Demartek

Consejos para Prevenir el Robo de Identidad y Comentario

16 de Diciembre de 2009

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 de 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 de robo de identidad. Los temas cubiertos incluyen el manejo de documentos de papel, y asuntos relacionados con el teléfono y la computadora. También se proporcionan referencias de agencias gubernamentales que brindan información y asistencia, además de que se discuten algunas leyes actuales y otras que todavía son propuestas. Se incluye información específica para los Estados Unidos y para Canadá.

Este informe Demartek se ofrece en forma gratuita a todos nuestros clientes y amigos debido a la enorme atención generada por el robo de identidad. Este documento es una versión actualizada del documento publicado en el año 2005.

Avisos Legales

Copyright © 2009 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 para hacer arreglos.

La Versión Más Actual: La versión más actual de este documento está disponible en http://www.demartek.com/Demartek_Identity_Theft_Prevention_Tips_and_Commentary_ES.html

Lineamientos para la Reproducción de este Documento: Usted puede hacer copias de este documento en su totalidad para ser distribuído 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 HICIERON ESFUERZOS PARA VERIFICAR LA EXHAUSTIVIDAD Y VERACIDAD DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO, 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

El *Robo de Identidad*, también conocido como *Fraude de Identidad*, se encuentra actualmente entre los delitos de más rápido crecimiento. Entre sus víctimas se encuentra todo tipo de gente de todas las edades, niveles económicos, razas, género, etc. En muchos casos las víctimas y sus victimarios nunca se han conocido entre sí. En algunos casos pueden pasar semanas o meses antes de que las víctimas se den cuenta de que un crimen 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 empresasy 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 lo hace 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 aún 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. Algunos ladrones de identidad utilizan computadoras para obtener información a través de inteligentes ataques técnicos o recurriendo a las brechas en el sistema de seguridad de las empresas.

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.

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 robo de identidad, los individuos pueden y deben tomar medidas para prevenir el robo de identidad. Asimismo las personas llevan el peso de la carga cuando se trata del esfuerzo y el trauma de la recuperación de un robo de identidad. El grave efecto del robo de identidad es frecuentemente subestimado, ya que la recuperación de un robo de identidad a menudo lleva años de trabajo. Las víctimas son sometidas a situaciones

vergonzosas, donde se les exige explicar las circunstancias del crímen en contra de ellos, y en algunos casos hasta han sido erróneamente arrestados y encarcelados.

La seguridad, incluída la seguridad física y 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 robo de identidad, ya que siempre habrá nuevas amenazas que emergerán, pero sí puede tomar medidas específicas para reducir su vulnerabilidad a estas amenazas. 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 gubernamentales y las empresas encontrarán aquí información muy útil, es principalmente para el beneficio de las personas que hemos elaborado este documento.

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 urgar 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 destruídos 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 los que se triture papel dentro de su área. 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.

Correo Saliente

Lleve todo su correo saliente y sus paquetes a la oficina postal, oficina de paquetería, etc. 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.

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 realistamente 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 aquí le recomendamos; 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 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 Excluírse de la pre-selección" lo cual impide que las compañías de información de crédito al consumidor usen su archivo de 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. En lugar de aplicar para su tarjeta de crédito, llame al número de teléfono y solicite ser registrado en su lista de "NO ENVIAR CORREO" de tarjetas de crédito. Ellos deben respetar esta solicitud y el representante de servicio al cliente generalmente seguirá el "script" que ellos usan para este proceso. Usted tendrá que repetir este proceso para cada oferta de tarjeta de crédito que usted reciba, pero 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 descontinuarlos.
- **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 supermercados, 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 el de su decisión.

Cheques bancarios

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 incluídos. 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 planee escribir un cheque para un propósito específico.

NO imprima en sus cheques su Número de Seguro Social, su número de Licencia de Manejo 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.

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 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.

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.

Muchas personas están 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. 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. 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.

Es una buena idea sacar copias fotostáticas de sus tarjetas y guardar esas copias en un lugar seguro. 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.

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 empieza 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. Es ilegal utilizar números de Seguro Social falsos, alterados o robados para obtener un empleo, un préstamo, 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.

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 incluída en esta declaración a la cantidad de dinero que usted reporta en sus 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 crédito utilizando el Número de Seguro Social de usted.

