TRANSCRIPCIOΝ

"Robo de Identidad: Ser Más Listo Que los Ladrones."

Narrador: Bienvenido a Robo de identidad: ser más listo que los ladrones.

Este video ha sido elaborado por el Departamento del Tesoro de los Estados Unidos.

Con ustedes, John Snow, Secretario del Tesoro.

Secretario John W. Snow Intro: Hola, soy John Snow y es un placer para mí estar hoy aquí para hablar de un serio problema que está afectando a los Estados Unidos, el problema del robo de identidad.

El robo de identidad hace daño a los individuos y a sus familias; amenaza con minar la confianza en nuestro muy eficiente sistema de crédito; y como resultado implica costos altos e innecesarios para nuestra economía.

El robo de identidad consiste en hurtar su información personal, como sus números de cuentas financieras, por ejemplo, e usar esa información para acumular facturas u obtener bienes fraudulentamente con su nombre.

Afortunadamente hay cosas que usted puede hacer, cosas que todos podemos hacer para protegernos.

Este video ayuda a definir el problema y fija los pasos que usted puede seguir para protegerse o reparar el daño si es que se convierte en víctima del robo de identidad.

También se hace una idea de cómo están actuando las autoridades por su bien.

Le ruego que aprenda las lecciones de este video y las aplique a su propia vida. Muchas gracias por su atención.

Una Historia de una Víctima: Me sorprendió ser víctima de robo de identidad. Acababa de graduarme de la universidad y estaba apenas comenzando. Conseguí un trabajo, gestionaba mi dinero y pagaba las facturas a tiempo. Tenía una tarjeta de crédito, pero no abusaba de ella.

Debía haber sospechado algo cuando recibí una carta de una compañía de tarjetas de crédito que me habían denegado una nueva tarjeta, pero pensé que había sido un error informático. Unas semanas después, recibí una carta de bienvenida de *otra* tarjeta de crédito agradeciéndome que hubiera abierto una cuenta nueva, pero sin tarjeta. Debía haber sabido entonces que algo estaba mal.

Llamé a la compañía de tarjeta de crédito y me dijeron que la nueva tarjeta había sido emitida con un cotitular, mi vecino. No sólo eso, sino que alguien ya se había gastado más de $300 comprando en otro estado. Me dijeron que hiciera una denuncia en la policía porque necesitarían hacer más verificaciones antes de cerrar la cuenta y quitar el cargo.

Mi vecino estaba tan sorprendido como yo y dijo que hablaría con la policía. Llamé a la policía local, tomaron mi información pero me dijeron que la situación era difícil porque el crimen había cruzado la frontera del estado. No sabía qué hacer, así que decidí llamar a las autoridades federales.

La investigación mostró que los ladrones se presentaban en mi edificio de apartamentos como a las tres de la tarde, antes de que la mayoría de la gente llegara del trabajo, y robaban la correspondencia: facturas, solicitudes de tarjetas de crédito y estados bancarios. Mi edificio tiene unas 30 unidades más. Los buzones están fuera y debajo de un arco y están organizados en suites. Por lo que si abres una de esas suites tienes acceso por lo menos a seis o siente buzones. Después de la investigación cambiamos los buzones a un lugar más seguro.

Narrador: Esto es más que una historia de precaución: le sucede a demasiada gente. De alguna manera alguien consigue robar nuestra identidad –quiénes somos– y abre cuentas bancarias y tarjetas de crédito, y obtiene préstamos en nuestro nombre. ¡Y la cuenta empieza a subir!

Este crimen es un tremendo derroche de dinero y una enorme pérdida de tiempo: el año pasado las víctimas emplearon cerca de 300 millones de horas -175 cada una- intentando separar las cuentas falsas y restaurar su crédito.

El Tesoro de los Estados Unidos le pidió a dos paneles de expertos que nos ayudaran a estar más conscientes del problema del robo de identidad y a protegernos del crimen, y que nos ofrecieran algunas claves para resolver el problema si nos convertimos en víctimas. Puede ver el DVD todo seguido o puede usar el menú para ver cualquier segmento del DVD en cualquier orden. Y lo más importante, hemos incluido una Biblioteca de Recursos: una colección de formularios, páginas web, y todo tipo de materiales de referencia. Ponga el disco en su computadora y descargue lo que necesite. También hay una lista de sitios web en los que puede encontrar más información en línea.

Moderador: Bien, pues empecemos. Nuestro primer panel incluye a Scott Parsons, Subsecretario Asistente para la Protección de Infraestructura Crítica, del Departamento del Tesoro; Agente especial en Jefe Larry Jonson, de la División de Investigación Criminal del Servicio Secreto de los Estados Unidos, Anthony Demangone, Consejero de Cumplimiento de Regulaciones, Asociación Nacional de Sindicatos de Crédito Federales y Alex Sanchez, Presidente Ejecutivo de la Asociación de Banqueros de Florida,

Bien, entremos directamente al tema. Scott, ¿qué es el robo de identidad?

Subsecretario Asistente Parsons: El robo de identidad es un fraude cometido o emprendido usando la información identificadora de otra persona sin su permiso. La ley FACT, la Fair and Accurate Credits Transactions Act, la define de esa manera. Y es importante porque aunque la definición es amplia, realmente hay dos tipos de robo de identidad, de los que estamos hablando hoy aquí. Uno es el secuestro propiamente dicho de la identidad de una persona para abrir cuentas nuevas, obtener nuevas tarjetas de crédito y crear un nueva cuenta bancaria. Ése es uno de los aspectos.

El otro es el fraude de la tarjeta de crédito, obtener su número de tarjeta de crédito o quizá alguna información que le permita a una persona completar una transacción con su número de tarjeta de crédito. Son dos tipos de fraude pero tienen el mismo resultado. Alguien trata de robarle su información e intentar robarle su dinero.

Moderador: Alex, ¿cómo pueden defenderse los consumidores?

Sr. Alex Sanchez: Deben cuidar su identidad como uno de sus bienes más preciados.

Moderador: Ya.

Sr. Sanchez: Como guardan su casa, aseguran su casa. Aseguran su carro. Bien, puede también deben cuidar de su identidad.

Moderador: Anthony, ¿cómo se sabe cuando uno es víctima? ¿De qué hay que estar pendiente?

Anthony Demangone: El indicativo más común es una transacción no autorizada. Un ejemplo de ello, como ha mencionado Scott antes, es el fraude de tarjeta de crédito. Puede que vea una transacción en su estado bancario que no sea suya. No tiene por qué ser una tarjeta de crédito, puede ser una cuenta corriente, una cuenta de ahorros. Al ver el estado encontrará una transacción que parece sospechosa o que no recuerda haber hecho.

El otro problema es que algunas veces, con el robo de identidad, los ladrones abren cuentas nuevas. Utilizan su información para crear una cuenta de la que usted no tiene conocimiento. En la mejor de las situaciones, se podría enterar al cabo de 24 horas. Puede recibir una llamada. Se puede enterar rápidamente de que es una víctima. En la peor de las situaciones, puede tomar semanas o meses. Algunas víctimas no se enteran hasta que reciben una llamada de una agencia de recaudación que les pregunta porqué no están haciendo sus pagos.

Moderador: Tengo entendido que una de las técnicas es que después de robarla, no actúan inmediatamente, por lo que uno cree que está seguro, pero después de un mes o dos-

Sr. Demangone: Exactamente.

Moderador: vuelven- y es cuando te atacan.

Sr. Demangone: Algo parece sospechoso, y bueno, pasa un semana, pasan dos semanas. Uno baja la guardia y como acabas de decir, el problema te está esperando.

Moderador: ¿Alex?

Sr. Sanchez: Bueno, como sabes, iba a decir que el sector banquero, el sector de los servicios financieros, gubernamentales y otros, están invirtiendo billones de dólares en tecnología para combatir el robo de identidad. No obstante, la mejor manera de combatir el robo de identidad es la más sencilla y la más barata: que el consumidor esté informado. Si nosotros, como consumidores, todos nosotros, individualmente, obramos juntos, ése es el modo más barato y más eficiente de luchar contra el robo de identidad, tomando las medidas para proteger nuestras propias identidades.

Moderador: Scott, ¿qué tipo de información personal se roba, y qué hacen los ladrones con ella?

Subsecretario Asistente Parsons: Bien, los ladrones de identidad andan buscando cualquier cosa que puedan usar para crear un perfil para obtener los instrumentos financieros con los que comprar bienes, servicios o propagar otros crímenes. Eso incluye su nombre, número de Seguro Social, dirección. La fecha de nacimiento también es algo importante; todos los datos de que se dan como identificación.

Pero también están buscando otras cosas. Vivimos en la era de algo maravilloso llamado la Internet, en la que la gente tiene acceso a sus cuentas en línea, por lo que también están buscando su nombre de usuario. Están buscando su número PIN. Están buscando cualquier información identificatoria que puedan encontrar para acceder a sus cuentas o para abrir cuentas nuevas.

Moderador: Si, y tenemos un montón de cosas que usamos todos los días. El otro día fui al médico y me pidieron mi número de Seguro Social. Les pregunté "¿Lo necesitan para procesar esto? Me respondieron "Sí así es como organizamos nuestros expedientes". Y dije "¿Y por qué no usar mi *nombre*?, ¿por qué no les vale mi nombre?" "Bueno, *podríamos* hacerlo pero sería mucho más difícil. Lo hacemos por número".Así que qué haces, ¿*no* dárselo?

Subsecretario Asistente Parsons: Eso es algo importante. Ahora se está haciendo un esfuerzo enorme para que el número de Seguro Social no sea la forma principal de identificación de los individuos. En mi estado, en mi estado de residencia, se solía dar el número de Seguro Social.

Moderador: Sí.

Subsecretario Asistente Parsons: Estaba en la propia licencia de manejo.

Moderador: Si, exactamente.

