezado los titulares de noticias por las razones equivocadas. Existen demasiados casos como para mencionarlos aquí, pero una búsqueda de "brechas de información" o "brechas de seguridad" proporcionará abundante información acerca de compañías que han sufrido de brechas de seguridad en la información.

- ◆ **Acta sobre las Brechas de Seguridad de la Información en California** (efectiva a partir del 01 de Julio de 2003) – Esta ley, también conocida como la SB 1386, exige a las empresas y a los gobiernos notificar a los individuos si una base de datos conteniendo cierta información personal está comprometida. Afecta a aquellas organizaciones que tienen a residentes de California como sus compradores o clientes. Especifica que se requiere una notificación individual, o en casos donde un gran número de personas puede ser afectado, esa notificación puede venir a través de los medios de comunicación.

- ◆ **Junta de la Reserva Federal de los Estados Unidos** (efectiva a partir del 23 de Marzo de 2005) – En respuesta a algunas de las recientemente publicadas brechas de seguridad, la Reserva Federal de los Estados Unidos emitió un fallo que establece que "cuando una institución financiera se da cuenta de un incidente de acceso no autorizado a información confidencial de sus clientes, la institución deberá conducir una investigación razonable para determinar la probabilidad de que la información ha sido o será usada mal... Si la institución determina que el mal uso de la información de un cliente ha ocurrido o es razonablemente posible que ocurra, debe notificar al cliente afectado tan pronto como sea posible." Los detalles se pueden encontrar en:
<http://www.federalreserve.gov/BoardDocs/Press/bcreg/2005/20050323/default.html>

- ◆ **Comisión Federal de Comercio de los Estados Unidos** (efectiva a partir del 08 de Julio de 2008) – Las instituciones financieras y los acreedores están obligados a elaborar e implementar programas escritos sobre la prevención de robo de identidad en el marco del nuevo "Reglamento de Alertas Rojas" (Red Flag Rules).

Este reglamento es parte de la "Ley de Transacciones de Crédito Justas y Precisas" (Fair and Accurate Credit Transactions Act o FACT) del año 2003. Según estas normas, las instituciones financieras y los acreedores con cuentas cubiertas deben tener programas de prevención de robo de identidad funcionando a partir del 01 de Noviembre de 2008, para poder identificar, detectar y responder a patrones, prácticas o actividades específicas que pudieran indicar un robo de identidad. Los detalles están disponibles en: <http://ftc.gov/opa/2008/07/redflagsfyi.shtm>

California fue el primer estado en aprobar una Ley de Notificación de Brechas de Seguridad, y la mayoría de los estados siguieron su ejemplo, promulgando leyes que requieren la notificación de brechas de seguridad que involucren información personal. Existe un debate en el Congreso de los Estados Unidos de una ley nacional similar a la ley de California, aunque esa legislación no ha sido aprobada todavía. Al momento de escribir este documento, 44 de los estados de la Unión Americana habían aprobado leyes similares a la ley de California.

Congelamientos de Crédito y Alertas de Fraude

Otra táctica disponible para que los consumidores puedan protegerse a sí mismos antes de que ocurra un robo de identidad, es el concepto de un "congelamiento" del crédito. Una vez que usted ha congelado sus archivos de crédito, los nuevos prestamistas no podrán tener acceso a la información de su cuenta. Esto impedirá que los ladrones puedan abrir nuevas cuentas bajo el nombre de usted. Mientras que esto puede ser un sistema de prevención viable para algunos, puede causar dolores de cabeza extra si su reporte de crédito se accede con frecuencia. Cada vez que usted desee abrir una nueva cuenta, usted tendrá que llamar a los burós de crédito para "descongelar" su cuenta. La mayoría de los estados han promulgado leyes de congelamiento de seguridad, a pesar de que las normas varían por estado.