El gobierno de Canadá ofrece un servicio en línea llamado "My Service Canada Account" (Mi Cuenta Service Canadá), la 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 necesitarán 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:

- ¿Esto es requerido por la 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.

Rehúsese 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 seguros," 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 ha estado recibiendo multas de tránsito bajo el nombre de usted.

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. La Asociación Nacional de Oficiales de Servicio a Veteranos del Condado ha compilado una lista de la Política de Confidencialidad de cada estado en: http://nacvso.org/wp-content/uploads/2008/12/statelist.pdf.

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.

Números no enlistados y números no publicados

Existen 3 categorías básicas de números de teléfono. Éstas 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 incluídos en los directorios telefónicos impresos y están disponibles a través del Servicio de Asistencia Telefónica. Su nombre y número de teléfono también están incluídos 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 incluídos 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 incluídos en los directorios telefónicos impresos ni tampoco están disponibles a través del Servicio de Asistencia Telefónica. Su nombre y número telefónico no están incluídos 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 telemercadeo, 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 beneficiencia y encuestadores telefónicos aun 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 Telemercaderes 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 beneficiencia, organizaciones que realizan encuestas o sondeos, de partidos políticos, o de periódicos en busca de suscripciones.
- **Asociación Estadounidense de Mercadeo Directo-Servicio Telefónico Preferencial** – A partir del 1o. de Noviembre del 2006, la Asociación de Mercadeo Directo ha suspendido el registro de consumidores a través de correo y correo en internet para sus Encuestas sobre Preferencias Telefónicas (TPS). Ellos sugieren registrarse con las listas nacionales y estatales de "NO LLAME."

- **Asociación de Mercadeo Canadiense (CMA) Servicio de NO CONTACTE** – La Asociación de Mercadeo Canadiense ya no opera una lista de "NO LLAME" y dirige a los consumidores a inscribirse en el registro nacional.

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 frecuentemente 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 escriba al URL de alguna empresa de confianza.

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 debe ser considerado obligatorio. Los firewalls inspeccionan el tráfico de red entrante y saliente y desechan el tráfico entrante que no está entrando en respuesta directa a solicitudes salientes. 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.

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 Windows Vista y aún más en Windows 7. 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 proporciona 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.

Los firewalls de hardware también hacen posible bloquear el acceso a sitios específicos o sitios con determinadas vinculos de texto en el nombre, para todo el tráfico procedente de dentro de su red.

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 ordenados en un CD-ROM. Las buenas prácticas de seguridad requieren diligencia, y mantenerse al día con las actualizaciones de seguridad 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 pieza 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 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 evitan hasta que los hackers u organizaciones más sofisticadas puedan recuperar información que pudiera ser posible encontrar aun después de que se hubieren realizado métodos "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 hacer 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.

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 harán 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 estos 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.

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.

1. **Contraseña en blanco** – No tener contraseña es totalmente inseguro y simplemente invita al robo.

2. **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*, y otras.

3. **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.

4. **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.

5. **Contraseñas Repetidas** – Esto es utilizar la misma contraseña para todo. Si un ladrón logra 'hackear' 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 de 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.

Con esta premisa básica en mente, considere cuidadosamente la información personal que usted publica en cualquier sitio web de redes sociales. Revise cuidadosamente las políticas de confidencialidad de estos sitios y personalice la configuración de privacía de su cuenta para que su información personal permanezca tan privada 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.

- **Fraudes Nigerianos 419/Lotería Extranjera** – Un fraude de correo común 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 protejerse es eliminar este tipo de correos electrónicos 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.
- **Fraudes a Abuelos** – Un estafador llama a una persona de la tercera edad, frecuentemente 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 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, dígale 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 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 su 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.
- **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_cen

sus_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 la Citación 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 una Citación 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 realiza a través del correo. Para mayor información acerca de las Citaciones para Servir como Jurado, contáctese con las oficinas de los tribunales locales.
- **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. Lo que sucede después es que un compañero de trabajo o familiar puede toparse con este tipo de imágenes. Si esto llega a oídos 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.

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.

