TRIBUNAL CIVIL DE LA CIUDAD DE NUEVA YORK
SERIE DE SEMINARIOS COMUNITARIOS
«ROBO DE IDENTIDAD»

Phaedra F. Perry

30 de enero de 2008

Transcripción hecha por Ubiqus Reporting
Irvine CA; (949) 477- 4972 New York, NY (212) 227- 7440
w w w . u b i q u s . c o m

[Inicio 108_425-AUDIO.MP3]

HABLA EL SR. EDGAR PÉREZ: Buenas tardes. Me llamo Edgar Pérez, y hoy vamos a hablar sobre el robo de identidad. Como sabemos, esto representa un grave problema en Estados Unidos, un gran error económico y eso es algo que tenemos que resolver hoy día. Vamos a informarnos más al respecto hoy ya que, al final del día, tendremos también algunas preguntas que contestar al respecto.

Nuevamante, me llamo Edgar Pérez y trabajo para el Citibank. Soy un especialista en educación financiera. Vamos a llevar a cabo una presentación hoy día y tal parece que todos recibieron un folleto con información relacionada con la presentación de hoy. No solo eso, sino que también hay un resúmen de esa información sobre robo de identidad, la cual ustedes necesitan conocer, tanto como un formulario de evaluación del seminario, el cual les agradeceré sobremanera si pueden llenarlo.

Habiendo dicho esto, vamos a comenzar. Y, mientras dejamos algunas preguntas para el final, les voy a hacer algunas preguntas, simplemente para que levanten la mano. Permítanme comenzar con esto. ¿Cuántas personas portan sus tarjetas de seguro social? Quizás dos o tres personas. Esa es una cifra buena. ¿Cuántas personas han revisado su historal de crédito este año? Quizás sea muy temprano para decir este año, pero digamos durante los últimos seis meses. Aún así, solo unas dos o tres personas. Muy bien. Déjenme preguntarles algo. ¿Tienen una trituradora de papeles en sus hogares? ¿Sí? Magnífico. Tal parece que un 50% de la gente tiene una trituradora de papel en sus casas. Maravilloso.

Estas son preguntas introductorias, y tal parece que ustedes están tomando la iniciativa para proteger sus identidades. Por lo

tanto, regresemos a lo que vinimos.

Hoy día, el robo de identidad es uno de los crímenes de crecimiento más acelerado en Estados Unidos. Cada año, medio millón de norteamericanos tienen este problema. ¿Y ustedes creen que la cifra es alta o baja? Bueno, déjenme decirles. Esa cifra es probablemente superior a eso. ¿Por qué? Porque muchas personas desconocen que sus identidades corren peligro. Y se enteran de ello mucho más tarde, cuando reciben una llamada telefónica por parte de una agencia de cobros, reclamando una deuda que usted desconoce. Definitivamente, es un crímen que va en aumento.

Consideramos que en Estados Unidos existen unas 25 millones de personas que han sido afectadas por robo de identidad, lo cual significa 1 de cada 12 norteamericanos.

Por lo tanto, hoy vamos a hablar sobre el robo de identidad. Vamos a definir lo que es, las diferentes clases, los síntomas para identificarlo, cómo protegernos al respecto y qué hacer de manera efectiva si algo así nos sucediera.

Por lo que vamos a definir el tema. El robo de identidad ocurre, básicamente, cuando alguien utiliza nuestros datos para establecer una cuenta de crédito, para obtener crédito. ¿Qué tipo de información pueden obtener? Bueno, un nombre, una dirección, un número de una cuenta de Seguro Social, una fecha de nacimiento y el apellido de soltera de una madre. Esos son los cinco datos que la gente va a necesitar, tan solo cinco datos informativos, para aplicar por una tarjeta de crédito a través del Internet, para aplicar por una cuenta nueva. Y, por lo tanto, ellos pueden hacerlo si nosotros, por alguna razón, se lo permitimos.

Así que, ciertamente, esos cinco datos informativos son muy importantes. Y como dije y pregunté antes, guardar su número de cuenta de Seguro Social - por lo menos la tarjeta - en un lugar seguro, es importante. Ustedes quieren asegurarse de que están protegiendo su número y no le están brindando esa información a nadie que le llame por teléfono, aunque digan que le llaman desde un banco o de cualquier otra institución. Así que, definitivamente, vamos a hablar de estas medidas dentro de unos segundos.

Hablemos de fraude y de robo de identidad. Sabemos lo que es el fraude. Digamos que usted tiene una chequera y por alguna razón la pierde. Quien la encuentra comenzará a escribir cheques. Va a usar sus cheques, van a falsificar su firma y van a pagar sus cuentas. ¿Es eso robo de identidad? Veo a algunas personas diciendo que no con sus cabezas. Muy bien.