Actualmente, Canadá no tiene ninguna ley sobre congelamiento de crédito, sin embargo los burós de crédito en Canadá y los Estados Unidos colocarán una alerta de fraude en su cuenta si usted sospecha que ha sido víctima de robo de identidad. Cuando una alerta de fraude se adjunta a su reporte de crédito, los acreedores necesitan ponerse en contacto con usted antes de abrir una nueva cuenta en su nombre. Una alerta de fraude inicial, permanece en su reporte de crédito por 90 días. Una alerta de fraude extendida, permanece en su reporte de crédito por 7 años, pero requiere de un Reporte de Robo de Identidad de parte de la policía para confirmar que usted ha sido una víctima.

Burós de Crédito

Las agencias de crédito principales en los Estados Unidos y Canadá se enumeran a continuación. En el caso de un robo de identidad, asegúrese de contactarlos para poner una alerta de fraude o congelamiento de crédito en su informe de crédito. También pueden ser contactados para obtener una copia de su informe de crédito o de algún conflicto que pudiera haber surgido.

Equifax

1-866-685-1111

[Sitio Web](#)**Experian**

1-888-397-3742

[Sitio Web](#)**TransUnion**

1-800-888-4213

[Sitio Web](#)**Equifax Canada**

1-800-465-7166

[Sitio Web](#)**TransUnion Canada**

1-800-663-9980

[Sitio Web](#)**TransUnion Canada****(Echo Group)**

1-877-713-3393

En los Estados Unidos, la Ley de Informe de Crédito Justo (Fair Credit Reporting Act) impuesta por la Comisión de Comercio Federal, garantiza a los consumidores el acceso a un informe de crédito anual gratuito. Para solicitar una copia de su informe de crédito gratuito, visite <https://www.annualcreditreport.com>. Los residentes de Canadá también tienen derecho a un informe de crédito gratuito una vez al año, aunque están obligados a enviar una solicitud a los burós de crédito junto con copias de identificación y comprobante de domicilio. Visite los sitios web de los burós de crédito para más información.

Pasaportes de Robo de Identidad

Algunos estados de la Unión Americana tienen un programa muy interesante llamado el Pasaporte de Robo de Identidad, el cual provee verificación por parte del gobierno de que una persona ha sido víctima de robo de identidad, a fin de evitar un arresto falso y proporcionar algún otro tipo de asistencia. Los programas no son idénticos, pero funcionan en forma muy similar. La premisa básica es que una víctima de robo de identidad complete una declaración jurada, certificando que es una víctima. Esta declaración incluye información acerca del

reporte de la policía y otra específica acerca de la víctima y del delito. Esta declaración jurada se presenta a la Dirección General del Estado o al Buró Federal de Investigaciones (FBI). Normalmente se requieren una foto, huellas digitales u otras formas de identificación positiva junto con la declaración jurada. Después de un período de investigación, la agencia estatal expide un "Pasaporte de Robo de Identidad" el cual puede ser presentado a las autoridades pertinentes cuando sea necesario. Cuando éste es presentado a las autoridades, ellos realizarán un chequeo dentro de una base de datos especial de robo de identidad para verificar la identidad de la persona que porta el Pasaporte de Robo de Identidad. El proceso para obtener un Pasaporte de Robo de Identidad puede incluir también la remoción de los registros erróneos tales como arrestos, cargos, etc. Normalmente, la información acerca de un Pasaporte de Robo de Identidad específico es sellada y no es considerada como un documento público. Debido a que cada caso de robo de identidad puede ser único, las medidas concretas adoptadas en cada caso pueden variar ligeramente. En la actualidad, el reto principal es la sensibilización a los programas, tanto por parte de las víctimas de robo de identidad como por parte de las autoridades.

No está claro si el Pasaporte de Robo de Identidad expedido en un Estado será aceptado en otro diferente. Otros Estados están considerando programas similares al de Pasaporte de Robo de Identidad, y seguramente veremos más en el futuro. Existe la posibilidad de que el gobierno federal vaya a crear un pasaporte nacional de robo de identidad. A continuación se encuentra una lista de recursos para los programas de pasaporte de robo de identidad.

