NEW JERSEY DIVISION OF CONSUMER AFFAIRS

FIGHTING FRAUD

ROBO DE IDENTIDAD Y PHISHING

(IDENTITY THEFT and PHISHING)

El gobierno federal ha reportado que el crimen financiero que está creciendo con más rapidez es el robo de identidad. Cada 79 segundos, un ladrón roba la identidad de una persona y abre cuentas en el nombre de la víctima.

Para proteger a los residentes de Nueva Jersey de robo de identidad, el Acta de Prevención de Robo de Identidad se puso en efecto el día 1 de Enero del 2006.

LA LEY DE NUEVA JERSEY:

- Requiere que las agencias de implementación de leyes tomen un reporte policial, si usted dice que ha sido víctima de robo de identidad;
- Permite que usted ponga un seguro de congelación en su reporte de crédito lo cual prohíbe a las agencias de reporte de crédito publicar su información a una tercera parte sin su permiso;
- Requiere que entidades públicas destruyan sus expedientes, si estos contienen información personal, cuando los expedientes son eliminados;
- Requiere que negocios o entidades públicas que compilan o mantienen expedientes computarizados que incluyen información personal que informen, si hubo una brecha de seguridad en esos computarizados expedientes, a cualquier residente de Nueva Jersey cuya información personal se cree ha sido obtenida por una persona sin autorización; y
- Prohíbe que cualquier entidad pública o privada ponga, publique o imprima su número de Seguro Social, o lo manden en materiales por correo, o intencionadamente hagan su número de Seguro Social disponible al público en general, o lo transmitan a través del internet a no ser que el número esté encriptado.

LOS CONSUMIDORES PUEDEN PROTEGERSE HACIENDO LO SIGUIENTE:

- Mantenga una lista de todos los números de sus cuentas incluyendo sus números de tarjetas de crédito y las fechas de expiración, así como los números de teléfonos de sus acreedores.
- Revise con cuidado sus extractos bancarios y facturas para ver si están correctos y póngase en contacto con sus acreedores si sus facturas no llegan a tiempo.
- NO conteste a emails (incluso cuando parecen oficiales) que le pidan información personal o su cuenta de banco. En vez llame a la compañía o vaya directamente al sitio web de la compañía si sabe la dirección correcta de la web.
- NO dé información personal por teléfono a los telemercaderes. Si decide comprar algo o donar a una caridad, pídales que le manden una factura.
- NO dé su información de tarjeta de crédito por teléfono a compañías a no ser que usted ha iniciado la llamada y tiene una relación establecida con la compañía que ha llamado.
- Cuando compre en el internet, provea su número de tarjeta de crédito solamente después que se haya asegurado que el sitio web es legítimo y que es controlado y mantenido por una compañía fidedigna. Revise la política de privacidad de la compañía para determinar cómo va a usar su información personal.
- Si pierde o le roban su cartera, tarjetas de crédito o cheques, cancélelos.
- Destruya todo lo que tenga su identificación personal incluyendo recibos de tarjetas de crédito. Asegúrese de destruir también ofertas pre aprobadas de crédito que le mandan por correo.

Continua

Sea un consumidor bien informado... ¡Podemos ayudarlo!

800-242-5846 ▪ NJConsumerAffairs.gov

PHISHING:

Hay una estafa usada por los ladrones de identidad llamada "phishing". Se atrae a las víctimas con emails disfrazados como avisos oficiales, mensajes de texto, o inesperadas llamadas telefónicas de una compañía u organización ilegal, pidiéndole su información personal y financiera, como el número de de su tarjeta de crédito o cuenta de banco. Según el National Consumer League, phishing es la cuarta estafa más común en el internet.

- Si recibe un email o ventana espontánea pidiendo su información personal, no responda.
- No mande por email información personal o financiera. Email no es una forma de transmitir información personal.
- Mire por indicaciones de que el sitio que está visitando es seguro. Un icono de un candado o una dirección que empieza por "https" (la "s" quiere decir segura) son seguros.
- Llame a la organización y pregunte si el email es legítimo.

SI CREE QUE ES UNA VÍCTIMA DE ROBO DE IDENTIDAD:

1. Ponga una alerta de fraude en su reporte de crédito llamando a las tres compañías de reporte de crédito:

Equifax	1-800-525-6285
www.equifax.com	P.O. Box 740241 Atlanta, GA 30374
Experian	1-888-397-3742
www.experian.com	P.O. Box 9532 Allen, TX 75013
Trans Union	1-800-680-7289
www.transunion.com	Fraud Victim Assistance P.O. Box 6790 Fullerton, CA 92834

2. Cierre todas las cuentas que sabe o que cree han sido manipuladas o abiertas fraudulentamente.
3. Ponga un reporte con su policía local o la policía en la comunidad donde cree el robo de identidad tuvo lugar.
4. Vaya a **www.NJConsumerAffairs.gov** para ponerse en contacto con la División de Asuntos del Consumidor en línea
5. Vaya a **www.consumer.gov/idtheft** para poner una queja con la Federal Trade Commission o FTC (Comisión Federal de Comercio).

   Puede llamar al FTC gratis a:

   1-877-438-4338
   TDD 202-326-2502 (sordomudos)
   O puede escribir o llamar a

   Identity Theft Clearinghouse
   Federal Trade Commission
   600 Pennsylvania Avenue
   NW, Washington, DC 20580

   1-877-FTC-HELP
   (1-877-382-4357)

Sea un consumidor bien informado... ¡Podemos ayudarlo!
800-242-5846 • NJConsumerAffairs.gov