Subsecretario ASISTENTE PARSONS: Pero actualmente, en muchos estados se está usando un número igual de sencillo, un número diferente, para que la gente no pueda tener acceso a tu información.

Moderador: Larry, ¿tienes algo que decir?

Agente especial en Jefe Johnson: Quería mencionar, Paul, respecto a lo que has dicho acerca de la necesidad o no de dar tu número de Seguro Social en la consulta del médico. Creo que es una pregunta importante que todo el mundo debe hacer. "¿Lo necesitan absolutamente para identificar mi archivo?" Si no, no les dé su número de Seguro Social.

Moderador: Anthony, ¿hemos oído hablar de muchas formas distintas de timos? ¿De qué otras cosas debemos estar pendientes?

Sr. Demangone: Creo que es importante que mencionemos que hay que ser consciente de la situación. Estos ladrones están tratando de reunir información de muchas maneras. Mirar a escondidas es una gran manera. Cuando está en un cajero automático, fíjese en si alguien está detrás de usted. Mirando por encima de su hombro, intentado ver su clave de identificación personal – PIN: ésa es otra forma en que consiguen información. Pero, una vez más, a través de la educación del consumidor creo que por lo menos podemos elevar el nivel y hacer que los ladrones lo tengan mucho más difícil para obtener información.

Moderador: Hay un término que se llama "skimming", que honestamente no había oído hasta hace poco. Larry, explícanos qué es eso de skimming y cómo se hace.

Agente especial en Jefe Johnson: Paul, he traído unas cuantas cosas, un scanner, un "skimmer" y un parásito que tiene un skimmer anexionado. Bien -

Moderador: Increíble.

Agente especial en Jefe Johnson: Este scanner se puede conectar fácilmente a este monitor. Este parásito –lo que ha averiguado el Servicio Secreto es que esto se puede conectar o poner encima de un cajero automático, y puede tener el skimmer o el scanner. Y cuando el cliente mete su tarjeta para sacar dinero de un cajero automático, aparece algo en la pantalla como "NO OPERATIVO", "FUERA DE SERVICIO. POR FAVOR, VUELVA MÁS TARDE", pero de hecho, ese cliente le acaba de dar al timador la información de la parte de atrás de su tarjeta de crédito.

Moderador: Esto es lo interesante.

Agente especial en Jefe Johnson: Los skimmers vienen en varios tamaños. Se venden con objetivos legítimos, así como para objetivos fraudulentos. Este skimmer se lo encontraron a un mesero que después de hacer una transacción, también usaba el skimmer y pasaba… la tarjeta del cliente y grababa toda la información de la tarjeta en el skimmer. Este tamaño de skimmer puede retener de 120 a 150 tarjetas de crédito –o la información de las tarjetas de crédito. Y luego se le vende a alguien que sabe qué hacer con ella. Después la descargaran en una computadora portátil o una computadora personal y la venderán en línea o incluso fabricarán la tarjeta de crédito. Hemos visto timos de tarjeta de crédito muy sofisticados que tienen que ver con el robo de identidad.

Moderador: Mi término favorito de todo esto es “recogida de basura”. ¿Qué es la recogida de basura Alex?

Sr. Sanchez: Se define como alguien que busca literalmente entre la basura. Tiramos nuestros estados financieros: los estados que recibimos del banco, la información de nuestra compañía de seguros, otra información sensible. La leemos y la tiramos, y la recogida de basura es cuando la gente más tarde busca en su basura mientras usted está en el trabajo y se lleva esa información. La obtiene, la limpia y la usa.

Sr. Sanchez: ¿Qué podemos hacer para combatir eso?

Moderador: Sí.

Sr. Sanchez: Obviamente, romperla. Cortarla en tiras, cortarla en tiras. Romperla. Primero asegúrese de leerla. Como ha dicho Anthony, creo que cuando recibe su estado debe mirarlo bien para comprobar que no hay ninguna compra no autorizada que se haya cargado a su cuenta. Pero una vez que lo haya leído, si lo va a tirar con la basura, asegúrese de que lo corta en tiras. Eso es muy, muy importante.

Sr. Demangone: Si pudiera añadir algo a lo que ha dicho Alex, ha mencionado lo de leer su estado. La mayoría de los sindicatos de crédito y los bancos le dan acceso a su cuenta en línea, por lo que en vez de tener que esperar hasta el día diez del mes siguiente, puede entrar en la Internet de vez en cuando y ver las transacciones que acaba de hacer. Esto va a reducir el tiempo y los costos relacionados con el robo de identidad. Es algo que deben considerar los consumidores.

Moderador: Y no tendrían 30 días para usar su cuenta si la miran todos lo días.

Sr. Demangone: Reducirá sustancialmente el tiempo.

Moderador: Sí.

Larry, tengo una pregunta para ti. De la basura a la autopista electrónica, lo acabamos de aludir con Anthony, la Internet y algo llamado “phishing”, con “ph”, están siendo motivo de preocupación, ¿verdad?

Agente especial en Jefe Johnson: Sí Paul. Creo que todo el mundo ha visto en su propia computadora lo que es “phishing”, y básicamente es un timo cibernetico. Es como pescar peces de verdad, el hecho de que el timador está buscando que alguien “muerda el anzuelo”. Y si en un sitio phishing lo consiguen dos de cada diez veces, consideran que han tenido éxito.

Los usuarios deben saber que necesitan comprobar el URL o la dirección IP del emisor del e-mail para ver si corresponde con la dirección de su banco, una subasta en línea, o cualquiera de los sitios que está siendo simulado o phished.

Sr. Sanchez: Respecto al phishing, sugiero a nuestros espectadores que cuando reciban un e-mail que tiene el logo de su banco y le pide su cuenta bancaria, lo borren. Simplemente lo borren.

Moderador: Le buscarán -

Sr. Sanchez: Simplemente lo borren.

Moderador: Si es suficientemente importante, le buscarán.

Sr. Sanchez: Bórrenlo porque ningún banco ni institución financiera le enviará un e-mail pidiéndole que confirme sus números de cuenta. Ellos le conocen, tienen sus números de cuenta. No tienen nada que confirmar. Simplemente bórrelo.

Subsecretario Asistente Parsons: El gobierno federal no le enviará un e-mail para decirle que no está -

Moderador: Exacto.

Subsecretario Asistente Parsons: -cumpliendo con el Patriot Act, y necesita darles su número de Seguro Social.

Moderador: Cierto.

Subsecretario Asistente Parsons: Eso no ocurre.

Moderador: De acuerdo.

Sr. Demangone: Hay otra cosa que iba a mencionar. Se parece al phishing y es un problema muy extendido. Los timadores usan una gran variedad de timos que juegan con la codicia; algo como esto.

"Paul, es usted un hombre afortunado. Hoy ha heredado $100,000" o "ha ganado la lotería". Va a recibir $250,000, pero esto es lo que tiene que hacer. Tenemos que pagar impuestos de antemano, y sólo necesitamos $500. Le vamos a dar $100,000". O quizá no sean $500. Tal vez sea su número de Seguro Social porque "Tenemos que llenar unos papeles".

Si le presentan ofertas como ésta, el viejo dicho sigue siendo acertado: "Si parece demasiado bueno para ser verdad, probable lo es". Es sólo una forma más en que los ladrones intentan sacarle su información personal.

Moderador: Clases de timos de loterías. ¿Hay alguna variación?

Sr. Sanchez: ¿Conoce el refrán "Sigue el dinero"?

Moderador: Sí.

Sr. Sanchez: ¿y "Muéstame el dinero"? Uno de nuestros grupos más vulnerables son los ancianos. Normalmente, es el grupo más acomodado de nuestra sociedad porque han tenido muchos años para acumular riqueza. Y eso es lo que a los timadores les gusta seguir, como sabe todo el mundo en este panel.

Sr. Sanchez: Por lo que pedimos a nuestros mayores que sean muy, muy cuidadosos con quién hablan y con quién hacen tratos. Si es demasiado bueno para ser verdad, no se lo crean.

Moderador: Cierto.

Larry, volvemos a ti como oficial de las autoridades. ¿Qué estamos haciendo contra esto?

Agente especial en Jefe Johnson: Hace unos años, teníamos muchos casos menores relacionados con el robo de identidad. Ahora se está encarcelando a la gente por casos mayores. Hace un año, un año y medio, se aprobó la Identity Theft Penalty Enhancement Act, que añade dos años por cualquier componente de robo de identidad relacionado con un crimen.

Automáticamente.

Moderador: ¡Qué bien!

Las autoridades están haciendo muy buen trabajo, estamos escuchando, arrestando a estos criminales y nuestro trabajo se refleja en el éxito de los procesamientos, como explica la Subsecretaria Asistente del Fiscal General Laura Parsky, de la División Criminal del Departamento de Justicia.

Subsecretaria Asistente del Fiscal General Laura Parsky : Hola, me llamo Laura Parsky, del Departamento de Justicia de los Estados Unidos. Me gustaría hablarles de lo que el Departamento de Justicia está haciendo agresivamente para procesar el crimen del robo de identidad. Tenemos 94 oficinas de Fiscales de los Estados Unidos en todo el país, así como fiscales de la división criminal que están trabajando con agentes federales para perseguir a los ladrones de identidad. Nuestro trabajo es poner a estos criminales entre barrotes y sacarlos de la circulación.

Recientemente hemos tenido mucho éxito consiguiendo sentencias largas que están garantizadas por el daño causado por el crimen de robo de identidad. Por ejemplo, en Nueva York, un hombre que preparó el robo y la venta de decenas de miles de informes de crédito recibió una sentencia de 14 años. En Washington, D.C. un hombre que dirigía un plan de robo de identidad y fraude de tarjetas de crédito de $1.1 millones también recibió 14 años de prisión. Un hacker de computadoras de Charlotte, Carolina del Norte, que entró en las computadoras de una gran compañía de venta al público para robar información de tarjetas de crédito, y alguien que dirigía un plan de phishing en Houston, Texas, fue sentenciado a casi cuatro años de cárcel.