Estado	Enlaces para Información del Programa de Pasaporte de Robo de Identidad
Arkansas	http://arkansasag.gov/programs/schools-educators-and-communities/id-theft/id-theft-passport/
Delaware	http://attorneygeneral.delaware.gov/consumers/protection/idtheft.shtml
Iowa	http://www.iowa.gov/government/ag/helping_victims/contents/IDPP.html
Maryland	http://www.oag.state.md.us/idtheft/IDTpassport.htm
Mississippi	Pasaporte ofrecido a víctimas con registros criminales falsos. Contacte a la Procuraduría de Justicia del estado.
Montana	https://doj.mt.gov/consumer/for-consumers/identity-theft
Nevada	http://ag.nv.gov/Hot_Topics/Victims/IDTheft_Passport

New Mexico	http://www.nmag.gov/consumer/investigations/nm-identity-theft-passport
Oklahoma	http://www.ok.gov/osbi/Criminal_History/Identity_Theft_Passport_Program
Virginia	http://www.oag.state.va.us/Programs%20and%20Resources/Identity_Theft

Similar en algunos aspectos al programa de pasaporte de robo de identidad es el proceso que se sigue en algunos estados, de borrar algunos registros de la corte pertenecientes a víctimas del robo de identidad. Aquí las víctimas necesitan hacer una petición al Tribunal de Justicia en determinadas jurisdicciones, además de que este proceso no tiene una organización centralizada como los programas de pasaporte de robo de identidad.

Seguro contra el Robo de Identidad

Recientemente se ha hecho disponible un seguro que proporciona cierta asistencia para las víctimas de robo de identidad. Muchas compañías de seguros están ofreciendo seguros contra robo de identidad como un aval para la póliza de seguro de un propietario o un arrendador de casa, o como pólizas autónomas. Algunos bancos están ofreciéndolos con cuentas de cheques mientras que ciertas empresas lo ofrecen como una prestación.

Estas pólizas suelen costar menos de \$100 dólares y ofrecen de \$15,000 a \$25,000 de cobertura. Es importante notar que este tipo de pólizas no cubren pérdidas monetarias directas sufridas como consecuencia de un robo de identidad. Este seguro proporciona reembolso de los gastos relacionados con la recuperación de robo de identidad. Algunos de los gastos, tales como los honorarios de abogados, pueden requerir un consentimiento previo de la aseguradora.

Agencias Gubernamentales

Las agencias gubernamentales proporcionan una gran cantidad de información acerca de los robos de identidad y qué hacer al respecto. Muchas de ellas se encuentran en la lista a continuación, la cual incluye a los Estados Unidos y Canadá.

Canadá – Nacional

- ◆ <http://www.publicsafety.gc.ca/prg/le/bs/consumers-eng.aspx/////>
- ◆ [FR] <http://www.securitepublique.gc.ca/prg/le/bs/report-fra.aspx/////>
- ◆ <http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-eng.htm>
- ◆ [FR] <http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimesfra.htm>
- ◆ http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp

- ◆ [FR] http://www.priv.gc.ca/fs-fi/02_05_d_10_f.cfm

Estados Unidos– Nacional

- ◆ <http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html>
- ◆ [ES] <http://www.consumidor.ftc.gov/destacado/destacado-s0014-robo-de-identidad>
- ◆ [ES] http://www.ftc.gov/index_es.shtml
- ◆ <http://www.justice.gov/criminal/fraud/websites/idtheft.html>
- ◆ <http://www.ojp.gov/programs/identitytheft.html>
- ◆ [ES] <http://www.ojp.usdoj.gov/ovc/library/espanol.html>
- ◆ <http://www.irs.gov/uac/Identity-Protection>
- ◆ <http://www.secretservice.gov/criminal.shtml>
- ◆ <http://publications.usa.gov/USAPubs.php?NavCode=XA&CatID=12>
- ◆ [ES] <http://publications.usa.gov/USAPubs.php?NavCode=XA&CatID=13>