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. Varias de estas fuentes 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

Estas organizaciones 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 de robo de identidad. Los problemas enfrentados por ellas 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 equivocados, cateos a casas y muchos otros. Consulte su fuente de noticias preferida, y seguramente encontrará muchas historias de fraude de identidad. Es siempre una buena idea mantenerse al día en cuanto a las últimas estafas.

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 algo arrogante de 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. Un buen número de organizaciones han encabezado los titulares de las 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.htm
- **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. Para un mapa interactivo de las leyes estatales sobre congelamiento de seguridad, visite: http://www.lawserver.com/maps/security-freeze-rights.

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
P.O. Box 740241
Atlanta, GA 30374
1-866-685-1111
http://www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
http://www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19022
1-800-888-4213
http://www.transunion.com

Equifax Canada
Servicio al Cliente
Box 190 Jean Talon Station
Montreal, QC H1S 2Z2
1-800-465-7166
http://www.equifax.ca

TransUnion Canada
(Para residentes de todas las provincias excepto Quebec)
Servicio al Cliente
Box 338, LCD 1
Hamilton, ON L8L 7W2
1-800-663-9980
http://www.transunion.ca

TransUnion Canada (Echo Group)
(Para residentes de Quebec)
Servicio al Cliente
1 Place Laval, Suite 370
Laval, PQ, H7N 1A1
1-877-713-3393
http://www.transunion.ca

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.

Pasaporte 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 es una 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 informe de la policía y otra información específica acerca de la víctima y del delito. Esta declaración jurada se presenta a la Dirección General del Estado o al Buró Estatal de Investigaciones. 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, los 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.

Los enlaces para los programas de Pasaporte de Robo de Identidad se enumeran a continuación

Año de Promulgación	Estado	Enlaces para información del programa de Pasaporte de Robo de Identidad
2003	Virginia	http://www.vaag.com/FAQs/FAQ_IDTheft.html
2004	Ohio	http://www.ohioattorneygeneral.gov/About/FAQ/Identity-Theft-Passport-FAQs#FAQ88
2004	Oklahoma	http://www.ok.gov/osbi/Criminal_History/Identity_Theft_Passport_Program
2004	Mississippi	Pasaporte ofrecido a víctimas con registros criminales falsos Contacte a la Dirección General del Estado
2005	Arkansas	http://ag.arkansas.gov/consumers_consumer_alerts_id_theft_passport.html
2005	Montana	http://www.doj.mt.gov/consumer/consumer/identitytheft.asp
2005	Nevada	http://ag.state.nv.us/idtheft/passport/passport.htm
2006	Maryland	http://www.oag.state.md.us/idtheft/IDTpassport.htm
2006	Delaware	http://regulations.delaware.gov/AdminCode/title6/100/101.shtml
2006	Iowa	La víctima debe solicitarlo en las oficinas de seguridad pública del estado

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 de 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 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 seguro contra robo de identidad como un aval para la póliza de seguro de un propietario o un rentador de casa, o como pólizas autónomas. Algunos bancos están ofreciéndolos con cuentas de cheques. Algunas empresas lo ofrecen como una prestación.

Estas pólizas suelen costar menos de $100 dlls. 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 robo de identidad y qué hacer al respecto. Muchas están en esta lista de los Estados Unidos y Canadá.

Canadá – Nacional

- http://www.safecanada.ca/identitytheft_e.asp
- [FR] http://www.securitecanada.ca/menu_f.asp
- 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.ftc.gov/bcp/edu/microsites/idtheft/en-espanol/index.html
- http://www.justice.gov/criminal/fraud/websites/idtheft.html
- [ES] http://www.justice.gov/criminal/fraud/telemercadeo
- http://www.ojp.gov/programs/identitytheft.htm
- http://www.secretservice.gov/criminal.shtml
- http://www.ncjrs.org/spotlight/identity_theft/programs.html
- http://www.pueblo.gsa.gov/cic_text/money/preventidtheft/preventing.htm
- http://www.pueblo.gsa.gov/cic_text/money/idtheft_crooks/idtheft_crooks.htm
- http://ftc.gov/bcp/edu/microsites/idtheft/reference-desk/state-crim-passport.html

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.acjnet.org/abnews/default.aspx?id=13355

Columbia Británica

- http://www.cio.gov.bc.ca/services/security/Awareness/identity_theft/default.asp
- http://www.nwpolice.org/CPU/edu_identity.php
- http://www.richmond.ca/safety/police/prevention/personal/idtheft.htm