Estas graves sentencias son posibles sólo gracias al sólido trabajo de investigación de las agencias de las autoridades locales, estatales y federal, como el FBI, el Servicio Secreto de los Estados Unidos y el Servicio de Inspección Postal de los Estados Unidos.

Pero también necesitamos su ayuda. Si usted es víctima de un robo de identidad, lo mejor que puede hacer por la justicia es presentar una denuncia en la policía. Cuantos más detalles pueda proporcionar a los investigadores, mayores probabilidades hay de que puedan traernos un buen caso para procesarlo. Juntos podemos privar de ganancias al robo de identidad. Gracias.

Moderador: Quiero darle las gracias a Laura Parsky y al Departamento de Justicia por ese video. Muchas gracias. Es alentador saber que cada vez hay más personas como ésas que están recibiendo sentencias largas.

Alex, ¿qué están haciendo las instituciones financieras para protegernos y prevenir este tipo de crimen?

Sr. Sanchez: Bueno, son las tres C's: cumplimiento, consumidores informados y cooperación. Primero, cumplimiento. Cada banco tiene un programa IT –programa de tecnología de la información. Los bancos están invirtiendo millones de dólares para asegurarse de que la información permanece confidencial. Una vez más, como saben, la educación de los consumidores es muy importante. Me gustaría pedirle a todo el mundo que tome todas las precauciones que pueda, como cortar los documentos en tiras, no dejar correspondencia en el buzón, no responder a los e-mails de phishing y borrarlos, y finalmente, está la cooperación. La cooperación con las autoridades es critica.

Como saben, en la Asociación de Banqueros de Florida, se ha creado un sistema junto con las autoridades de Florida, que ahora existe a nivel nacional. Hay veintitrés estados usando este sistema llamado FraudNET, para compartir información entre ellos, los bancos y las autoridades. Por lo que compartir información es esencial para sacar a estas personas de nuestras calles.

Moderador: Eso es muy bueno. Eso está ocurriendo a nivel institucional.

Scott, ¿qué podemos hacer nosotros como individuos para prevenir este crimen, o por lo menos para reducir las oportunidades de los ladrones de identidad?

Subsecretario Asistente Parsons: Bien, los individuos pueden hacer varias cosas básicas que pueden disminuir drásticamente la incidencia del robo de identidad. Una es comprobar su informe de crédito. Los consumidores ahora tienen, gracias al FACT Act, ley que fue firmada por el presidente Bush en 2003, la capacidad de obtener un informe de crédito gratuito cada año de las tres agencias de información acerca del consumidor. Y el informe de crédito es una manera importante de ver si su identidad está siendo usada indebidamente por los ladrones.

Hay un par de cosas más que puede hacer si es un consumidor. No lleve su tarjeta de Seguro Social en su cartera. Hemos hablado de varias maneras en las que pueden actuar los consumidores. Mire su correo. Lea los estados de su tarjeta de crédito.

Sr. Sanchez: Otra cosa más, con permiso, es no llevar encima el número de PIN de su tarjeta de cajero automático o ningún otro PIN. Como detalle curioso, mi PIN es el número de mis dos jugadores de béisbol favoritos, el número que llevaban en su camiseta.

Moderador: UH-huh. Ésa es difícil.

Sr. Sanchez: Sí, ¿y quiénes son? Sólo yo lo sé.

Moderador: Exactamente

Sr. Sanchez: No use su –si vive en el 1010 de Mockingbird Lane, no use el 1010 como su número PIN.

Moderador: Cierto, cierto. Las cosas comunes que se usan normalmente, su cumpleaños o cosas como ésas.

Sr. Sanchez: Correcto.

Moderador: Y es muy probable que si lo usa en una cosa, también lo use en otras 20, para no tener que recordarlo-

Sr. Sanchez: Correcto.

Moderador: -tenga un lista en su nevera.

Agente especial en Jefe Johnson: Y eso nos lleva al tema de cambiar la contraseña. Entiendo que es algo difícil porque no puede recordar cuál era su última contraseña pero actualizar los firewalls y cambiar la contraseña es una buena práctica.

Moderador: Hemos hablado de los informes de crédito, que es importante obtenerlos y que son gratuitos. Una vez al año son gratis en las tres agencias de información acerca del consumidor. Éste es un buen momento para mostrarles cómo obtener esos informes. Nos lo explica Stuart Pratt, Presidente de la Asociación de la Industria de Datos del Consumidor.

Sr. Stuart Pratt: Hola, soy Stuart Pratt, Presidente de la Asociación de la Industria de Datos del Consumidor. Representamos agencias de información acerca del consumidor o “agencias de crédito”, como se llaman con frecuencia. Conservan informes de crédito que le ayudan a obtener tarjetas de crédito, hipotecas, préstamos para carros y otras formas de crédito.

Un paso importante es revisar su informe de crédito. Debe hacerlo antes de una compra grande como una casa o un carro. El Fair Credit Reporting Act le garantiza que puede encargar una copia de su informe en cualquiera de las agencias de información acerca del consumidor y le da los casos en los que tiene derecho a ver su crédito gratuitamente.

El modo más fácil y rápido de obtener su informe gratuitamente es en línea en annualcreditreport.com. Creemos que un consumidor informado funciona mejor en el mercado y para eso es crítico entender su informe de crédito y la información que contiene.

Moderador: Ése es muy buen consejo. Ver su informe de crédito en una forma de darse cuenta de un robo de identidad antes de que el daño sea mayor y de empezar a limpiar su informe.

Subsecretario Asistente Parsons: Si usted es víctima de un robo de identidad tiene acceso a su informe de crédito más de una vez al año.

Moderador: Sí, porque quiere ir viéndolo y saber lo que está ocurriendo.

Subsecretario Asistente Parsons: Por supuesto.

Moderador: Anthony, ¿algún otro consejo sobre cómo alejar a los ladrones de identidad?

Sr. Demangone: Creo que, como ha mencionado Alex, si es cliente de un banco, si es miembro de un sindicato de crédito, ellos están haciendo todo lo posible para proteger su identidad, pero necesitan su ayuda. Si le parece que algo está mal, si le falta un estado –no ha recibido un estado– póngase en contacto con su institución financiera para ver qué pasa. Y por último, simplemente no hay que dejar información por ahí. Hay lugares que puede pensar que son seguros pero quizá no sean tan seguros como usted cree. Su lugar de trabajo y su casa –ha de guardar bien su información financiera, los recibos, los estados. No los deje por ahí. Llévese su recibo del cajero. No deje el recibo en la gasolinera.

Una vez más, no se puede proteger contra las probabilidades del robo de identidad, pero hay muchas cosas que pueden hacer los consumidores.

Moderador: ¿Y cuando usamos la computadora, qué pasa con poner un número PIN para acceder a la propia computadora?

Agente especial en Jefe Johnson: Creo que lo mejor es, si deja la computadora prendida –una vez superada la parte de la contraseña de protección, se marcha, y tanto en el trabajo como en casa, hay gente por ahí, o si es en el trabajo– lo mejor es apagar la computadora. De otra forma, sería muy fácil que cualquiera entrara y mirara sus documentos, o buscara en otros lugares y encontrar información personal. Incluso tengo un reloj, que de darse el caso, puedo descargar alguna información en un thumb drive y llevármela de su cuarto u oficina.

Moderador: ¡Vaya, eso es increíble!

Sr. Sanchez: Y otra cosa. A medida que actualizamos nuestra computadora, y compramos una nueva, se recomienda limpiar el disco duro antes de donarla a una beneficencia o a otro grupo, porque puede haber mucha información almacenada que se ha acumulado a lo largo de los años y que puede ser fácilmente recuperada cuando dona la computadora a un beneficencia.

Moderador: Cierto.

Algunos de los espectadores que nos estén viendo pensarán "Qué buena idea, ¿pero cómo se hace?" Hable con su nieto o hijo de ocho años.

Sr. Sanchez: Si, sí.

Moderador: Ellos saben cómo hacerlo.

Sr. Sanchez: Cierto, cierto.

Moderador: Hable con alguien joven y se lo podrá hacer.

Okay. Hemos mencionado algunas cosas sofisticadas, pero todavía nos falta enfatizar algunas más, Scott, como firmar las nuevas tarjetas de crédito inmediatamente, y cosas como ésas.

Subsecretario Asistente Parsons: Ésa es una de las cosas más importantes que puede hacer. Firmar sus tarjetas. Es un mecanismo de verificación que se puede usar para saber que realmente es usted. Se comparan las firmas.

Otra cosa que ha surgido y que creo que es muy buena idea es que cada vez más los comerciantes están pidiendo su identificación cuando usa su tarjeta de crédito. No es una mala idea si es usted un consumidor.

Un par de cosas más. Anthony mencionó las transacciones de cajero automático. Asegúrese de que no tiene a nadie mirándole por encima del hombro tratando de ver su número PIN. Y por ultimo, los que llaman para pedir algo no necesitan su información personal, ni su número de Seguro Social ni su número de tarjeta de crédito. Si alguien le llama, hoy hemos comentado historias sobre esto con el asunto del phishing, si le llaman pidiendo que les dé información, no tiene por qué hacerlo. Su institución financiera ya conoce su información como cliente. Si se lo piden lo mejor es colgar el teléfono o desconectarse y contactar a su institución usted mismo para enterarse de qué es lo que está ocurriendo realmente.

Moderador: Éstas son las cosas que puede hacer para proteger su información y a sí mismo, pero qué ocurre cuando hay un desastre. Alex, tú eres de Florida.

Sr. Sanchez: Bien -

Moderador: Tú sabes mucho de esto.

Sr. Sanchez: Algo que todo el mundo debe hacer sin importar dónde vive –no importa si se encuentra en una zona en la que se producen desastres o no. Todo el mundo debería revisar su casa y poner en un sobre certificados de nacimiento y otros documentos sensibles como los números de las cuentas financieras y otros rasgos identificadores que pueda tener. Póngalos en ese sobre y métalo en un cajón del que vaya a acordarse después.