Canadá – Provincias y Territorios

Alberta

- ◆ <http://www.servicealberta.gov.ab.ca/560.cfm>
- ◆ http://www.servicealberta.gov.ab.ca/pdf/tipsheets/Identity_theft.pdf
- ◆ <http://www.albertacanada.com/immigration/living/identitytheft.html/////>
- ◆ <http://www.lawcentralalberta.ca/LawCentralAlberta/default.aspx>

Columbia Británica

- ◆ <http://www2.gov.bc.ca/gov/topic.page?id=2A477231EF934E22B0FBC8C43A98B9D9>
- ◆ <http://www.nwpolice.org/community-services/crime-prevention9/crime-prevention-education/identity-theft/>
- ◆ <http://www.richmond.ca/safety/police/personal/idtheft.htm>

La Isla Prince Edward

- ◆ http://www.cliapei.ca/content/page/front_news/id/40

Manitoba

- ◆ <http://www.gov.mb.ca/cca/cpo/identity.html>
- ◆ <http://www.gov.mb.ca/finance/cca/consumb/identity.html/////>

Nuevo Brunswick

- ◆ <http://www.gnb.ca/cnb/promos/justice/theft-e.htm>
- ◆ <http://www.gnb.ca/0062/Rentalsman/CA/faqs-e.asp>

Nueva Escocia

- ◆ http://www.gov.ns.ca/just/prevention/tips_consumer_IDtheft.asp

- ◆ <http://www.gov.ns.ca/snsmr/access/individuals/consumer-awareness/consumer-alerts/identity-theft.asp>
- ◆ http://novascotia.ca/seniors/partners_against_fraud.asp

Ontario

- ◆ <http://cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00084.html>
- ◆ <http://www.opp.ca/ecms/index.php?id=133>
- ◆ **[FR]** <http://www.opp.ca/ecms/index.php?id=355>

Quebec

- ◆ **[FR]** <http://www4.gouv.qc.ca/FR/Portail/Citoyens/Evenements/proteger-identite-Internet/Pages/accueil.aspx>
- ◆ **[FR]** <http://cacq.ca/Vol-d-identite-Attention>

Saskatchewan

- ◆ <http://www.justice.gov.sk.ca/identity-theft>
- ◆ <http://www.justice.gov.sk.ca/TipIdentityTheft-Jan2008.pdf>

Terranova y Labrador

- ◆ http://www.servicenl.gov.nl.ca/consumer/consumer_affairs/ident_en.html
- ◆ <https://www.nlcu.com/Home/ProductsAndServices/YourMoney/FraudAwareness>

Territorios del Noroeste

- ◆ <http://www.justice.gov.nt.ca/VictimServices/index.shtml>
- ◆ <http://www.gov.ns.ca/snsmr/pdf/ans-consumer-identity-theft.pdf>

EUA – Estados, Estados Libres Asociados, Territorios, y El Distrito de Columbia

La Conferencia Nacional de Legislaturas Estatales tiene una lista muy útil de las Leyes de Robo de Identidad por Estado. No todos los estados tienen leyes específicas para el robo de identidad.

- ◆ <http://www.ncsl.org/programs/lis/privacy/idt-statutes.htm>

Aunque la mayoría de los estados proporcionan materiales en línea sobre el robo de identidad, muchos han hecho su información más accesible y fácil de encontrar que otros. Estos recursos se encuentran a menudo a través de la Dirección General del Estado o las Agencias de Protección al Consumidor, a través del Estado mismo o de Departamentos de

Policía locales. Algunas de estas direcciones URL son bastante largas, sin embargo se encuentran vigentes al día de esta publicación.