Bueno, permítanme informarles. Eso no es robo de identidad, ya que la gente roba. Ellos pueden cometer fraude, sí, pero aún, ellos no pueden abrir cuentas nuevas. No pueden ir al banco y decir, «Soy el Sr. X, y quisiera solicitar una tarjeta de crédito.» Eso es robo de identidad. ¿Sí?

Vamos a continuar. Definitivamente hay diferentes tipos de robo de identidad. Pero hoy nos vamos a concentrarnos en el robo de identidad financiero. ¿Qué significa eso? Básicamente, crímenes financieros. Cuando la gente usa su identidad para obtener nuevo crédito y para tener acceso al mismo, potencialmente arruinando su crédito.

Ahora bien, la pregunta es ¿Cómo obtienen nuestra información? Créanlo o no, la gente es muy astuta al respecto y no tiene nada que ver con la alta tecnología. Puede ser algo muy sencillo,

tecnológicamente hablando. Si no tenemos una trituradora de papeles en nuestro hogar, la gente revisa la basura. Ellos pueden llegar a las afueras de su hogar, la basura que tiramos y creemos que se la han llevado... eso puede ser una mina de oro. Y ellos pueden revisar esa información para ver si pueden tener acceso a su nombre, dirección, número de cuenta de Seguro Social y fecha de nacimiento. Ya ellos saben donde usted vive. Conocen su nombre. Pero les falta su número de Social, su fecha de nacimiento y el apellido de soltera de su madre para obtener un esbozo completo. Así que los cubos de la basura son importantes. Cualquier información que tengamos en casa va a ser desecha si no la nececitamos más. Usemos una trituradora de papel. De lo contrario, si se va a quedar en casa, protéjala.

Documentos importantes, tales como pasaportes, tarjetas de Seguro Social, fechas de nacimiento y actas de nacimiento, deben ser protegidos en un lugar seguro. No se puede dejar nada ni siquiera sobre la mesa, porque la gente entra y sale. Quizás sus amistades invitan a otras amistades y ellos quieren llevarse ciertos documentos. Más tarde, usted nota que sus documentos no están allí. De nuevo, el proteger nuestra información comienza en la casa.

Usted no tiene que llevar consigo todas las cosas que ha de necesitar dentro de su billetera. Usted quiere llevar consigo tan sólo lo mínimo necesario. Usted porta su tarjeta de cajeromático, lo que puede ser una buena idea para minimizar cargar con dinero en efectivo, pero si porta sus tarjetas, asegúrese de cambiar su clave de acceso tan a menudo como pueda. Esos cuatro dígitos no pueden ser su fecha de nacimiento, ya que eso es algo que alguien puede adivinar o saber de una forma u otra. De nuevo, tiene que ser una

clave que tenga sentido sólo para usted y que sea cambiada de vez en cuando, para que nadie la recuerde. Y aunque la conozcan, no funcionará la próxima vez.

El correos es también importante, especialmente para personas que residen en las afueras de la ciudad. Si nos vamos de vacaciones, y la correspondencia llega, y llega, y llega y nadie la recoje, alguien que pase por allí puede pensar: "Oh, no hay nadie en casa. Déjame recoger la correspondencia." Señores, especialmente en las afueras, cuando no hay nadie afuera, es muy fácil hacer eso. El caso es que si van a vacacionar por una o dos semanas, es una buena idea indicarle al cartero o a la oficina de correos que frenen la entrega de correspondencia, que usted ha de recojerla cuando regrese. A menos que tenga a alguien que la recoja por usted. Pero, definitivamente, eso es algo que podemos hacer para protejer nuestra información.

Algo más, recibimos mucha correspondencia, estados de cuentas bancarias, de compañías de tarjetas de crédito, del Seguro Social, del Departamento de Vehículos de Motor, etc. Queremos reducir todos esos papeles. ¿Cómo hacerlo? Si tiene cuenta bancaria, quizás sea una buena idea informarle al banco que usted no desea continuar recibiendo estados bancarios por escrito, sino que desea que se los envíen por correo cibernético, para que cada vez que tenga un nuevo estado de cuentas, usted reciba un mensaje cibernético indicando que su estado de cuentas está disponible y puede revisarlo en cualquier momento a través del Internet. Esa es otra manera de reducir esos papeles tan peligrosos.

