News
New Jersey
Office of the Attorney General
NEW JERSEY DEPARTMENT OF LAW & PUBLIC SAFETY

Christopher S. Porrino
Fiscal General

Para publicación inmediata:
Día 30 de Octubre del 2017

Para más información contacte:
Prensa: Sharon Lauchaire
609-292-4791
Ciudadanos: 609-984-5828

NJ por primera vez publica estadísticas anuales de filtraciones de cibernética

El Fiscal General les recuerda a los ciudadanos que estén alerta y ofrece recursos durante el Mes Nacional de Educación de Ciber-seguridad

---

TRENTON – El Attorney General Christopher S. Porrino y la New Jersey State Police hoy anunciaron que 676 filtraciones de información de datos fueron reportados a la State Police en el 2016 afectando a más de 116,000 titulares de cuentas de New Jersey. Octubre es el National Cybersecurity Month, y el anuncio – la primera publicación de estadísticas anuales de filtraciones de datos en el estado – ha sido hecho al mismo tiempo que New Jersey ofrece aviso y recursos a los residentes para proteger su información confidencial personal. La Attorney General's Office también ha subrayado las acciones legales tomadas este año por la Division of Law y la Division of Consumer Affairs para tratar las filtraciones de datos.

"Hacer negocios en línea y en nuestros aparatos se ha convertido en una rutina por lo que es fácil descuidar nuestra protección. Pero como estas estadísticas de filtraciones de datos subrayan, es importante que protejamos nuestra información personal confidencial de los muchos que buscan accederla por fines fraudulentos," dijo el Attorney General Christopher Porrino. "El internet toca todos los aspectos de nuestra vida cotidiana, ya lo reconozcamos o no, y el Cyber Security Awareness Month es un tiempo bueno para examinar si nuestras cuentas están protegidas. Les urjo a todos que se aprovechen de los muy buenos recursos que New Jersey ofrece en este área."

Para asistir en estos retos de medidas de seguridad, el New Jersey Cybersecurity & Communications Integration Cell *(NJCCIC)* actúa como una tienda de una sola parada del estado para compartir información, analizar amenazas, y reportar incidentes. Localizado en el State Police Regional Operations Intelligence Center *(ROIC),* el *NJCCIC* trae juntos a analistas e ingenieros para promover educación por todo el estado de las amenazas de cibernética y las más amplias adaptaciones de las mejores prácticas.

"Nuestra misión es ayudar a hacer a NJ más resistente a ataques de cibernética. Animamos a los residentes de NJ y a los negocios que se pongan en contacto con NJCCIC para consejo, inscribirse a

nuestras alertas, y reportar incidentes a través de nuestro sitio web – www.cyber.nj.gov," dijo Michael Geraghty, Director del *NJCCIC*.

"Las estadísticas recopiladas presentan un panorama serio de los retos que nos enfrentamos cuando nos referimos a ciber-seguridad," dijo Sharon Joyce, Acting Director de la Division of Consumer Affairs. "Urgimos a los ciudadanos que usen los recursos disponibles a través de la Division of Consumer Affairs para que puedan protegerse a sí mismos y a su familia de robo de identidad y de otras formas de ciber-crimen. Además, la División está comprometida a proteger a los consumidores de aquellas compañías que no protegen o inapropiadamente recogen información personal."

La información presentada hoy por la Attorney General's Office y la State Police detallan las filtraciones en los datos en New Jersey que ocurrieron en el 2016. Las filtraciones de datos envuelven el acceso a información personal sin autorización, la cual puede incluir el nombre y apellido con el número de Seguro Social, el número de licencia de conducir, o de cuenta de banco, o de tarjetas de débito o crédito. Bajo la ley de New Jersey, cualquier negocio que opera en New Jersey o cualquier entidad pública que recogen o mantienen archivos computarizados que incluyen información personal tienen que comunicar cualquier filtración de seguridad a los clientes que son residentes de New Jersey y cuya información personal se cree que ha sido accedida por una persona sin autorización.

Los sectores de negocios que con más frecuencia están envueltos en filtraciones incluyen finanzas/ banca, servicios de cuidado de salud y comercio al por menor. Otras áreas incluyen educación, restaurantes, industrial/fábrica, hoteles, organizaciones sin fines de lucro, seguros que no son médicos, y telecomunicaciones, entre otros.

Los métodos usados para filtraciones de seguridad fueron *phishing,* una forma de fraude en la que el atacador intenta recoger información para acceder a la computadora o a la información de cuentas de banco disfrazado de una persona o entidad de buena reputación en un email, mensaje u otros canales de comunicación, y piratería. Website con programas maliciosos, incidente de empleado, acceso a emails sin autorización, y *ransomware*, también fueron utilizados.