Alabama

- ◆ <http://www.ago.state.al.us/Page-Consumer-Protection>
- ◆ <http://www.ago.state.al.us/File-Consumer-Protection-Brochure-Identity-Protection>
- ◆ <http://alabamaidtheft.com/>
- ◆ <http://www.identitytheftportal.com/alabama.html>

Alaska

- ◆ <http://www.law.alaska.gov/department/civil/consumer/IDtheft.html>
- ◆ [ES] http://www.law.state.ak.us/department/civil/consumer/cp_spanish_brochures.html
- ◆ <http://www.identitytheftportal.com/alaska.html>

Arizona

- ◆ http://www.azdps.gov/Services/Crime_Victims/
- ◆ http://www.azag.gov/cybercrime/ID_Theft.html
- ◆ <http://identitytheftnetwork.org/arizona>
- ◆ <http://www.identitytheftportal.com/arizona.html>

Arkansas

- ◆ <http://arkansasag.gov/programs/schools-educators-and-communities/id-theft>
- ◆ <http://gotyourbackarkansas.org/identity/>
- ◆ <http://www.identitytheftportal.com/arkansas.html>

California

- ◆ <http://oag.ca.gov/idtheft>
- ◆ https://www.ftb.ca.gov/individuals/id_theft.shtml
- ◆ [ES] https://www.ftb.ca.gov/individuals/id_theft_spanish.shtml
- ◆ <http://www.identitytheftportal.com/california.html>

Carolina del Norte

- ◆ <http://www.ncdoj.com/Protect-Yourself/2-4-3-Protect-Your-Identity.aspx>
- ◆ <http://www.ncdot.gov/dmv/licensetheft/>

Carolina del Sur

- ◆ <http://www.justice.gov/usao/sc/programs/resources.html>
- ◆ http://www.scdmvonline.com/DMVNew/default.aspx?n=reporting_fraud

Colorado

- ◆ http://www.coloradoattorneygeneral.gov/initiatives/identity_theft
- ◆ <https://www.colorado.gov/cbi>
- ◆ <http://www.identitytheftportal.com/colorado.html>

Connecticut

- ◆ <http://www.ct.gov/dcp/cwp/view.asp?a=1629&Q=289476&PM=1>
- ◆ http://www.ct.gov/ag/cwp/browse.asp?A=2066&BMDRN=2000&BCOB=0&C=1920_0
- ◆ <http://www.identitytheftportal.com/connecticut.html>

Dakota del Norte

- ◆ <http://www.ag.state.nd.us/cpat/idtheft/idtheft.htm>
- ◆ <http://www.psc.nd.gov/public/consinfo/index.php>
- ◆ <http://www.ag.nd.gov/Brochures/FactSheet/IdentityTheft.pdf>

Dakota del Sur

- ◆ <http://atg.sd.gov/Consumers/IdentityTheft.aspx>

Delaware

- ◆ <http://attorneygeneral.delaware.gov/fraud/cpu/idtheft.shtml>

Florida

- ◆ <http://myfloridalegal.com/pages.nsf/Main/CBBEBA3F2583433385256DBA004BC600>
- ◆ **[ES]** <http://www.myfloridalegal.com/pages.nsf/0/CBBEBA3F2583433385256DBA004BC600?Open&LN=SP>
- ◆ <http://www.identitytheftportal.com/florida.html>

Georgia

- ◆ <http://consumer.georgia.gov/consumer-topics/identity-theft-1>
- ◆ http://law.ga.gov/00/article/0,2086,87670814_87670971_88025112,00.html
- ◆ <http://investigative.gbi.georgia.gov/identity-theft>
- ◆ <http://www.identitytheftportal.com/georgia.html>

Hawaii

- ◆ <http://ag.hawaii.gov/quick-links/id-theft/if-you-are-a-victim/>
- ◆ http://www.hawaii.gov/dcca/helping_hand/identity_theft
- ◆ <http://honoluluupd.org/information/index.php?page=identity>
- ◆ <http://www.identitytheftportal.com/hawaii.html>