La Isla Prince Edward

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

Manitoba

- http://www.gov.mb.ca/id_theft/index.html
- http://www.gov.mb.ca/finance/cca/consumb/identity.html
- http://www.consumermanitoba.ca/scam/ID_theft.html

Nueva Escocia

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

Nuevo Brunswick

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

Ontario

- http://www.sse.gov.on.ca/mcs/en/Pages/Identity_Theft.aspx
- http://www.gov.on.ca/MGS/en/ConsProt/STEL02_045996.html
- http://www.opp.ca/Organization/InvestigationsOrganizedCrime/opp_000533.html

Quebec

- [FR] http://www.vol-identite.info.gouv.qc.ca/fr/index.asp
- [FR] http://www.cacq.ca/info-consommation/capsules-informations/volidentite.html

Saskatchewan

- http://www.justice.gov.sk.ca/Default.aspx?DN=10db2c4f-a6c5-4de5-b84d-14af0ceccdc6
- http://www.justice.gov.sk.ca/identity-theft
- http://www.justice.gov.sk.ca/TipIdentityTheft-Jan2008.pdf

Terranova y Labrador

- http://www.gs.gov.nl.ca/cca/tp/consumer-affairs/ident-en.stm
- https://www.nlcu.com/Home/ProductsAndServices/YourMoney/FraudAwareness

Territorios del Noroeste

- http://www.dot.gov.nt.ca/_live/pages/wpPages/newDLandGIC.aspx
- 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 buena lista 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. Algunas son a través del Estado o de Departamentos de Policía locales.

Algunas de estas direcciones URL son bastante largas, pero al día de esta publicación, estaban en funcionamiento.

Alabama

- http://www.familyprotection.alabama.gov/identity.cfm

Alaska

- http://www.law.state.ak.us/consumer
- [ES] http://www.law.state.ak.us/department/civil/consumer/cp_spanish_brochures.html

Arizona

- http://www.azvictims.org
- http://www.azag.gov/cybercrime/ID_Theft.html
- [ES] http://www.azag.gov/index-esp.html

Arkansas

- http://ag.arkansas.gov/consumers_consumer_alerts_id_theft.html
- http://ag.arkansas.gov/consumers_consumer_alerts_id_theft_how_protect.html

California

- http://www.ag.ca.gov/idtheft
- http://www.privacy.ca.gov
- http://www.ftb.ca.gov/individuals/id_theft.shtml
- [ES] http://www.ftb.ca.gov/individuals/id_theft_spanish.shtml
- http://www.idtheftsummit.ca.gov

Carolina del Norte

- http://www.ncdoj.com/Protect-Yourself/2-4-3-Protect-Your-Identity.aspx
- http://www.ncdot.org/dmv/other_services/licensetheft/identityTheft.html

Carolina del Sur

- http://www.scfederal.org/home/gs/fra
- http://www.scdmvonline.com/DMVNew/default.aspx?n=reporting_fraud
- http://www.charlestoncity.info/dept/content.aspx?nid=793

Colorado

- http://www.ago.state.co.us/idtheft/IDTheft.cfm.html
- http://cbi.state.co.us/idtheft/contents_victims.cfm

Connecticut

- http://www.ct.gov/dcp/cwp/view.asp?a=1629&Q=289476&PM=1

Dakota del Norte

- http://www.ag.state.nd.us/cpat/idtheft/idtheft.htm
- http://www.ag.state.nd.us/cpat/consumerinfo.htm
- http://www.nd.gov/ndins/consumer/miscellaneous-consumer-information/identity-theft

Dakota del Sur

- http://www.state.sd.us/attorney/office/divisions/consumer/idtheft/Default.asp
- http://www.state.sd.us/attorney/office/publications/pdf/Privacy.pdf

Delaware

- http://attorneygeneral.delaware.gov/consumers/protection/idtheft.shtml

Florida

- http://myfloridalegal.com/pages.nsf/Main/CBBEBA3F2583433385256DBA004BC600
- [ES]http://www.myfloridalegal.com/pages.nsf/0/CBBEBA3F2583433385256DBA004BC600?Open&LN=SP
- http://www.fdle.state.fl.us/Fc3/NewFC3Site/idtheft.html

