Para su publicación inmediata: 17/02/2017 **GOBERNADOR ANDREW M. CUOMO**

EL GOBERNADOR CUOMO ADVIERTE SOBRE LAS NUEVAS Y AVANZADAS ESTAFAS EN LA TEMPORADA DE IMPUESTOS DIRIGIDAS A PREPARADORES DE IMPUESTOS Y PROFESIONALES DE RR. HH.

Al Menos 37 Empresas con Empleados de Nueva York que Fueron Víctimas de Ladrones de Identidad Comprometen a Más de 5.000 Números de Seguro Social

El gobernador Andrew M. Cuomo advirtió hoy a preparadores de impuestos y profesionales de recursos humanos sobre las nuevas estafas dirigidas a robar información confidencial sobre clientes y empleados, luego de que el Departamento de Impuestos del Estado de Nueva York identificara al menos a 37 empresas en la ciudad de Nueva York, la Región Capital, la región Central de Nueva York y la región Oeste de Nueva York que habían sido impactadas, afectando a miles de contribuyentes.

"A medida que la tecnología continúa avanzando, los ladrones y estafadores cibernéticos utilizan cada vez más métodos sofisticados para intentar robar información personal y estafar a los trabajadores neoyorquinos", **dijo el Gobernador Cuomo.** "Debemos tener tolerancia cero en estos casos y quiero animar a todos, especialmente a aquellos en estas áreas, a permanecer alerta y denunciar inmediatamente cualquier actividad sospechosa a las autoridades estatales y locales".

Nonie Manion, comisionada del Departamento de Impuestos y Finanzas del Estado de Nueva York, manifestó: "Ahora que estamos atravesando la temporada de declaraciones de impuestos, los criminales están ansiosos por presentar reclamaciones falsas para recibir devoluciones de impuestos utilizando información personal robada. Resulta de suma importancia que cualquiera que maneje la información personal de otra persona tenga presente las técnicas de fraude comunes a fin de evitar convertirse en víctimas".

El gobernador Cuomo advirtió a los neoyorquinos sobre varios fraudes que aparecieron esta temporada de impuestos, entre otros:

Los estafadores renuevan el esquema dirigiéndose a profesionales de nómina y RR. HH.
Los criminales cibernéticos que se hacen pasar por ejecutivos de empresas envían correos electrónicos a profesionales de nómina y RR. HH. solicitando listas de

empleados y su información personal. Esta vez, los estafadores expandieron su alcance a otras industrias, incluidos los distritos escolares, las organizaciones tribales y sin fines de lucro.

Estos correos electrónicos parecen legítimos porque contienen el nombre del director ejecutivo de la empresa. Sin embargo, si usted recibe un correo electrónico de estas características, no incluya datos de nómina, tales como los formularios W-2 y los números de Seguro Social, en una respuesta.

El Departamento de Impuestos tiene conocimiento de que al menos 37 empresas con empleados de Nueva York han caído en esta estafa y considera que involucra a más de 5.000 números de Seguro Social. El Departamento de Impuestos está en contacto con esas empresas y está trabajando con ellas para proteger a sus empleados.

Si usted es un empleador que ha sido víctima de esta estafa y, en respuesta, ofreció datos de nómina, tales como información sobre el W-2 y números de Seguro Social, consulte la Guía para empleadores afectados por una estafa de suplantación de identidad ("phishing") del W-2 para obtener instrucciones.

Esquema "spear-phishing" dirigido a preparadores de impuestos
Este esquema está presente en toda la comunidad de preparadores de impuestos. Compromete a estafadores que se presentan como Fastsupport.com u Onlyforsupport.com. Están contactando a preparadores de impuestos luego de haber identificado qué proveedor de datos electrónicos o Generador de Devoluciones Electrónicas (ERO, por sus siglas en inglés) autorizados por el IRS ha utilizado el preparador para transmitir las devoluciones.

La persona que llama, quien declara falsamente que trabaja en nombre del ERO, sugiere la necesidad de reinstalar o corregir problemas con el software del preparador. El estafador le pide al preparador que se conecte a su sitio web y comparta su contraseña y acceso a la computadora del preparador. Si el preparador accede, el estafador puede robar información sensible del cliente para cometer fraudes.

Un ERO es un proveedor de datos electrónicos autorizado por el IRS para presentar devoluciones de impuestos para su procesamiento.

Criminales cibernéticos se hacen pasar por clientes que solicitan servicios de agentes de impuestos
En un esquema de phishing a nivel nacional, los estafadores dirigen sus ataques a los agentes de impuestos para obtener su información y tramitar devoluciones fraudulentas. Estos estafadores suelen enviar a los agentes de impuestos dos correos electrónicos: en el primero, una solicitud de preparación de impuestos de un "cliente"; en el segundo, los estafadores ofrecen un enlace o adjuntan un PDF que contiene un enlace que les permite robar el correo electrónico y la contraseña del preparador de impuestos.

Si usted recibe un correo electrónico sospechoso, por ejemplo, de un destinatario desconocido, no seleccione ningún enlace ni abra ningún documento adjunto al correo electrónico. Este es el ingreso del estafador a su computadora, que lo expone a

software malicioso. Esto le podría permitir al criminal cibernético capturar información sensible sin que usted se dé cuenta de que está siendo comprometido.

Correo electrónico phishing con el asunto: "¡Correos en espera!" ("Mails on Hold!") dirigido a asesores de impuestos
Algunos asesores de impuestos han recibido correos electrónicos que aparentan ser del IRS o del equipo de servicios electrónicos del IRS con el asunto: "¡Correos en espera!" Estos correos electrónicos pueden incluir referencias al personal del IRS o PTIN, pero no son enviados por el IRS.

Si usted recibe un correo electrónico con este asunto, no seleccione ningún enlace ni abra los adjuntos que se incluyen en estos correos electrónicos. Nuevamente, esto podría ofrecer acceso a su computadora, exponiéndolo a software malicioso y haciendo vulnerable información privada.

Protéjase usted y a sus clientes
Los asesores de impuestos deben proteger la información personal de sus clientes ofreciéndola únicamente a fuentes de confianza tales como el IRS y el Departamento de Impuestos del Estado de Nueva York. Esto incluye destruir los documentos que contienen datos privados antes de desecharlos, y presentar las devoluciones de impuestos de los clientes oportunamente para reducir el plazo que un ladrón de identidad podría tener para reclamar devoluciones de impuestos fraudulentas utilizando su información.

El Departamento de Impuestos del Estado de Nueva York y el IRS nunca realizarán amenazas por teléfono ni le pedirán información fiscal o financiera por correo electrónico.

Denuncie
Si usted ha sido contactado por un estafador que se hizo pasar por un agente del IRS, debe contactar al IRS. Para conocer como denunciar el incidente, haga clic aquí.

Si usted ha sido contactado por un estafador que declara ser del Departamento de Impuestos del Estado de Nueva York, visite la página web para denunciar fraudes, estafas y robos de identidad del Departamento de Impuestos y conozca como denunciarlo. El Departamento de Impuestos revisa de inmediato cada denuncia y toma las medidas correctivas adecuadas.

###