Idaho

- ◆ http://cybersecurity.idaho.gov/identity_theft.html
- ◆ <http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf>
- ◆ [ES] <http://www.ag.idaho.gov/publications/spanish/InternetSafetySpanish.pdf>
- ◆ <http://www.identitytheftportal.com/idaho.html>

Illinois

- ◆ <http://www.ag.state.il.us/consumers/hotline.html>
- ◆ http://www.ag.state.il.us/consumers/consumer_publications.html
- ◆ [ES] http://www.ag.state.il.us/consumers/consumer_publications_span.html
- ◆ <http://illinoisissues.uis.edu/features/2002mar/name.html>

Indiana

- ◆ <http://www.in.gov/idoi/2561.htm>
- ◆ <http://www.in.gov/attorneygeneral/2349.htm>
- ◆ <http://www.in.gov/attorneygeneral/2409.htm>
- ◆ <http://www.in.gov/dfi/idtheft.pdf>

Iowa

- ◆ http://www.iowa.gov/government/ag/consumer_advisories/credit_finance/protect_privacy.html
- ◆ http://www.iowa.gov/government/ag/images/pdfs/Identity_Theft_GUIDE.pdf
- ◆ http://www.iowaattorneygeneral.org/consumer/brochures/avoid_identitytheft.html

Islas Vírgenes

- ◆ <http://www.idtheftcenter.org/States/virgin-islands.html>

Kansas

- ◆ <http://ag.ks.gov/consumer-protection/consumer-tips/protect-yourself>
- ◆ http://www.ksinsurance.org/consumers/id_theft.htm

Kentucky

- ◆ <http://ag.ky.gov/civil/consumerprotection/idtheft>

Luisiana

- ◆ <http://www.revenue.louisiana.gov/forms/Fraud/IdentityTheftChecklist.pdf>

Maine

- ◆ http://www.maine.gov/ag/consumer/identity_theft/identity_theft.shtml
- ◆ http://www.maine.gov/pfr/consumercredit/documents/identity_theft.htm

- ◆ http://www.maine.gov/pfr/financialinstitutions/consumer/credit_report.htm

Maryland

- ◆ <http://www.oag.state.md.us/idtheft/index.htm>
- ◆ <http://www.oag.state.md.us/consumer/idtheft.htm>

Massachusetts

- ◆ <http://www.mass.gov/ago/consumer-resources/consumer-information/scams-and-identity-theft/identity-theft/>
- ◆ <http://www.mass.gov/ago/docs/consumer/id-theft-guide.pdf>

Michigan

- ◆ http://www.michigan.gov/ag/0,4534,7-164-17337_20942-230557--,00.html
- ◆ http://www.michigan.gov/msp/0,1607,7-123-1589_35832---,00.html
- ◆ http://www.michiganlegalaid.org/library_client/resource.2005-05-29.1117417906674
- ◆ http://www.michigan.gov/documents/ID_Theft_94764_7.pdf

Minnesota

- ◆ <http://www.ag.state.mn.us/Consumer/Handbooks/GuardingYPrivacy/default.asp>
- ◆ <https://dps.mn.gov/divisions/ojp/help-for-crime-victims/Pages/Identity%20Theft.aspx>

Mississippi

- ◆ <http://www.ago.state.ms.us/publications/identity-theft-what-to-do-when-theres-more-than-one-you/>
- ◆ <http://www.ago.state.ms.us/publications/identity-theft-brochure-protecting-your-good-name/>
- ◆ <http://www.ago.state.ms.us/consumer-protection/identity-theft-affidavit/>

Missouri

- ◆ <http://ago.mo.gov/publications/idtheft.htm>
- ◆ <http://missourifamilies.org/features/consumerarticles/idtheft.htm>

Montana

- ◆ <https://doj.mt.gov/enforcement/investigations-bureau/computer-crime/>
- ◆ <https://doj.mt.gov/consumer/for-consumers/identity-theft/>