Cuando hablamos de computadoras, eso es otra frontera relacionada con el robo de identidad. Por alguna razón, tenemos una de escritorio,

pero compramos una nueva y portátil. ¿Sacamos la de escritorio a la basura? No, tenemos que asegurarnos que va a ser destruída, que toda la información que contenga será totalmente destruída. Así que, si tienen, por así decirlo, un disco de almacenamiento de datos, él contiene un exceso de información. Y algunas personas pueden andar persiguiendo esa información para tener acceso a ella, para saber quiénes somos. Entonces, ¿qué hacemos al respecto? Asegúrense de destruír el disco de almacenamiento de datos. Pueden usar Norton Utilities, pueden usar Symantec, esos programas que borran toda la información. Si no, ahógenlo en Coca Cola o usen un imán superpotente, destruyan el disco. O colóquenlo en un horno de microondas por diez minutos. De esa forma, se ha de destruír toda la información. ¿Bien?

Vamos a continuar. Y con relación a cuentas de crédito y de débito, hay algo muy importante que debemos saber. ¿Cuántas personas usan tarjetas de crédito en el Internet? Una, dos, tres, cuatro, cinco, seis. Parace que la mayoría lo hace. Y, claro está, es muy cómodo, podemos hacer eso, claro que sí. Por otro lado, si desea comprar libros, podemos visitar Amazon.com y podemos estar seguros de que ellos van a proteger nuestra información. Sin embargo, hay pequeños sitios Web que no invierten suficiente dinero en proteger la información del cliente. Así que, ¿cómo – qué podemos hacer si todavía queremos comprar algo de estas compañías, pero no tenemos acceso, ni otra forma de comprar a través de ellos?

Bueno, en esos casos, los bancos pensaron sobre eso y decidieron crear el número de cuenta virtual. ¿Pero qué es eso? Si queremos usar nuestra tarjeta de crédito a través del Internet, pero no queremos dar nuestro verdadero número de tarjeta de crédito, podemos marcar

el número telefónico, localizado an el reverso de la tarjeta de crédito, del departamento de servicios al consumidor, y podemos decirles que vamos a utilizar nuestras tarjetas de crédito hoy y mañana, por un total, por ejemplo, de US$300.00. Queremos obtener un número de cuenta virtual. Y eso es precisamente lo que obtendremos. Ellos nos asignarán un número de 16 dígitos que funcionará como un número de tarjeta de crédito, pero sólo por los días solicitados y por la cantidad que decidamos. Después de esto, vamos a decir que queremos usar esa tarjeta de crédito o ese número virtual hoy y mañana. Después de esto, expirará. Nadie podrá usarlo. Muy bien. Así que eso es un número de cuenta virtual. Y la belleza del mismo consiste en que hoy día, hasta usted puede dirigirse hacia el sitio Web de su compañía de tarjeta de crédito y generar usted mismo un número de cuenta virtual que usted puede copiar y pegar en el sitio Web donde quiera usarlo. ¿Bien? Así que eso es algo que podemos hacer ahora para proteger nuestros veraderos números de tarjetas de crédito, para evitar el robo de identidad.

Es siempre importante ser cuidadosos con las personas que manejan nuestras tarjetas de crédito cuando hacemos compras. Si vamos a ir a un restaurante, debemos asegurarnos de que si recibimos dos copias de la información de nuestra tarjeta de crédito, que las mismas sólo contengan los últimos cuatro dígitos. ¿Sí? Lo mismo aplica para nuestras copias. De igual modo, si vamos a usar nuestras tarjetas de débito, debemos asegurarnos de usarlas, exclusivamente, en los bancos, no en los delis. Por alguna razón, algunas personas van a los cajeromáticos de los delis y les insertan ciertos materiales para obtener información que haya sido usada en ellas. Así que, de nuevo, usen las tarjetas

de débito exclusivamente en sus bancos, ya que brindan una protección mejor y más segura. Y, claro está, si va a ser nuestro banco, no hay que pagar una tarifa por usar la tarjeta.

Continuemos aquí. El Internet es otra frontera, como dije antes. Habrá formas en que la gente tratará de obtener nuestra información utilizando el Internet. Y, probablemente, estemos familiarizados con eso. Digamos que algunas veces recibimos mensajes por correo electrónico, los cuales nos informan que nuestra cuenta bancaria ha sido embargada y que tenemos que actualizar nuestra información. Básicamente nos muestran un formulario con muchas casillas, tales como nombre, dirección, número de cuenta de seguro social, fecha de nacimiento, todo. Y ellos quieren que actualicemos esa información y la enviemos. Tan pronto recibamos tales mensajes, tenemos que borrarlos, ya que ninguna institución seria nos va a solicitar que actualicemos nuestra información a través del Internet. Si hay que actualizar algo, nos pedirán que visitemos la sucursal bancaria. Así que, por lo tanto, eso va a ser una historia distinta. Solamente personas inescrupulosas harían algo de esa naturaleza. Y lo hacen. Y continúan haciéndolo porque algunas personas se dejan engañar. Así que, cuando reciban esos mensajes por el Internet, pidiendo información personal, hay que borrarlos. Y hay que marcarlos como mensajes basura (spam).