La New Jersey Attorney General's Office, a través de la Division of Law y la Division of Consumer Affairs, ha tomado acción este año en los siguientes casos para proteger a los consumidores:

Vizio:

En Febrero 6, 2017, el Attorney General Christopher S. Porrino y la Division of Consumer Affairs anunciaron que Smart TV fabricante VIZIO, Inc. ("VIZIO") y sus sucursales VIZIO Inscape Services, LLC, ("Inscape") acordaron a pagar al Estado y a la Federal Trade Commission ("FTC") $2.5 millones y a cambiar sus prácticas de negocios para tratar las alegaciones de que violaron el New Jersey Consumer Fraud Act y el Federal Trade Commission Act por clandestinamente rastrear las costumbres de los televidentes y vender la información a las compañías de mercadeo y corredores de datos. En una junta Complaint puesta en United States District Court para el District of New Jersey, el Estado y la FTC alegaron que VIZIO e Inscape violaron las leyes estatales y federales por no efectivamente informar a los consumidores que las televisiones inteligentes VIZIO estaban continuamente coleccionando y guardando información acerca de lo que los consumidores veían en las teles, y que la información era vendida a partes terceras para propósito de mercadeo. Bajo los términos del acuerdo, VIZIO e Inscape pagaron al Estado $915,940 en multas civiles y $84,060 en pagos de abogados y costos de investigación. VIZIO e Inscape también acordaron a destruir la información que los consumidores habían visto antes de Marzo 1, del 2016, prominentemente diciéndoles a los consumidores que clase de data recogería la función "Smart Interactivity", obtener el claro

consentimiento de estos antes de colectar la información de lo que estaban viendo, e implementar y mantener un programa completo de privacidad.

Horizon:
En Febrero 17, del 2017, the NJ Division of Consumer Affairs anunció un acuerdo con Horizon Healthcare Services, Inc. (haciendo negocios como Horizon Blue Cross Blue Shield of New Jersey) para resolver reclamos bajo el New Jersey Consumer Fraud Act ("CFA") y el Health Insurance Portability Accountability Act federal, enmendado por el Health Information Technology For Economic and Clinical Health Act ("HIPAA/HITECH"). En una queja puesta en la United States District Court por el District of New Jersey, el Estado alega que Horizon violó el CFA y el HIPAA/HITECH por no proteger apropiadamente la privacidad de casi 690,000 de asegurados de New Jersey cuya información personal no encriptada estaba en dos computadoras portátiles robadas de las oficinas principales en Newark. Bajo los términos del acuerdo, Horizon acordó a pagar al Estado $1.1 millones e implementar un Corrective Action Plan.

Target:
En Mayo 23, 2017, el Attorney General Christopher S. Porrino anunció que Target Corp. ("Target") acordó a pagar a New Jersey, y a otros 46 estados y al District of Columbia un total de más de $18 millones para resolver una investigación de múltiples estados de una filtración de datos que comprometió la información de pago de más de 41 millones de compradores por toda la nación. New Jersey, el cual era un miembro del Executive Committee de los múltiples estados, recibió un pago total de $680,411 de Target. Además de los términos de dinero, Target acordó a implementar una variedad de reformas de ciber-seguridad designadas a prevenir semejantes filtraciones de datos en el futuro, incluyendo la creación de un Information Security Program.

El NJCCIC este mes lanzó una campaña por todo el estado:

"2FA for New Jersey" o "#2FA4NJ" – para promover educación de dos factores de autenticación (2FA). Desde asegurar las cuentas de emails, a herramientas de acceso remoto, y al banco en línea, 2FA es una sencilla pero práctica muy efectiva para proteger contra robo de identidad y reforzar la privacidad. Para más información, vaya al sitio web de NJCCIC: www.cyber.nj.gov. El sitio web permite a individuos que reporten directamente filtraciones de datos o incidentes de cibernética, y permite a los residentes a que se registren para recibir alertas, advertencias, boletines e información de entrenamiento

La Division of Consumer Affairs también se ha involucrado en lo siguiente para abordar al público:

- **Abordo a los consumidores** - La DCA's Cyber Fraud Unit protege los derechos de privacidad constitucionales de los consumidores de New Jersey en la era digital. La seguridad de datos y los datos de privacidad son las preocupaciones económicas y personales que más afectan a los consumidores de New Jersey. La Unidad implementa el New Jersey Consumer Fraud Act, el cual prohíbe ciertas prácticas de comercio, incluyendo rastrear las costumbres de los consumidores en línea, descargar malware en las computadoras de estos sin proveer aviso adecuado, y sin obtener consentimiento explícito de los consumidores. La Unidad también implementa el New Jersey Computer Related Offenses Act *(CROA),* el cual prohíbe, entre otras cosas, el intencionado o conocimiento y acceso sin autorización a los datos de los consumidores de New Jersey, a la base de datos, programa de computadora, software de computadora, o equipo de ésta; el federal Children's Online Privacy Protection Act de 1998 y las regularizaciones *(COPPA)*;

el New Jersey Identity Theft Protection Act; el Health Information Technology for Economic and Clinical Health Act *(HITECH)*; y el Health Insurance Portability and Accountability Act of 1996 *(HIPPA).* Los investigadores de la Unidad toman un papel activo en educar a los consumidores concerniendo como pueden proteger su información personal cuando usan las tecnologías del internet.

