



**JOHN J HOFFMAN**

*Fiscal General Interino*

**División de Asuntos del Consumidor**

Steve C. Lee, *Director Interino*

**Prensa:**

Jeff Lamm 973-504-6327

Neal Buccino 973-504-6327

**Para publicación inmediata**

Día 21 de Mayo del 2014

**La División de Asuntos del Consumidor de New Jersey urge a los clientes de eBay que cambien sus contraseñas, tomen otras medidas protectoras en contra del robo de identidad en respuesta a un ataque de cibernética**

**NEWARK** – El Fiscal General Interino John J. Hoffman y la División de Asuntos del Consumidor de Nueva Jersey (New Jersey Division of Consumer Affairs) hoy urgen a todos los residentes de New Jersey que son clientes de eBay Inc. que cambien sus contraseñas, como eBay ha recomendado, y tomar otras medidas protectoras en contra del robo de identidad, debido a un ataque de cibernética que se ha reportado pone en peligro la seguridad de cierta información, no financiera, como los nombres de los clientes, las contraseñas encriptadas, las direcciones de emails, las direcciones físicas, los números de teléfonos, y las fechas de nacimiento.

“Cualquiera que ha sido un cliente de eBay debe tomar pasos proactivos para asegurarse que un ataque de cibernética o violación de datos no termine en un problema peor de robo de identidad,” dijo el Fiscal General Interino John J. Hoffman. “Cambiar su contraseña, es un paso importante. Medidas adicionales como obtener sus reportes de crédito y mantener vigilancia en sus cuentas financieras le proveerá sosiego mental – y puede prevenir que sea una víctima de fraude.” Estos pasos están delineados en detalle abajo.

Un representante de eBay Inc. hoy se puso en contacto con el Fiscal General Interino Hoffman y con el Director Interino de la Division of Consumer Affairs, Steve Lee, acerca del ataque cibernético, que según la compañía tuvo lugar a finales de Febrero y principios de Marzo, y fue detectado al comienzo de este mes. El ataque se cree pone en peligro la base de datos que contenía las contraseñas encriptadas y otra información no financiera de los clientes de eBay.

“Urgimos que todos los individuos que han podido ser afectados por este acontecimiento, no solamente cambien sus contraseñas pero que tomen otros pasos básicos para protegerse de robo de identidad,” dijo el Director Interino de la Division of Consumer Affairs Director Steve Lee. “La mejor protección contra el robo de identidad es una acción rápida por aquellos cuya información personal puede haber sido puesta en peligro.

Dice eBay que ha tomado pasos para cerrar acceso sin autorización a su sitio web y ha mejorado sus medidas de seguridad, y está cooperando con los implementadores de las leyes y los expertos de seguridad. La compañía está pidiendo a todos los usuarios que cambien sus contraseñas. Individuos que usan la misma contraseña en otros sitios webs, se les está también pidiendo que las cambien. La compañía tiene 145 millones de compradores activos, y dice que va a notificárselo a todos los usuarios.

La compañía dijo que consumidores que solamente van a eBay como *guest users* y que no tienen contraseñas archivadas, también tienen que estar vigilantes. Varias clases de fraude, incluyendo ataques de *phishing*, con frecuencia siguen a estos ataques de cibernética. Ataques de *phishing* y artimañas de fraude de identidad pueden ocurrir por email, correo o llamada telefónica. Los criminales pueden abordar a posibles víctimas, pretendiendo ser representantes de una compañía, en este caso eBay, que ha sido el tema de un ataque de cibernética de gran publicidad, para pedir información personal. Los consumidores nunca deben dar su información personal en respuesta a un email, carta, o a una llamada telefónica, sin primero tomar pasos para independientemente verificar que el pedido es legítimo.

La Division of Consumer Affairs les dice a los clientes de eBay que no solamente cambien sus contraseñas, pero que tomen ocho pasos adicionales que todos los consumidores deben tomar cuando creen que están expuestos a robo de identidad.

Estos ocho pasos están delineados en la Cyber Safe NJ website, [www.NJConsumerAffairs.gov/cybersafe](http://www.NJConsumerAffairs.gov/cybersafe), y proveídos abajo.