Nebraska

- ◆ http://www.ago.ne.gov/resources/dyn/files/392571za5a5011a/ fn/AGO_IDTheftBroch_122910.pdf
- ◆ <http://www.dmv.ne.gov/dvr/pdf/theftpacket.pdf>

Nevada

- ◆ [http://ag.nv.gov/About/Consumer Protection/Bureau of Consumer Protection/](http://ag.nv.gov/About/Consumer%20Protection/Bureau%20of%20Consumer%20Protection/)
- ◆ http://fightfraud.nv.gov/IdentityTheft_new.html

Nueva Jersey

- ◆ <http://www.state.nj.us/lps/dcj/idtheft.htm>
- ◆ <http://www.state.nj.us/lps/njsp/tech/identity.html>
- ◆ [ES] <http://www.state.nj.us/lps/ca/espanol/spbrief/identitytheftbus.pdf>
- ◆ http://www.state.nj.us/dobi/division_consumers/finance/identitytheft.htm
- ◆ <http://www.state.nj.us/dobi/creditreport6.htm>

Nueva York

- ◆ <http://www.ag.ny.gov/consumer-frauds-bureau/identity-theft>
- ◆ http://www.nyc.gov/html/dca/html/initiatives/identity_theft_prevention.shtml
- ◆ http://www.nyc.gov/html/dca/downloads/pdf/shredfest_biztips.pdf
- ◆ <http://www.longislandexchange.com/identity-theft.html>

Nuevo Hampshire

- ◆ <http://doj.nh.gov/consumer/sourcebook/identity-theft.htm>
- ◆ <http://www.doj.nh.gov/consumer/identity-theft/>

Nuevo Mexico

- ◆ <http://www.nmag.gov/consumer/for-students/identity-theft>
- ◆ <http://www.nmag.gov/consumer/investigations/nm-identity-theft-passport>
- ◆ <http://www.cabq.gov/police/prevention/identity.html>

Ohio

- ◆ <http://www.ohioattorneygeneral.gov/IdentityTheft>
- ◆ <http://www.ohioattorneygeneral.gov/Individuals-and-Families/Consumers/Identity-Theft>
- ◆ <http://www.pickocc.org/annualreports/2007/hotline.shtml>
- ◆ <http://www.sos.state.oh.us/Businesses/BusinessInformation/BusinessIdentityTheft.aspx>

Oklahoma

- ◆ <http://www.oag.ok.gov/oagweb.nsf/Consumer!OpenPage>
- ◆ <http://www.odl.state.ok.us/usinfo/pubs/idtheft.pdf>
- ◆ http://oklahomamoneymatters.org/Consumers/ID_Theft.shtml

Oregon

- ◆ http://www.doj.state.or.us/consumer/Pages/id_theft.aspx
- ◆ <http://www.oregon.gov/ODOT/DMV/driverid/idtheft.shtml>
- ◆ https://www.oregonlegislature.gov/citizen_engagement/Reports/2004IF_Identity_Theft.pdf

Pensilvania

- ◆ https://www.attorneygeneral.gov/Consumers/Bureau_of_Consumer_Protection/
- ◆ https://www.attorneygeneral.gov/Consumers/Identity_Theft/
- ◆ [ES] http://www.portal.state.pa.us/portal/server.pt/gateway/PTARGS_0_496447_0_0_18/identity_theft.pdf
- ◆ <http://www.dmv.state.pa.us/forms/idTheftReportingForms.shtml>

Puerto Rico

- ◆ [ES] http://www.justicia.gobierno.pr/rs_template/v2/DivEco

Rhode Island

- ◆ <http://www.doit.ri.gov/documents/security/Brochure%20Fight%20back%20against%20identity%20theft.pdf>
- ◆ <http://www.doit.ri.gov/documents/security/IRS%20ID%20Theft%20Message.pdf>
- ◆ http://www.risp.ri.gov/docs/Guide_Identity_Theft_RISP.pdf