Se pasa por tiempos difíciles cuando ocurren estos desastres, ya sea inundaciones, huracanes u otras cosas. Debe estar preparado para llevarse ese sobre en el momento de la evacuación, de forma que pueda tener esos documentos sensibles consigo.

Moderador: ¿Y que pasaría si no lo hace?

Sr. Sanchez: Tendría que reconstruir su identidad, y no es que sea algo difícil de hacer. Lo primero que debe hacer es llamar a su institución financiera y decirles lo que ha ocurrido. Obviamente, necesita hablar con las autoridades estatales, la oficina de licencias de manejo. Llamar a otras agencias gubernamentales, su agencia del Seguro Social. Y en tiempos de desastres, todos estos grupos se preparan para prestar servicio a un nivel más alto porque saben que la demanda de sus servicios será muy alta.

Moderador: Y además puede que le hagan preguntas más detalladas, porque está empezando desde cero. Por lo que-

Sr. Sanchez: Correcto.

Moderador: -no debe ser demasiado cauteloso porque en ese caso sería-

Sr. Sanchez: Cierto.

Moderador: -necesario.

Sr. Sanchez: Ellos saben que es difícil recuperarse de un desastre, que ha perdido su identidad y le ayudarán a recuperarla.

Moderador: Pero al mismo tiempo tiene que tener cuidado de que no le time alguien que le llama en estos momentos de angustia.

Sr. Sanchez: Cierto. En lo que se refiere al gobierno, ellos tienen su número de Seguro Social. En el caso de una institución financiera, ellos conocen sus números de cuenta. Por lo que sea receloso respecto a quién está al otro lado del teléfono. No dé su número de tarjeta de crédito o su número del Seguro Social.

Moderador: Alex, parece que, como has dicho, nuestros números del Seguro Social se usan para establecer nuestra identidad en muchos campos. ¿Por qué es importante resguardar nuestros números del Seguro Social en la lucha contra el robo de identidad?

Sr. Sanchez: Es muy importante. Es la piedra angular de cualquier institución financiera para salvaguardar su información.

Sr. Demangone: Y creo que es importante saber que muchas de las organizaciones o instituciones que le piden su número de Seguro Social lo hacen más como una costumbre que como una necesidad. Si está haciendo una solicitud y no está claro por qué le piden el número de Seguro Social, ya sabe que debe tomar el control. Pregunte "¿Es absolutamente necesario? Prefiero no dárselo". Le sorprenderá saber que en la mayoría de los casos, las instituciones o las entidades no lo necesitan. Y no les importa que lo mantenga en privado.

Moderador: Pero las instituciones financieras *sí* necesitan esa información.

Sr. Sanchez: Cierto, Paul. Obviamente, las instituciones financieras necesitan los números de Seguro Social para hacer las declaraciones que necesitan hacer al gobierno en cuestiones de impuestos y por otras razones de identificación.

Moderador: La precaución consiste en usar la cabeza y no darle esta información a cualquiera. Pero hay circunstancias en la que tendrá que darla.

Sr. Sanchez: Correcto.

Moderador: El IRS usa su número de Seguro Social como identificador del contribuyente. De hecho, hemos acudido al Servicio de Impuestos Internos, una agencia del Departamento del Tesoro, para saber más acerca de nuestro número del Seguro Social y nuestros impuestos.

Sra. Julie Rushin:

Hola, me llamo Julie Rushin y trabajo para el Servicio de Impuestos Internos. ¿Sabía que su número de Seguro Social también puede ser usado por los ladrones de identidad para presentar una declaración de impuestos y obtener reembolsos usando su nombre?

¿Y qué pasa si alguien usa su número del Seguro Social para conseguir un trabajo? El empleador de esa persona reportaría al IRS el salario W-2 ganado usando su información. Por lo que podría parecer que usted no reportó todos sus ingresos en la declaración verdadera.

¿Y qué pasa si hacen una declaración con su número del Seguro Social para recibir un reembolso? Cuando usted presenta su declaración *verdadera*, el IRS pensará que usted ya ha presentado la declaración, recibido el reembolso y que la declaración verdadera es una copia o duplicado.

En lo que se refiere a los archivos de los impuestos, si usted no prepara su propia declaración, debe tener cuidado a la hora de elegir a su contable, tanto como al elegir a un médico o a un abogado. Esa persona tendrá acceso a sus archivos financieros personales. También debe saber que el IRS no se comunica con los contribuyentes por e-mail. Por lo que si recibe alguna solicitud de información en ese formato, es fraudulenta. Conocer estas reglas sencillas puede ayudar a prevenir el robo de identidad.

Si recibe una notificación del IRS que le hace pensar que alguien ha usado su número del Seguro Social fraudulentamente, por favor notifíquelo inmediatamente respondiendo a la persona y número impresos en la notificación. Nuestros inspectores de impuestos trabajarán con usted y otras agencias como la Administración del Seguro Social para resolver estos problemas.

El Servicio del Defensor del Contribuyente también puede ayudar. Si usted ha intentado resolver sus problemas a través de nuestros procesos normales y está a punto de sufrir una penuria considerable, el Servicio del Defensor del Contribuyente tiene expertos que pueden ayudarle. Para más información visite nuestro sitio web en www.irs.gov y seleccione “Taxpayer Advocate” al final de la página. O llame al número gratuito que aparece en la pantalla: 877-777-4778.

En el IRS según nos enteramos de formas de robos de identidad contra los contribuyentes hacemos avisos públicos para estar pendientes de esas estafas. Esos avisos están en nuestro sitio web, junto con información sobre procesamientos criminales contra autores de robos de identidad relacionados con la administración de impuestos.

Moderador: Gracias al IRS por ofrecernos toda esta información acerca de este tema. Hasta ahora hemos hablado de la maneras en las que los ladrones pueden robar nuestra identidad, nuestro crédito, nuestros números y nuestras cuentas bancarias, y hemos oído hablar de algunas de las cosas que podemos hacer para protegernos a nosotros mismos. Quiero darles las gracias a nuestro panel, Scott, Alex, Anthony y Larry.

En nuestra próxima discusión de panel, aprenderemos dónde podemos encontrar ayuda. Y éste es un buen momento para recordarle que tenemos una Biblioteca de Recursos. Inserte este DVD en su computadora para bajar la información que necesite. También hay muchos sitios web donde podrá encontrar más información.

Narrador: Es importante que revise regularmente sus informes de crédito. Para el 1 de septiembre de 2005 todo el mundo podrá obtener anualmente un informe gratuito de las tres agencias nacionales de información acerca del consumidor, o agencias de crédito: Equifax, Experian, y Trans Union. Contacte con su sistema centralizado de respuesta para obtener su informe anual gratuito en annualcreditreport.com.

Segundo, hay algunas condiciones bajo la cuales puede solicitar un informe gratuito de cualquier agencia de crédito. Si está desempleado y está buscando trabajo, si recibe ayuda de beneficencia pública o si cree que la información de su crédito es incorrecta debido a un fraude, puede solicitar un informe de cualquier agencia de información acerca del consumidor contactándolos directamente.

Además, si una compañía deniega su solicitud de crédito o seguro, por ejemplo, debe notificarle de la negativa. La notificación de denegación le dirá cómo puede solicitar un informe de crédito gratuito de la agencia de crédito apropiada.

Finalmente, si sospecha que ha sido o está a punto de ser víctima de un fraude – incluido el robo de identidad- puede poner una alerta de fraude en su expediente de crédito y obtener un informe de cada una de las agencias de crédito nacionales. Sólo necesita llamar a una de ellas para disparar este servicio. Cualquiera de las que contacte le pasará la información a las otros dos. Aquí está la información de contacto de esas agencias de crédito: Equifax [pausa], Experian [pausa], TransUnion.

Por supuesto, también puede pagar un informe en cualquier momento y se puede suscribir a servicios de monitorización de crédito.

Encontrará más información sobre informes de crédito en la Biblioteca de Recursos o en consumer.gov/idtheft.

Una historia de una víctima: El agente federal con el que hablé me ayudó mucho. Hizo la denuncia, que yo a su vez llevé a mi compañía de tarjeta de crédito. El informe fue importante para aclarar el lío. Me di cuenta de que alguien había intentado sacar dinero de mi cuenta corriente y abrir un par de cuentas en línea con mi nombre. Pero no se escaparon. Los bancos y las compañías de crédito están siendo muy eficientes en detectar estas cosas.

Debí haber llamado a la compañía de tarjeta de crédito cuando recibí la primera carta de denegación para averiguar lo que pudiera sobre la solicitud falsa. Afortunadamente me puse en contacto con una de las principales agencias de crédito para poner una alerta de fraude en mi informe. Me alegro mucho de haberlo hecho. La alerta avisa a los posibles acreedores de que puede que sea víctima de un robo de identidad u otro fraude.

De hecho, unas semanas después, una compañía de tarjeta de crédito me llamó para verificar más información luego de que yo hubiera solicitado una tarjeta. Dijeron que probablemente no me hubieran llamado si no hubiera tenido esa alerta en mi informe de crédito. Como atajé el problema relativamente pronto, fue una molestia más que nada. No perdí dinero y mi crédito está bien. No obstante, fue una experiencia innecesaria.

Moderador: En el último segmento repasamos una serie de pasos a tomar para tratar de prevenir el robo de identidad. En esta discusión, aprenderemos sobre los recursos que están a su disposición para proteger su información y tomar acción si cree que corre el riesgo de ser una víctima. Para ayudarnos a contestar algunas preguntas tenemos con nosotros a Nessa Feddis de la Asociación de Banqueros Americanos; Betsy Broder de la Agencia de Protección del Consumidor de la Comisión Federal de Comercio; Michael Desrosiers del Servicio de Inspección Postal de los EE. UU., y Howard Schmidt, exconsejero de seguridad cibernética de la Casa Blanca y actual Agente Especial de la Reserva del Ejército de los EE. UU. para la Unidad de Investigaciones de Crímenes por Computadora.