- **El abordo al público de las Juntas Profesionales** - La Junta de Contables. En respuesta a los reportes de esquemas de los emails *phishing* y otras invasiones en las computadoras enfocándose en los preparadores de impuestos, la Board of Accountancy (Junta de Contables) hizo un boletín para proveer recomendaciones a los proveedores de servicio de contabilidad que tratan información personal de identificación.

La Division of Consumer Affairs ofrece las siguientes sugerencias a los consumidores :

- Evite pulsar en los enlaces de emails o adjuntos de individuos que no conoce, instituciones financieras, servicio de computadoras o agencias del gobierno. Chequee el mensaje, vaya al sitio web legítimo público, y use la información de contacto proveída.

- Ajuste las configuraciones de privacidad del aparato para controlar la compartición de data entre aplicaciones, software y libro de direcciones.

- Escoja una contraseña fuerte que contenga letras, números y símbolos. Si el sitio web ofrece dos factores de identificación úselos.

- Para proteger su aparato de acceso sin autorización, y software malware, instale software de seguridad, con frecuencia disponible de su proveedor de internet, y asegúrese que su firewall y protección de anti-virus están actualizados constantemente.

- Antes de eliminar cualquier aparato electrónico, limpie el disco duro usando un software especializado que borrará su información; o dé el aparato a una facilidad de reciclaje certificada que sigue los estándares del gobierno para destruir data.

- Evite WiFi gratis, especialmente para servicio de salud, finanzas, y otras transacciones personales.

- Antes de dar su información personal para ganar un concurso o participar en una encuesta, lea los "Terms and Conditions" (Términos y Condiciones) y "Privacy Policy" (Política de Privacidad) dentro del sitio web o de la aplicación (app). Estas secciones pueden claramente decirle cómo se va a usar el sitio web y como se compartirá su información

- Bajo la ley federal, los consumidores pueden obtener tres reportes de crédito gratis una vez al año www.AnnualCreditReport.com. La ley de New Jersey permite que los consumidores obtengan tres reportes adicionales anualmente - uno por cada una de las tres agencia de reporte de crédito. Revisando con cuidado su reporte de crédito, expedientes del banco y sus extractos de tarjetas de crédito, y servicios de subscripciones, se puede parar a los ladrones de identidad personal en las primeras etapas.

- Los padres pueden reportar preocupaciones que tengan acerca de los sitios webs dedicados a los niños, directamente a la Division of Consumer Affairs, la cual implementa el federal Children's Online Privacy Protection Act *(COPPA)*. Los padres deben aprovecharse de la software de

control ofrecida por su proveedor de servicio de internet, ajustar las configuraciones del buscador para limitar el acceso de los niños, y revisar el historial del registro para monitorear el uso.

Recursos de ciber-seguridad:

- New Jersey Division of Consumer Affairs, Office of Consumer Protection, Cyber Fraud Unit
  https://www.njconsumeraffairs.gov/ocp/Pages/cyberfraud.aspx
- New Jersey Cybersecurity and Communications Integration Cell *(NJCCIC)*
  https://www.cyber.nj.gov
- New Jersey State Police Cyber Crimes Unit
  http://www.njsp.org/division/investigations/cyber-crimes.shtml
- Federal Trade Commission
  https://www.ftc.gov
- Federal Communications Commission Cyberplanner
  https://www.fcc.gov/cyberplanner
- U.S. Department of Health and Human Services - HIPAA for Professionals
  https://www.hhs.gov/hipaa/for-professionals/index.html
- United States Small Business Administration's "Cybersecurity for Small Businesses" training
  https://www.sba.gov/tools/sba-learning-center/training/cybersecurity-small-businesses
- American Institute of CPAs - Cybersecurity Resource Center
  https://www.aicpa.org/INTERESTAREAS/FRC/ASSURANCEADVISORYSERVICES/Pages/cyber-security-resource-center.aspx
- United States Computer Emergency Readiness Team
  https://www.us-cert.gov
- United States Department of Homeland Security, Cyber Security Division
  https://www.dhs.gov/science-and-technology/cyber-security-division
- National Cybersecurity and Communications Integration Center
  https://www.us-cert.gov/nccic
- Free Annual Credit Report Website Authorized by Federal Law
  https://www.annualcreditreport.com/index.action and 1-877-322-8228
- U.S. Department of Health and Human Services - HIPAA for Individuals
  www.hhs.gov/hipaa/for-individuals/index.html
- FDIC - A Bank Customer's Guide to Cybersecurity
  https://www.fdic.gov/consumers/consumer/news/cnwin16/

Siga la New Jersey Attorney General's Office en línea en Twitter, Facebook, Instagram & YouTube. Los enlaces a los medios sociales proveídos son por referencias solamente. La New Jersey Attorney General's Office no apoya o patrocina ningún sitio web, compañías o aplicaciones que no sean del gobierno.