Georgia

- http://consumer.georgia.gov/00/article/0,2086,5426814_39039081_39480072,00.html
- http://law.ga.gov/00/article/0,2086,87670814_87670971_88025112,00.html
- http://gbi.georgia.gov/00/channel_modifieddate/0,2096,67862954_113980209,00.html

Hawaii

- http://hawaii.gov/ag/theft/id_files/id_files/faqs
- http://www.hawaii.gov/dcca/helping_hand/identity_theft
- http://www.honolulupd.org/community/idtheft.htm

Idaho

- http://www2.state.id.us/ag/consumer/privacy.htm
- [ES] http://www2.state.id.us/ag/consumer/spanish/index.htm
- http://www2.state.id.us/ag/consumer/identitytheft.htm
- http://www2.state.id.us/ag/consumer/manuals/IdentityTheft.pdf
- [ES] http://www2.state.id.us/ag/consumer/spanish/identitytheft-spanish.pdf

Illinois

- http://www.ag.state.il.us/consumers/consumer_publications.html
- [ES] http://www.ag.state.il.us/consumers/consumer_publications_span.html
- http://www.illinois.tomorrowsmoney.org/youngpeople/section.cfm/400/identity_theft
- [ES] http://illinois.ahorrando.org/section.cfm/509/1858
- http://illinoisissues.uis.edu/features/2002mar/name.html

Indiana

- http://www.in.gov/idoi/2429.htm
- http://www.in.gov/legislative/house_democrats/lawson_news_20090428.html
- 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
- http://www.iowadot.gov/mvd/omve/theft.htm
- http://www.iowastatebanks.com/financialEducation.aspx?show=idTheft

Islas Vírgenes

- http://www.vipd.gov.vi/crime/id-theft-index.aspx
- http://scotiabank.com/vi/cda/content/0,1679,CCDvi_CID4100_LIDen_SID56_YID13,00.html

Kansas

- http://www.ksag.org/page/internet-fraud
- http://www.ksinsurance.org/consumers/id_theft.htm
- http://www.lawrencepolice.org/index.php?page=identitythefttips

Kentucky

- http://ag.ky.gov/civil/consumerprotection/idtheft
- http://ag.ky.gov/civil/consumerprotection/idtheft/tips.htm

Luisiana

- http://ag.state.la.us/Article.aspx?articleID=354&catID=0

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
- http://www.marylandpirg.org/issues/stop-identity-theft

Massachusetts

- http://www.mass.gov/?pageID=cagosubtopic&L=4&L0=Home&L1=Consumer+Protection&L2=Scams+and+Identity+Theft&L3=Identity+Theft&sid=Cago
- http://www.mass.gov/?pageID=ocaterminal&L=3&L0=Home&L1=Consumer&L2=Identity+Theft&sid=Eoca&b=terminalcontent&f=surviving_theft_of_financial_identity&csid=Eoca
- http://www.masschiefs.org/page.php?pageid=65
- http://www.mass.gov/da/suffolk/help_id.html

Michigan

- http://www.michigan.gov/ag/0,1607,7-164-34739_20942-80479--,00.html
- http://www.michigan.gov/msp/0,1607,7-123-1589_35832---,00.html
- http://www.michigan.gov/documents/ID_Theft_94764_7.pdf

Minnesota

- http://www.ag.state.mn.us/consumer/privacy/guardingyprivacy/default.asp
- http://www.hsem.state.mn.us/HSem_view_Article.asp?docid=66&catid

Mississippi

- http://www.ago.state.ms.us/index.php/pages/identity_theft

Missouri

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

Montana

- http://www.doj.mt.gov/consumer/consumer/identitytheft.asp

Nebraska

- http://www.ago.ne.gov/consumer/idtheft.htm
- http://www.nebankers.org/public/consumer/consumeralerts/idfraud.html
- http://www.opd.ci.omaha.ne.us/how-to-/protect-against-identity-theft

Nevada

- http://ag.state.nv.us/idtheft/idtheft.htm
- http://www.lvmpd.com/bureaus/financial_property_identity.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/bureaus/consumer_frauds/identity_theft.html
- [ES] http://www.ag.ny.gov/spanish/bureaus/consumer_frauds/identity_theft.html
- 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.html
- http://www.state.nh.us/liquor/fictitious_identification.shtml