Howard, me gustaría darle seguimiento al asunto de la seguridad cibernética que se mencionó en el segmento anterior de phishing. ¿Es cierto que hoy en día las personas se están desanimando de realizar transacciones de negocios o bancarias en línea por miedo al robo de identidad?

Sr. Howard Schmidt: Por lo general, no. Creo que hoy en día es más seguro realizar transacciones en línea que nunca antes, aunque todavía tenemos que estar atentos para protegernos mejor.

Moderador: Okay. ¿Y qué puedes decirnos del phishing? ¿Es eso todavía un problema en la Internet?

Sr. Schmidt: Hemos visto que el número de e-mails con phishing ha aumentado, pero el número de víctimas ha disminuido, lo cual es bueno porque la gente está más consciente de los riesgos y de lo que necesita hacer en línea.

Moderador: Aunque sean más sofisticados.

Sr. Schmidt: Absolutamente, lo son.

Moderador: Sí.

El Servicio Secreto de los EE.UU. tiene un informe que da ejemplos de e-mails con phishing.

Agente Especial Stanley Crowder: Hola, soy Stanley Crowder, Agente Especial de la Unidad de Crímenes Electrónicos del Servicio Secreto de los Estados Unidos. Quiero hablarles del "phishing", escrito con "p-h". Es un timo común que le invita a revelar información confidencial personal que puede ser usada para robarle su dinero, y lo que es peor, su identidad.

El phishing normalmente se hace mediante e-mails basura que se envían a miles de personas. Los filtros de correo no solicitado o spam descartan la mayoría de ellos pero algunos le llegan a usted. Digamos que recibe un e-mail que parece que es de su banco.

Le dicen que el banco está haciendo una actualización de las computadoras y que necesita que entre en una página web para verificar e introducir algunos datos.

El e-mail tiene el aspecto de otros e-mails legítimos que puede que haya recibido de su banco. Tiene los logos y gama de color. El enlace del e-mail le lleva a un sitio web igual que el de su banco. Pero de hecho, tanto el e-mail como el sitio web pueden ser falsos. Los ladrones están copiando, o simulando, las imágenes de la verdadera página web del banco para que su e-mail parezca legítimo.

Y los ladrones están haciendo "phishing" para conseguir información como su nombre, dirección y número de teléfono; su número de Seguro Social, fecha de nacimiento, apellido de soltera de su madre, números de cuenta e información de banca en línea, como su contraseña. Incluso intentarán obtener la fecha de expiración y el código de seguridad impreso en el reverso de sus tarjetas.

Cerca del 65% de los ataques de "phishing" imitaban una institución financiera. Otros fingen pertenecer a organizaciones como la Corporación Federal de Seguros de Depósitos, la agencia que asegura sus depósitos bancarios y de ahorros; el Servicio de Impuestos Internos (IRS); compañías de software para computadoras o sitios de comercio electrónico.

El "phishing" se ha hecho tan popular que lo sabio es suponer que va a recibir uno de estos e-mails falsos. Primero, nunca responda a un e-mail de nadie que le pida información personal o de su cuenta. Si usted no ha iniciado la comunicación, no dé esta información, sin importar cómo de legítimo o genuino parezca el e-mail.

Segundo, visite un sitio web sólo introduciendo la dirección web en el navegador web, no oprimiendo un enlace de un e-mail. Cuando contacte con su banco, por ejemplo, use la dirección web que aparece en sus estados mensuales o en los folletos de la institución. Acuérdese de que su banco o compañía de tarjeta de crédito ya debe tener toda la información que necesita. No tienen por qué enviarle un e-mail pidiéndosela.

Mediante el reconocimiento de estas formas de fraude, al instalar y actualizar su software de antivirus y anti-spyware, y hablando del "phishing" por Internet, puede ayudar a prevenir estos crímenes. No sea el anzuelo.

Para más información o para reportar un caso de “phishing”, contacte a las autoridades locales o a la oficina más cercana del Servicio Secreto que aparece en la portada de su guía de teléfonos. También puede visitar el sitio web del Grupo de Acción Anti-Phishing en antiphishing.org o la página de la Comisión Federal de Comercio en ftc.gov.

Moderador: Me gustaría darle las gracias al Servicio Secreto y al Agente Especial Crowder por ese video.

Howard, parece muy elaborado. ¿Qué se ha hecho para detener a los phishers, o como se los llame?

Sr. Howard Schmidt: Bueno, hay cuatro categorías básicas de cosas que se están haciendo. Lo primero, y lo más importante, es la nueva tecnología. Hay diferentes compañías, ya sean de comercio electrónico u operadores de sistemas de computación, incluso compañías pequeñas, que están desarrollando nuevas tecnologías para combatir el phishing.

Lo segundo es la perspectiva institucional, porque las compañías están trabajando juntas, las divisiones de seguridad de las compañías se están comunicando entre sí. Se llaman y se informan, por ejemplo: “Hemos encontrado algo que pueda afectarlos a ustedes”. Comparten información, lo cual es algo natural.

Por otro lado, hay un nivel mayor de educación y esto es algo muy importante, porque podemos fabricar carros muy, muy seguros, pero si se manejan demasiado rápido y no le has puesto líquido de frenos, vas a tener un problema. Educar a la gente acerca de lo que tienen que estar pendientes es el tercer elemento.

El cuarto es claramente el papel que desempeñan las autoridades. Si los primeros tres no tienen un 100 por ciento de éxito, lo cual nunca se espera que suceda, las autoridades tienen nuevas herramientas y nuevos mecanismos para investigar estas cosas y atrapar a los criminales.

Moderador: Howard, te tengo una pregunta. ¿Qué me dices del software?

Sr. Schmidt: En muchos casos, por ejemplo, con los navegadores – los puentes entre el mundo virtual en línea y nosotros – suceden dos cosas. Lo primero, y lo más importante, hay que mantenerlos actualizados. Es de una importancia vital hacerlo, y esto lo mencionamos todo el tiempo. Uno tiene que asegurarse de usar un softwate antivirus. Si uno tiene una conexión de alta velocidad como un módem de cable o un sistema de DSL, uno debe usar un “firewall”personal. Ahora hay distintos tipos de software que incluyen antivirus, spyware, spamware y firewalls personales y todos vienen en un solo paquete que es muy fácil de usar.

También estamos viendo la proliferación de aparatos de entrada. Por ejemplo, cuando usas un módem de cable o de DSL, éstos traen conexiones inalámbricas y software en el aparato de modo que uno tiene que pasar menos trabajo.

Moderador: Ahora bien, no podemos simplemente regresar a las direcciones de URL y hacer clic en ellas porque quizás no sea adónde realmente queremos ir. ¿Cuántas de las instituciones o personas con las que nos comunicamos tienen una “s” al final de su “http”, lo cual indica que es un sitio web seguro?

Sr. Schmidt: Eso es correcto. Básicamente es una codificación o una conexión especial entre tu desktop y el de ellos. Cada vez que estás realizando una transacción que implica el uso de tarjetas de crédito o dinero, busquen por esa “s”al final de “https” y asegúrense de que ustedes mismos han tecleado la dirección de URL, el localizador universal de recursos. No vayan a esos que se reciben por e-mail y que dicen “Haga clic aquí para actualizar su información. Puede que tenga una “s” pero esa “s” no es *legítima*.

Sr. Schmidt: O sea, teclee usted mismo: www.mybank.com

Moderador: O sea que --

Sr. Schmidt: -- No importa cual sea el nombre, para que sepas que estás realmente ahí.

Moderador: Ah. O sea que --

Sr. Schmidt: Y busca la “s” y también busca por el icono de un candado. Por lo regular se encuentra en la esquina inferior derecha de la pantalla, y te indica que es una sesión codificada.

Moderador: Okay.

Nessa, un crimen es un crimen, ya sea en línea o no, ¿correcto?

Sra. Nessa Feddis: Si un consumidor cree que le ha dado información a un phisher, lo que debe hacer depende de la información que le haya dado. Si han dado información de una cuenta, de una tarjeta de crédito, de una tarjeta de débito, deben contactar la institución financiera inmediatamente. Quizás tengan que cerrar la cuenta, obtener una tarjeta nueva, etc. Pero los consumidores deben estar pendientes de las transacciones que no hicieron ellos. Y si ven que hay transacciones que no fueron hechas por ellos deben contactar la institución financiera inmediatamente.

En la mayoría de los casos, se pueden resolver con bastante rapidez, pero cuanto antes se lo digan a la institución, más fácil será y más rápido se resolverá el asunto.

Ahora bien, en el caso de “phishing” – cuando uno no provee información de una cuenta pero sí información personal – como su dirección o número de Seguro Social, o fecha de nacimiento o el apellido de la madre, toda esa información – que se puede usar para abrir una cuenta en tu nombre, se deben tomar otras medidas. Quizás sea buena idea poner una alerta en su informe de crédito de modo que un acreedor que esté revisando una solicitud se asegurará de que la persona que está solicitando un préstamo en su nombre sea, en efecto, usted. Y además, si provee información personal, quizás quiera revisar periódicamente su informe de crédito para asegurarse de que no se han abierto cuentas en su nombre.

Moderador: Okay, y con eso cubrimos el "phishing".

Howard, hay algo nuevo que se llama "spyware". Yo creía que eso era algo *bueno*.

Sr. Schmidt: Bueno, no necesariamente. El spyware puede ser del tipo que, sin tú saberlo, instala software en el sistema de tu computadora y literalmente registra lo que tecleas. Así, por ejemplo, si visitas tu banco y tecleas tu nombre de identificación y tu contraseña, lo registraría y lo transmitiría a otro lugar y otra persona podría hacerse pasar por ti en ese banco.