No solo eso, podemos recibir dichos mensajes o podemos recibir enlaces. Y esos enlaces, cuando los activamos, nos llevarán a otra pantalla con los mismos formularios, solicitando nombres, direcciones, números de cuenta de seguro social, fechas de nacimiento, etc. Todos esos documentos para que los llenemos. No tenemos que caer en la

trampa. Tan pronto recibamos esos mensajes, hay que borrarlos, ya que esa es la forma más fácil de obtener información. Y algunas personas, como dije, todavía se dejan engañar.

Si hace negocios con, digamos, cualquier banco, y quiere entrar al Internet, asegúrese de visitar el sitio Web exacto que le hayan indicado. Digamos que desea hacer negocios con el Citibank, visite www.citibank.com, porque ese es el sitio que desea visitar. No confíe en los enlaces. Algunas veces recibimos mensajes que parecen exactamente iguales a los mensajes de Citibank, el mismo color, el mismo logo y todo lo demás. Cuando los activamos, nos llevan a un sitio que parece ser el sitio del Citibank. Pero no es así. Ellos no le pedirían que haga eso. Tenemos que asegurarnos de que la dirección cibernética que vamos a visitar es la correcta, y no demos nuestra información tan facilmente. ¿Entendido? Así que esas van a ser medidas extras de precaución, las que hay que tomar para protejer nuestras identidades.

Cuando pensamos en sitios Web, es importante que protejamos nuestra información utilizando programas antivirus y filtros electrónicos de seguridad (firewalls). Como sabemos, la gente es muy ingeniosa. Siempre están inventando virus nuevos, y algunos de esos virus tratan de obtener información de nuestras computadoras. Pueden hasta borrar información. Y pueden hasta instalar rastreadores para saber exactamente qué sitios Web visitamos, qué nombres y qué claves y qué contraseñas utilizamos.

Esta es la razón por la cual es importante instalar programas antivirales, tales como Norton Antivirus, Symantec, cualquiera de los dos. Es importante instalarlos en nuestras computadoras.

También es importante saber que no debemos usar ni procurar tener acceso a información confidencial en locales públicos. Quizás tengamos confianza al hacer eso en nuestros hogares, o en nuestros trabajos, pero no en las bibliotecas públicas. Porque, al irnos, alguien puede venir, puede que lleguen a tener acceso a la información que quede allí. Simplemente regresando una y otra vez, podrían ver información que no deben ver.

De nuevo, tengan cuidado al usar eso, aunque quieran usar una red inalámbrica. Como sabrán, ellas no son seguras. Así que, básicamente, la información entre usted y la red será información pública. Por lo que es algo que tenemos que proteger, y no debemos procurar acceso en esos locales inseguros a información bancaria, a la información de nuestros fondos mutuales ni a la información de nuestra jubilación.

Permítanme revisar el punto final sobre cómo la gente puede tener acceso a nuestra información. Si recibimos un mensaje cibernético ofreciendo descuentos para un crucero por el Caribe, 5 días por $300, podríamos enviar la información que solicitan, pero la mayoría de las veces no volvemos a saber de ellos. Ellos tan sólo desean nuestra información. Por lo que tenemos que ser cuidadosos. Siempre que alguien solicite nuestra inforamción, debemos asegurarnos de que conocemos a quien solicita dicha información.

Vamos a decir que estamos navegando el Internet, y vemos un anuncio que dice «Gratis! Reporte de Crédito!» Entonces decimos, «¡Oh! Quiero saber cómo está mi crédito. Déjame activar esa página Web.» Bueno, si activamos ese enlace, algunos de ellos tan sólo quieren tener acceso a nuestra información y, por lo tanto, no dan nada a cambio. Simplemente nos dan cierta información y hasta nos cobran

por ello. Vamos a ver más tarde cómo obtener nuestro verdadero puntaje, cómo hacerlo, dónde ir para obtener informació y saber cómo está nuestro crédito. Pero no a través de esos mensajes cibernéticos, no a través de esos enlaces en esas páginas Web.

De nuevo, esas van a ser las diferentes formas en que la gente trata de obtener nuestra información. Tenemos que ser extremadamente cuidadosos antes de proporcionar nuestra información. Más tarde, hablaremos de las formas específicas en que podemos lidiar con esto, qué podemos hacer para proteger nuestra información. Por ahora, hemos aprendido de qué es capaz la gente para obtener nuestra información. Por lo que continuaremos dentro de unos minutos con la próxima parte de la presentación.