Tennessee

- ◆ <http://tennessee.gov/attorneygeneral/cpro/identitytheft.html>
- ◆ <http://tennessee.gov/consumer/documents/IdentityTheftBrochurenew.pdf>

Texas

- ◆ http://www.oag.state.tx.us/consumer/identity_theft.shtml
- ◆ [ES] http://www.oag.state.tx.us/consumer/idtheft_span.shtml
- ◆ <http://www.oag.state.tx.us/newspubs/opeds/200302blues.shtml>

Utah

- ◆ <http://www.idtheft.utah.gov>
- ◆ <http://publicsafety.utah.gov/investigations/IDTheftlink.htm>

Vermont

- ◆ http://www.justice.gov/usao/vt/fraud_idtheft.html
- ◆ <http://www.justice.gov/usao/vt/vwdocs/VictimServicesDirectory.pdf>

Virginia

- ◆ <http://www.ag.virginia.gov/index.php/citizen-resources/identity-theft>
- ◆ <http://www.ag.virginia.gov/CCSWeb/Reports/IDTheftBook02.pdf>
- ◆ <http://www.dmv.virginia.gov/webdoc/citizen/drivers/identitytheft.asp>

Washington

- ◆ <http://www.atg.wa.gov/ConsumerIssues/ID-Privacy.aspx>
- ◆ <http://www.atg.wa.gov/ConsumerIssues/ID-Privacy/Tips.aspx>
- ◆ [ES] [http://www.atg.wa.gov/uploadedFiles/Home/Safeguarding_Consumers/Consumer_Issues_A-Z/Identity_Theft_\(Privacy\)/IDTheft_Consumer07-07%20Spanish.pdf](http://www.atg.wa.gov/uploadedFiles/Home/Safeguarding_Consumers/Consumer_Issues_A-Z/Identity_Theft_(Privacy)/IDTheft_Consumer07-07%20Spanish.pdf)
- ◆ <http://www.dol.wa.gov/driverslicense/identitycrimes.html>

Washington, D.C.

- ◆ <http://mpdc.dc.gov/page/identity-theft>
- ◆ <http://mpdc.dc.gov/node/206412>

West Virginia

- ◆ <http://www.ago.wv.gov/consumerprotection/Pages/default.aspx>
- ◆ <http://www.ago.wv.gov/consumerprotection/Documents/Identity%20Theft%20Brochure.pdf>

Wisconsin

- ◆ http://datcp.wi.gov/Consumer/Office_of_Privacy_Protection/index.aspx
- ◆ <http://cwagwisconsin.org/elder-law-center/wi-identity-theft-coalition/>
- ◆ <http://privacy.wi.gov/>
- ◆ [ES] <http://privacy.wi.gov/spanish/factsheets/FilingComplaintSPANISH.jsp>
- ◆ http://www.doj.state.wi.us/sites/default/files/dls/consumer-protection/ID_theft_broc.pdf
- ◆ [ES] http://www.doj.state.wi.us/sites/default/files/dls/consumer-protection/ID_theft_broc-sp.pdf

Wyoming

- ◆ <http://www.justice.gov/usao/wy/divisions/criminal/criminaldivision.html>
- ◆ http://www.uwyo.edu/studentatty/civil_criminal/civil_law/consumercredit/identitytheft.html
- ◆ <http://identitytheftnetwork.org/resource-map/wyoming>

Comentarios adicionales

Además de todos los diversos métodos para proteger su identidad y de hacer más difícil para los ladrones la tarea de obtener información personal, una de las mejores prácticas es la de estar actualizado en cuanto a las nuevas formas en las que su información puede verse comprometida. Con la velocidad con que avanzan las comunicaciones, incluyendo los nuevos métodos para los pagos de bienes y servicios, las maneras en que su identidad e información personal pueden ser robadas, sigue en aumento. Cualquier esfuerzo por mantenerse a la vanguardia frente a estas tendencias, siempre resultará en una mayor protección para usted y para sus seres queridos.