También existe otro tipo, por el cual registran tus actividades en la Internet con propósitos de mercadeo. Muchas veces no te das cuenta que lo haces. Te crees que estás bajando un juego interesante, o un programa de geografía o algo por el estilo y sin darte cuenta se instala el spyware.

Y una de las cosas en las que uno se debe fijar bien cuando se baja software como ése es el asunto de las licencias. Asegúrate de que básicamente estás recibiendo lo que crees que estás recibiendo y nada más.

Moderador: Entonces, ¿qué podemos hacer al respecto? Me refiero al spyware.

Sr. Schmidt: Bueno, hay varias cosas. Lo primero, y lo más importante, hay software anti-spyware que está disponible, lo cual es fácil. Es parte de los suites de seguridad que están disponibles hoy en día. Usar software para los miembros más jóvenes de la familia, software con controles parentales, que en realidad también bloquea es tipo de actividad. O sea que hay dos mecanismos para hacerlo.

Moderador: Bueno, Michael, pasamos del correo electrónico al buzón de correo. Se supone que también debemos tener cuidado con el correo postal, ¿no es cierto?

Inspector Postal Desrosiers: Así es Paul. El Servicio Postal entrega correspondencia a cerca de 142 millones de direcciones todos los días. La mayoría de estas entregas se hacen a los buzones de correo típicos que se encuentran en rutas rurales, en la entrada de las casas, en las aceras, y la mayoría de estos buzones – los buzones típicos americanos – no son seguros. No tienen protección alguna, y eso los hace potencialmente atractivos para los ladrones.

Y la posibilidad de obtener información por medio del robo de correspondencia es enorme. No pensamos muchos sobre lo que recibimos por correo o en lo que podría sucederle a la correspondencia si cae en manos de ladrones. Cosas como cheques, tarjetas de crédito, estados de cuenta mensuales, licencias de manejo, todas llegan por correo.

En el correo se incluyen su nombre, dirección, número de Seguro Social, número de teléfono, números de cuentas bancarias o de tarjetas de crédito - y todo puede ser usado por un ladrón para realizar un timo de robo de identidad para su beneficio y ganancia personal.

Moderador: Vaya. Con toda esa información realmente somos vulnerables. ¿Y qué podemos hacer para protegernos?

Inspector Postal Desrosiers: Bueno, primero que nada, en cuanto al correo que recibe, es decir, el correo que el Servicio Postal le entrega a su buzón, el Servicio Postal recomienda que la correspondencia debe ser recogida en cuanto sea entregada. Cuanto más tiempo esté en el buzón, mayor es el riesgo de que sea robada o manipulada. Por eso uno debe buscar la correspondencia lo antes posible.

Lo segundo, se recomienda que el buzón tenga algún tipo de mecanismo de seguridad, algún tipo de llave o candado.

Lo tercero, también se recomienda obtener un apartado postal en una oficina de correos. No hay un modo más seguro de recibir la correspondencia porque en cierto modo nunca sale del servicio postal.

Moderador: ¿Y qué se puede hacer para enviarla? ¿De qué modo nos podemos proteger?

Inspector Postal Desrosiers: La correspondencia que se envía, es decir, cuando enviamos algo por el sistema de correo – digamos que le estás enviando algo a un primo – lo pones en tu buzón que está en la acera al frente de tu casa, un buzón que no es seguro y levantas la banderita roja. Todos sabemos para qué es la banderita, para que tu cartero sepa que has puesto algo en el buzón que necesitar ser enviado.

Sin embargo, también se lo informa a los ladrones de correspondencia que están buscando la oportunidad de robar algo. Estarán pasando por tu vecindario, verán tu banderita y es como decirles: "Aquí hay algo. Ven y búscalo".

Por eso exhortamos a que si va a poner correspondencia en su buzón para enviar algo, no levante la banderita. Recomendamos que lleve la correspondencia al Servicio Postal, a los buzones grandes y azules que se ven en cada esquina. O que se lleve a la oficina de correos. Esa es la manera más segura de enviar correspondencia.

Moderador: Es alentador escuchar que hay varios modos en los que podemos evitar el robo de identidad, pero algunos de nosotros seremos víctimas de todos modos.

Betsy, ¿qué debemos hacer cuando creamos que hemos sido víctima del robo de identidad?

Sra. Betsy Broder: Si cree que ha sido víctima de robo de identidad, debe tomar medidas y hacerlo rápido. Lo primero que se debe hacer es contactar a las agencias de crédito. Ellos llevan cuenta de cómo paga sus cuentas y de las cuentas que están abiertas a su nombre. Se comunicas con ellos y le informa de que cree que es o podría ser víctima de robo de identidad y ellos deben poner una alerta de fraude en su expediente. Podemos hablar más --

Moderador: Okay.

Sra. Broder: -- un poco más sobre esto más adelante.

Lo segundo que debe hacer es contactar a las instituciones financieras donde tenga cuentas abiertas o se hayan realizado transacciones a su nombre – una tarjeta de crédito a su nombre o retiros de su cuenta de banco. Póngase en contacto con la compañía. Quizás inicialmente prefiera hacerlo por teléfono, pero déle seguimiento por correo – con una carta certificada, y mantenga un récord de todo lo que hace.

Lo tercero que debe hacer es ponerse en contacto con el departamento de policía local. Es una víctima de un crimen y debe llevar cuenta de lo que sucede. Cuando vaya a la policía, explíquele con lujo de detalles lo que ha ocurrido y pida una copia del informe policial porque eso será esencial más adelante.

Moderador: Yo iba a decir que eso es muy importante.

Sra. Broder: Lo es.

Y finalmente, la cuarta cosa que se debe hacer es ponerse en contacto con la Comisión Federal de Comercio. Contamos con muchos recursos para las víctimas de robo de identidad, los pasos que se deben tomar para recuperar o minimizar el daño que se les hace, y muchas herramientas que pueden usar. También tenemos un formulario en línea para reclamaciones y un número gratuito. Esos son los cuatro pasos.

Moderador: Okay. ¿Y en cuántos de esos casos se necesita documentación?

Sra. Broder: Bueno, cada vez que envíe una carta, debe sacarle una copia. Debe tener una copia de cualquier documento que indique fraude. Por ejemplo, puede haber recibido una factura de una cuenta de su tarjeta de crédito que fue abierta a su nombre de un modo fraudulento. Uno, por supuesto, debe conservarla y llevar cuenta de cada paso que tome, desde contactar a la policía hasta contactar a las instituciones financieras, de modo que cada vez que surja una pregunta pueda rendir cuenta de lo que ha hecho y cuándo.

Moderador: En otras palabras, documentación.

Sra. Broder: Sí.

Moderador: Bueno, las instituciones financieras ciertamente son un factor importante.

¿Y qué podemos esperar de ellas, Nessa?

Sra. Feddis: Como dijo Betsy, uno debe contactar a la institución financiera lo antes posible. Se les debe llamar y luego se les debe enviar una carta. En la mayoría de los casos lo que debe esperar es que cierren su cuenta. Si es una cuenta que ha sido usada indebidamente – quizás una transacción de tarjeta de débito no autorizada, o algún tipo de acceso a una cuenta que la víctima abrió – esto probablemente significa que esa persona tendrá que obtener cheques nuevos, una nueva tarjeta y número PIN, o si es una cuenta de una tarjeta de crédito, una nueva tarjeta y una nueva contraseña, etc.

Algunas personas quizás deban tomar medidas adicionales. Muchas personas han hecho arreglos para hacer pagos – como el pago de la hipoteca o por servicios públicos – que se deducen de un modo automático electrónicamente o por tarjeta de crédito mensualmente. Uno debe ponerse en contacto con esas agencias para asegurarse de que sus pagos continúen y de que no lleguen tarde y luego tengan problemas. Por eso deben ponerse en contacto con esas compañías con la nueva información.

En otros casos cuando el ladrón ha abierto la cuenta a nombre de la víctima o ha usado su cuenta por un tiempo prolongado – quizás incluso han cambiado la dirección – eso es un poco más serio. La cuenta, por supuesto, será cerrada, pero uno prefiere no tener un nuevo número de cuenta. Pero en esos casos, uno sí debe alertar a las agencias de crédito para que cuando un acreedor reciba una solicitud, se asegure de que la persona de que está solicitando crédito es, de hecho, esa persona. Y también es una buena idea en esos casos de averiguar periódicamente cuál es su informe de crédito para asegurarse de que no se hayan abierto cuentas nuevas a su nombre y de que las cuentas fraudulentas ya no aparecen en el informe.

El tiempo apremia. Los estudios de la FTC y otros estudios demuestran que cuando el robo de identidad se identifica en poco tiempo, son menos los inconvenientes. Es menos costoso para todos. Por eso el factor del tiempo es tan importante.

Recomiendo altamente el sitio web de la FTC. Ahí hay mucha información muy buena, y tienen una declaración jurada. También sugieren otras ideas sobre cómo prevenir el robo de identidad y lo que se debe hacer si uno se convierte en una víctima.

Moderador: Creo que tienen muestras de cartas que uno puede enviar a las instituciones como parte de la documentación, para saber cómo --

Sra. Feddis: Nosotros creemos que el mejor modo de resolver estos asuntos es que el consumidor se haga responsable de hacerlo. Como tú dices, Paul, hay muestras de cartas para enviar a los acreedores y a las agencias de crédito para indagar sobre cuentas fraudulentas. Como mencionó Nessa, hay declaraciones juradas que puedes usar para enviarlas a varios acreedores e instituciones financieras. Queremos facilitarle el trabajo a las víctimas para lidiar con una situación que es muy estresante.

Sobre la declaración jurada, yo añadiría que es un buen comienzo y que las instituciones financieras aprecian una declaración jurada uniforme. Pero las víctimas también deberían saber que esa declaración se debe complementar con información adicional sobre los detalles de las transacciones y esos detalles pueden variar de acuerdo a la situación.