Nuevo Mexico

- http://www.nmag.gov/office/Divisions/Com/internetsafety/identity.aspx
- http://www.nmaging.state.nm.us/idtheft.html
- http://www.cabq.gov/police/prevention/identity.html

Ohio

- http://www.ohioattorneygeneral.gov/IdentityTheft
- http://www.ohioconsumers.com/resources.htm
- http://www.ohioconsumers.org/slides/IDtheft2005.pdf
- http://www.pickocc.org/annualreports/2007/hotline.shtml
- [ES] http://www.pickocc.org/spanish/index.shtml

Oklahoma

- http://www.oag.ok.gov/oagweb.nsf/Consumer!OpenPage
- http://www.odl.state.ok.us/usinfo/pubs/idtheft.pdf
- http://www.oklahomamoneymatters.org/Financial/scams-and-schemes.shtml

Oregon

- http://www.doj.state.or.us/finfraud/idtheft.shtml
- http://www.oregon.gov/ODOT/DMV/driverid/idtheft.shtml
- http://www.leg.state.or.us/comm/commsrvs/background_briefs2004/Public%20Safety/IF_Identity_Theft2004.pdf

Pensilvania

- http://www.attorneygeneral.gov/idtheft.aspx?id=1757
- http://www.attorneygeneral.gov/consumers.aspx?id=289
- http://www.identitytheftactionplan.com
- [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.riag.ri.gov/civilcriminal/consumerfaq.php
- http://www.riag.ri.gov/civilcriminal/consumerfraud.php
- http://www.risp.ri.gov/docs/Guide_Identity_Theft_RISP.pdf

Tennessee

- http://tennessee.gov/attorneygeneral/cpro/identitytheft.html
- http://tennessee.gov/safety/cididtheft.htm
- http://tennessee.gov/consumer/documents/IdentityTheftBrochurenew.pdf
- http://tennessee.gov/commerce/documents/pr_DeathCertificateScam_04112008.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.txdps.state.tx.us/administration/driver_licensing_control/idtheft/idtheft2.htm
- http://www.oag.state.tx.us/AG_Publications/pdfs/idtheft_pf.pdf
- http://www.oag.state.tx.us/newspubs/opeds/200302blues.shtml

Utah

- http://www.idtheft.utah.gov
- http://publicsafety.utah.gov/investigations/IDTheftlink.htm
- http://hsdaas.utah.gov/protect_your_id.htm
- [ES] http://www.provo.lib.ut.us/resources_finanzas_y_fraude.html

Vermont

- http://www.dps.state.vt.us/vtsp/id_theft.htm

Virginia

- http://www.vaag.com/FAQs/FAQ_IDTheft.html
- http://www.vaag.com/FAQs/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
- [ES] http://www.atg.wa.gov/teenconsumer/espanol/es_your_social_security_number.htm
- http://www.dol.wa.gov/driverslicense/identitycrimes.html

Washington, D.C.

- http://dmv.dc.gov/info/identitytheft.shtm
- http://grc.dc.gov/grc/cwp/view,a,1253,q,461835.asp
- http://newsroom.dc.gov/file.aspx/release/14497/Preventing%20Identity%20Theft.pdf

West Virginia

- http://www.wvago.gov/takeaction.cfm?fx=Idtheft
- http://www.wvs.state.wv.us/wvag/PDFReader/IDTheft.pdf

Wisconsin

- http://www.doj.state.wi.us/dls/ConsProt/cp_identitytheft.asp
- http://privacy.wi.gov/
- [ES] http://privacy.wi.gov/spanish/factsheets/FilingComplaintSPANISH.jsp
- http://www.doj.state.wi.us/docs/ID_theft_broc.pdf
- [ES] http://www.doj.state.wi.us/docs/ID_theft_broc-sp.pdf

Wyoming

- http://ces.uwyo.edu/FRM/Consumer/ConsumerProtectionAddresses.htm
- http://attorneygeneral.state.wy.us/consumer.htm
- http://www.uwyo.edu/CES/FRM/Consumer/ConsumerIssues/PrivacySurvivalGuide.PDF