### **Si está expuesto a robo de identidad:**

1. Ponga una queja con la Federal Trade Commission o FTC (Comisión Federal de Comercio) en [www.ftc.gov/complaint](http://www.ftc.gov/complaint) (pulse en español) o llame al 877-438-4338. <http://www.protecciondelconsumidor.gov/> (vea paso 2).
2. Su queja se llama un "FTC Affidavit." Tiene que llevar una copia del affidavit a su policía local;
3. Ponga una queja con su policía local y entréguele una copia del affidavit del FTC. Una vez que ha puesto una queja con la policía obtenga una copia para que pueda mandarla a las tres agencias reportadoras de crédito, y a sus acreedores.
4. Pídale a las agencias de crédito una copia de su reporte de crédito (usted tiene el derecho de recibir una copia gratis de cada agencia una vez al año)

Póngase en Contacto con éstas en:

**Equifax Credit Information Services**  
Consumer Fraud Division  
(800) 525-6285  
[equifax.com](http://equifax.com)

**Experian**

(888) 397-3742

[experian.com/consumer](http://experian.com/consumer)

**Trans Union**

Fraud Victim Assistance Department

(800) 680-7289

[tuc.com](http://tuc.com)

Dígale a las agencias de reporte de crédito que usted sospecha robo de identidad, y que pongan una alerta en todas sus cuentas.

5. Revise sus tarjetas de crédito y débito todos los meses. Muchos proveedores de tarjetas de crédito ofrecen acceso a su cuenta de tarjeta de crédito en línea. Si puede, revise su cuenta diariamente. Si no puede acceder su cuenta en línea, llame al número en la parte de atrás de la tarjeta que sospecha ha sido afectada.
6. Contacte sus compañías de tarjetas de crédito, acreedores, bancos, y cualquier institución financiera con la cual hace negocios. Cierre la tarjeta de crédito afectada o las cuentas bancarias, y obtenga reemplazos para las tarjetas de crédito con nuevos números de cuentas. Cambie sus contraseñas en las cuentas de banco, incluyendo los PIN. Después de su conversación por teléfono confirme lo que les ha dicho con una carta.
7. Póngase en contacto con la United States Social Security Administration (Administración de Seguro Social de EEUU):

**Social Security Administration**

Social Security Fraud Hotline

P.O. Box 17768

Baltimore, MD 21235

(800) 269-0271

TTX: (866) 501-2101

[ssa.gov/oig/hotline](http://ssa.gov/oig/hotline)

8. Mantenga un archivo con toda la documentación y haga copias de todo lo relacionado con el asunto incluso los correos electrónicos. Escriba todo lo que habló por teléfono y anote el nombre de la persona y de la agencia, acreedores, o recaudadores de deudas. Cuando hable con alguien por teléfono pregúntele el nombre y anótelo junto con la fecha cuando hizo la llamada. Confirme todas sus conversaciones por teléfono y escríbales una respuesta por escrito. Mandé su correo certificado con recibo de retorno. Guarde los recibos de los gastos incurridos en la infiltración de robo de identidad, en caso de que pueda obtener restitución en un juicio en contra del ladrón de identidad.
9. Puede también ponerse en contacto con agencias sin fines de lucro que proveen asistencia a víctimas de robo de identidad. Por ejemplo:

## **Identity Theft Resource Center**

(888) 400-5530

[www.idtheftcenter.org](http://www.idtheftcenter.org)

La New Jersey Division of Consumer Affairs protege a los consumidores del robo de identidad, invasión ilegal de la privacidad, y otras violaciones relacionadas con las computadoras implementando el New Jersey's Consumer Fraud Act (Acta de Fraude para el Consumidor) , el Computer Related Offenses Act (Acta de Ofensas Relacionadas a la Computadora), el Identity Theft Protection Act (Acta de Protección de Robo de Identidad), y otras leyes como la federal COPPA, Children's Online Privacy Protection Act (Acta de Protección de Privacidad en Línea de Niños) .

El sitio web de la División Cyber Safe NJ, en [www.NJConsumerAffairs.gov](http://www.NJConsumerAffairs.gov), provee sugerencias provechosas para ayudar a los consumidores a tomar un papel activo para que puedan protegerse a sí mismos y a su información en el mundo cibernético.

Los consumidores que creen han sido defraudados o engañados por un negocio, o sospechan cualquier otra clase de abuso al consumidor, pueden poner una queja con la Division of Consumer Affairs yendo al sitio web de la División:

<http://www.njconsumeraffairs.gov/espanol/spcomplaint/spcomplaint.htm>

o llamando al 1-800-242-5846 (gratis si llama desde New Jersey) o al 973-504-6200.

Siga la Division of Consumer Affairs en Facebook, y chequee nuestro calendario de eventos en Consumer Outreach.

###