Moderador: Betsy, Nessa ha hablado sobre las instituciones financieras. Danos un poco más de información acerca de qué debemos hacer con las agencias de crédito en casos como estos.

Sra. Broder: Si es víctima de robo de identidad hay elementos clave. Por ejemplo, existen tres agencias de crédito principales, y si se da cuenta de que su información ha sido obtenida y usada indebidamente o ya lo ha sido – digamos que le roban la cartera y contenía documentos con su número de Seguro Social o fecha de nacimiento – debe poner una alerta para proteger su expediente de crédito porque alguien podría usar esa información para cometer un robo de identidad. Solíamos creer que si nos robaban la cartera o el bolso lo peor que podía suceder es que se llevaran su dinero. Ahora es un poco más peligroso porque tienen su información que se puede usar de otros modos.

Y si hay tres agencias de crédito principales, debe asegurarse de que las tres pongan en efecto una alerta en su expediente. La buena noticia es que sólo tiene que llamar a una de las agencias.

El sitio web de la FTC a la cual Nessa aludió es www.consumer.gov/idtheft. Y ahí hay una lista de la información de contacto para las tres agencias de crédito. Si llama a una y dices “Mi información ha sido obtenida. Siento que corro el riesgo de fraude. Por favor pongan una alerta de fraude en mi expediente.” Esa agencia se pondrá en contacto con las otras dos y les informará de su petición, o sea que sólo tiene que hacer una llamada.

Después de que la alerta sea puesta en efecto también le darán una copia gratuita de su informe de crédito.

Moderador: Y aunque no se sospeche de fraude, ¿se puede obtener un informe de crédito gratuito anual?

Sra. Broder: Claro que sí. Según la ley federal, uno tiene el derecho de recibir un informe de crédito gratuito independientemente de si sea--

Moderador: Sólo para --

Sra. Broder: -- víctima de fraude.

Moderador: -- comprobar y ver lo que aparece ahí o no.

Sra. Broder: Financieramente es saludable para poder establecer que la información es correcta. A veces se cometen errores. A veces hay más de una Betsy Broder, y desafortunadamente yo podría obtener su información en mi expediente. Quiero asegurarme de que toda la información que aparece en mi expediente es correcta, porque la próxima vez que vaya a refinanciar mi casa o a comprar un carro, quiero estar segura de que mi crédito está en la mejor condición posible.

Inspector Postal Desrosiers: Betsy, si se es víctima de robo de identidad, se puede conseguir todo lo necesario en el sitio web www.ftc.gov?

Sra. Broder: Sí, y si visita nuestra página de la Comisión Federal de Comercio, hay un enlace a la página de robo de identidad. También tenemos un número de teléfono gratuito para víctimas de robo de identidad, es el 877-IDTHEFT.

Moderador: Y debo añadir, para todo el que nos esté escuchando, que todas estas direcciones electrónicas que hemos mencionado son parte de nuestro archivo de recursos que es parte de este DVD. Cuando tengan pueden examinarlo con más detenimiento.

Sra. Broder: Asé es.

Moderador: Howard, hay miles de hombres y mujeres en la Guardia Nacional o cualquiera de los Servicios Armados que no pueden levantar el teléfono para hacer lo que hemos estado hablando aquí. ¿Y qué pasa al respecto?

Sr. Schmidt: Bien, hay una cláusula especial en el FACT Act de 2003 de la que hemos hablado antes, en la que se incluye una “alerta de personal militar en servicio activo”. Por lo que los hombre y mujeres que están sirviendo en el ejército, ya sea activamente, en la Guardia Nacional o los Reservistas- y están desplegados en algún lugar, pueden llamar a la agencia de crédito, sólo hace falta una llamada porque se aplica a todas las agencias de crédito, y decirles que quieren una alerta de personal militar en servicio activo en su expediente de credito. Y eso se traduce en dos cosas. Una, se queda ahí durante un año y se puede renovar si están desplegados más tiempo. Pero también le dice a los comerciantes y a los prestadores básicamente que deben prestar una especial atención a la aplicación porque puede que sea esa persona o no, ya que esa persona está sirviendo en algún lugar.

Moderador: Seguro.

Sr. Schmidt: Una mayor protección muy necesitada para los militares que están desplegados.

Moderador: Betsy, eso nos lleva al tercer punto de los cuatro originales y es que cómo, por qué y qué debemos hacer cuando nos reportamos a las autoridades.

Sra. Broder: Bien, puede reportarse a su comisaría de policía local. De hecho, nosotros aconsejamos a los consumidores que lo hagan. Repórtelo en el lugar donde reside. Se supone que las comisarías de policía deben aceptar la denuncia en su lugar de residencia. Es importante que vaya a la policía y denuncie el crimen por un par de razones. Primero porque es bueno para usted que lo investiguen y le hagan seguimiento, para lo que hace falta que quede registrado.

Usted debe quedarse con una copia del informe policial porque documenta su denuncia y esto, a la vez, tiene dos objetivos. Primero, establece que usted es una víctima bona fide, por lo que si alguien trata de recaudar la deuda adquirida por el ladrón, usted tiene una documentación que dice "Ése no soy yo, se trata de alguien más". Y hay casos todavía más serios en lo que alguien víctima de robo de identidad se entera de que el malo ha usado su nombre para cometer un crimen. Por lo que tiene el informe policial que establece que usted es la víctima de un crimen, no el malo.

Pero la denuncia policial en sí misma tiene mucho valor a la hora de resolver los problemas del robo de identidad. Según la ley, si tiene un informe policial puede tomar pasos importantes para limpiar el daño financiero hecho por el robo de identidad. El primero es que puede quitar de su informe de crédito todas las cuentas fraudulentas. Puede proporcionar una copia del informe policial a las agencias de información acerca del consumidor, y ellos deben bloquear esas cuentas que usted especifique que son producto de un fraude.

También facilita las cosas el tener copias de los documentos que se usaron para abrir las cuentas fraudulentas. Déjame que hable un poco más de eso.

Moderador: Claro.

Sra. Broder: Okay. Soy una víctima de robo de identidad. Alguien va a unos grandes almacenes y abre una cuenta usando mi nombre y mi información, y yo empiezo a recibir las facturas. Quiero disputar esa cuenta, llamo a los grandes almacenes y digo, "Esto es fraudulento. No soy responsable de esta deuda y me gustaría ver una copia de la solicitud". Y ellos contestan "Usted dice que no firmó la solicitud. No es suya, por lo tanto no podemos dársela, pero necesita pagar sus facturas".

El Congreso se dio cuenta de que ése era un problema grave, por lo que si tiene una copia del informe policial y le puede dar a la compañía otra documentación que necesite, ellos le proporcionarán una copia de la solicitud. También puede autorizar a las autoridades para que accedan a esa información sin una citación. Por tanto el informe policial le permitirá bloquear la información fraudulenta de su archivo. Le dará acceso a los documentos que se utilizaron para cometer el fraude y también, si quiere una alerta de fraude de siete años en su archivo porque es, de hecho, una víctima, el informe policial le ayudará con eso.

Moderador: Muy bien, está muy bien.

Michael, ¿debemos llamarlos si pasa algo cuando somos víctimas?

Inspector Postal Desrosiers: Definitivamente deben llamar al Servicio de Inspección Postal de los Estados Unidos. Para aquellos que no lo sepan, el Servicio de Inspección Postal es la agencia de cumplimiento de la ley del Servicio Postal de los EE.UU. Somos las personas responsables de investigar todas las violaciones federales que tienen que ver con las disposiciones federales que implican al Servicio Postal y la correspondencia. Somos las personas que investigamos todos los timos de fraude con correo, los ladrones de correspondencia y cerca de otras 200 disposiciones federales.

Por lo que si es víctima de un robo de identidad, le animo a que se ponga en contacto con nosotros y la mejor manera de hacerlo es a través de nuestro sitio web www.usps.gov/postalinspectors. Cuando entre en el sitio web podrá encontrar la dirección y el teléfono del Inspector Postal más cercano.

Sra. Broder: ¿Puedo añadir algo?

Moderador: Por supuesto.

Sra. Broder: Yo sé que estos casos son procesados porque cada vez que veo a Mike me cuenta de los nuevos casos en los que está trabajando. Y eso es alentador.

Hablamos de "obtener una copia del informe policial" y suena muy sencillo. Pero a veces a los consumidores se les puede hacer difícil conseguir una copia de ese informe policial. Nuestro consejo es "Sea perseverante". Ser perseverante. Vuelva las veces necesarias. Diga en su comisaría local que "La FTC y las instituciones financieras me dicen que necesito una copia del informe policial". Si no puede obtenerlo de la comisaría local, debe buscar otras agencias de cumplimiento de la ley en su jurisdicción, en el nivel federal, quizá la oficina del fiscal general. Una vez más, es esencial-

Inspector Postal Desrosiers: Sí.

Sra. Broder: Que obtengan una copia del informe policial.

Moderador: Creo que las cosas de las que hemos hablado son lógicas. Algunas personas pueden estarse preguntando por qué el elemento de la FTC es tan importante. ¿Betsy?

Sra. Broder: Estamos aquí para el consumidor. Estamos para apoyarlo. Trabajamos muy de cerca con las autoridades. También trabajamos muy de cerca con la industria y la tecnología. Pero entendemos que hay muchas cosas que los consumidores pueden hacer para protegerse a sí mismos, para minimizar el riesgo del robo de identidad y en la recuperación.

He mencionado antes que tenemos un sitio web en www.consumer.gov/idtheft que tiene un formulario de queja en línea. Cuando la gente entra en nuestro sitio web, pasan un par de cosas. Como dijo Nessa, tienen acceso a nuestra declaración jurada. Tienen acceso a un montón de material que les ayudará a tomar los pasos hacia la recuperación. Pero también queremos algo de ellos, esto es, toda la información que han podido reunir acerca de cómo se produjo el crimen, porque la ponemos en nuestra base de datos y la compartimos con más de 1400 agencias de cumplimiento de la ley de todo el país.

Metemos todos estos datos de las quejas en el sistema y luego alguien como Mike Desrosiers del Servicio de Inspección Postal, se encuentra una queja en su escritorio y puede entrar en la base de datos de la FTC y puede meter cualquier rasgo, cualquier dato que tenga e investigarlo, y darse cuenta de que no es un único incidente de robo de identidad que ha sido reportado, quizá hay otras cinco personas que han presentado una queja. Por tanto, de repente, tiene un caso más grande, más sólido, que es más fácil de procesar. Y cuando se procesa, es más probable que la condena para ese sospechoso sea mayor. Funciona en beneficio de todos.

Moderador: Entonces eso es. Uno, llamamos a la institución. Dos, contactamos a las agencias de crédito nacionales para poner una alerta de fraude y obtener un informe de crédito gratuito. Tres, presentamos un denuncia en la policía y conseguimos un informe que ayuda a aclarar las disputas. Cuatro, se lo decimos a la Comisión Federal de Comercio. ¿Algo más?

Sra. Broder: Déjame añadir algo más

Moderador: Okay.

Sra. Broder: que no hemos tocado. Algunas veces la gente se entera del robo de identidad porque le llama un comerciante que dice “Se ha abierto una cuenta pero parece sospechosa”. A veces, uno se entera porque ve su informe de crédito. A veces la gente se entera porque le llama un recaudador de deudas, y sólo entonces se da cuenta de que alguien ha usado su nombre para abrir nuevas cuentas y adquirir un montón de deudas que han sido referidas a un recaudador de deudas.

Según la ley federal, usted tiene derecho a pedir a ese recaudador de deudas información acerca de la naturaleza, de qué se trata, e información sobre el propio recaudador de deudas. Y así es como se enterará de esa cuenta fraudulenta, y podrá tomar los otros pasos para disputar la cuenta. Toda esa información está en la biblioteca de recursos y en el sitio web de la FTC.

Moderador: Hay que conseguir toda la información posible, ¿verdad?

Sra. Broder: Documéntelo todo, documente meticulosamente todo lo que haga.

Moderador: Obtenga los informes policiales y asegúrese –esto es de sentido común pero tenemos que insistir en ellos para entender lo que está ocurriendo.
¿Alguno quiere añadir algún comentario?

Sra. Feddis: Bueno, como acabamos de decir, éste es un esfuerzo colectivo. Y con la atención y la educación de los consumidores, con la imaginación y el compromiso de las instituciones financiera y la energía y cooperación de las autoridades, realmente podemos minimizar el impacto en los consumidores y en las instituciones financieras.

Moderador: Me gustaría dar las gracias a nuestro panel, a Howard, Betsy, Michael y Nessa, por su presencia y por compartir con nosotros en este programa esta información tan valiosa.

En resumen, hay cosas evidentes que puede hacer para proteger su e-mail y su correspondencia para que no se cometa un robo de identidad contra usted. Si piensa que ha sido víctima del robo de identidad debe trabajar con las instituciones financieras para cerrar las cuentas fraudulentas y tomar los pasos para asegurar las cuentas que estén en riesgo. Debe contactar a las tres agencias nacionales de crédito para poner una alerta de fraude en sus expedientes y solicitar una copia de su informe de crédito para saber bien cuál es su situación. Y debe pedir ayuda a las autoridades y a la Comisión Federal del Comercio y denunciar el crimen.

El Departamento del Tesoro de los Estados Unidos espera que esta presentación le haya resultado de ayuda. Esperamos que la información proporcionada en este DVD le haya ayudado a entender lo que es el robo de identidad, cómo puede protegerse a sí mismo y qué debe hacer si es una víctima.

Acuérdese de que la Biblioteca de Recursos, también en este DVD, se puede ver insertándolo en un lector de discos. La Biblioteca de Recursos contiene documentos valiosos y enlaces a sitios web que le proporcionarán información y consejos sobre el robo de identidad.

Muchas gracias por su atención.

Subsecretario Asistente Segundo Parsons: ¡Hola! Mi nombre es Scott Parsons. Soy Subsecretario Asistente del Departamento del Tesoro para la Protección de Infraestructura Crítica. Lo que ha visto hasta ahora es un ejemplo de los sectores público y privado trabajando juntos para enviar el mensaje de que el robo de identidad no es aceptable, y nosotros podemos hacer mucho para detener a los ladrones responsables de este crimen.

Antes de que concluyamos, creemos que le gustaría ver desde dentro lo que las autoridades federales están haciendo para asumir el reto de detener el robo de identidad. Vayamos al Centro de Operaciones de Crímenes Cibernéticos en la sede central del Servicio Secreto de los Estados Unidos en Washington DC.

Narrador: Éste es el Centro de Operaciones de Crímenes Cibernéticos del Servicio Secreto de los EE. UU. Es el punto central de contacto para la recopilación de pruebas para el procesamiento, inteligencia e investigación. Aquí los agentes enfocan mejor sus esfuerzos en la lucha contra el crimen por Internet a gran escala.

Se necesita el trabajo en equipo para descifrar crímenes cibernéticos complicados. Normalmente se empieza aquí con los especialistas forenses que descodifican los discos duros de los criminales.

USSS Agent #1: Lo que he hecho es tomar su computadora, sacarle el disco duro y hacer una copia. Hice una copia, una copia exacta. Se llama copia forense. Y ahora estoy repasando mi copia, buscando pruebas, o información secreta, o cualquier cosa que nos pueda ayudar con el caso.

Narrador: Tienen que tener mucho cuidado con cómo obtienen pruebas de computadoras si quieren usar esas pruebas en corte.

USSS Agent #1: Lo que encontré fue un documento en su computadora que contiene lo que parecen ser números de tarjeta de crédito y fechas de caducidad. Obviamente ésa es una buena pista para nosotros porque ahora tenemos algo a partir de lo que podemos seguir.

Narrador: El equipo sigue la pista de las acciones del criminal con la información obtenida del disco duro, empezando con los datos recuperados gracias a la inspección forense.

USSS Agent #2: Lo que estoy haciendo es mirar la información de identificación bancaria para ver quién emitió las tarjetas de crédito, y luego podremos llamar a los investigadores de fraude de esos bancos para determinar si se ha producido un fraude con las tarjetas y, posiblemente si los investigadores del banco han determinado un punto desprotegido del que se obtuvo la información.

Narrador: Toda investigación requiere cooperación y una atención especial a los requisitos legales.

USSS Agent #3: Lo que voy a hacer ahora es determinar de dónde llegó esta tarjeta. Creo que llegó de un e-mail. Ahora tomo el e-mail y lo miro desde los encabezamientos para determinar dónde se originó. Algunas de las cosas que busco en el encabezamiento del e-mail es quién lo envió, la dirección IP de donde se originó y la identificación del mensaje.

Narrador: Esos números de tarjeta de crédito robados que vimos antes son bienes muy valiosos en la calle. Los ladrones que reúnen números necesitan convertirlos en efectivo. ¿Qué mejor lugar que la Internet para hacerlo? Los ladrones usan tablones de avisos para anunciar sus artículos especiales en lo que es un bazar virtual.

USSS Agent #4: "Tarjetas de crédito", "Seguridad de celulares", "Registradores de teclas físicas", "Timos de Money Order", "Navegación anónima", "Guía del criminal para quitar retenciones en deudas", "Tutoría"…

Narrador: Los agentes especiales del Servicio Secreto se ponen de incógnito para desmantelar estos mercados cibernéticos altamente organizados.

USSS Agent #4: Algunos funcionan como empresas Fortune 500, en las que hay un presidente que se encarga de todo el mundo. Tiene un grupo de hackers. Tiene un grupo de robo de identidad. Tiene un grupo de pasaportes. Y cada una de las facciones se responsabiliza sólo de lo que hace. Así que si contrata un golpe contra un procesador de tarjetas de crédito o una empresa, hacen la penetración y le dan los números. Él se los da a su gente, les proporciona las tarjetas de crédito y fabrican las tarjetas falsas. Así que hacen las cosas de una manera muy estructurada y jerarquizada.

Narrador: Lo que se comercia en la superautopista cibernética encuentra su valor en efectivo en la calle.

USSS Agent #5: En otras palabras, los números de cuenta, los números del Seguro Social, los certificados de nacimiento, toda esta información robada, no tiene ningún valor hasta que vuelve a la calle en forma de identidades falsas, tarjetas de crédito falsas, y de hecho se usan.

Narrador: El Servicio Secreto ayuda a entrenar a las autoridades locales.

USSS Agent #5: En el Servicio Secreto hemos estado dirigiéndonos a las autoridades locales para entrenarlas en cómo identificar pruebas de estos crímenes, para que cuando hacen una detención de tráfico rutinaria o cosas así, puedan reconocer lo que puede que esté en el asiento de atrás del carro que han detenido, o cuando están ejecutando una orden de registro reconozcan las herramientas de estos crímenes.

Narrador: Con un equipo creciente de 200, el Servicio Secreto trabaja desde todos los lados del problema para agarrar a estos ladrones cibernéticos cada vez más ingeniosos.

Subsecretario Asistente Parsons: Esperamos que la información de este programa le haya sido de utilidad ya que describe el problema del robo de identidad, lo que puede hacer para proteger mejor su información personal y que acciones puede tomar si desafortunadamente se convierte en víctima del robo de identidad. Con una tecnología inteligente e innovadora, instituciones financieras comprometidas y ciudadanos informados, podemos seguir disfrutando de un sistema financiero fuerte y vital, que es parte de nuestra vida diaria.

Además quiero recordarle la Biblioteca de Recursos que también contiene este DVD, la cual incluye documentos importantes y proporciona enlaces a sitios web que le proporcionarán consejos e información valiosa acerca del robo de identidad

Quiero dar las gracias a los participantes y a los panelistas. En nombre del Departamento del Tesoro, quiero agradecerle su atención.