De publicación inmediata: 22/03/2022 **GOBERNADORA KATHY HOCHUL**

LA GOBERNADORA HOCHUL ADVIERTE A LOS CONSUMIDORES SOBRE ESTAFAS Y AMENAZAS DE CIBERSEGURIDAD EN MEDIO DE LA INVASIÓN DE UCRANIA POR PARTE DE RUSIA

Done a organizaciones verificadas y reputadas que usan las contribuciones para brindar ayuda a los ucranianos que lo necesitan

Las agencias estatales emiten recomendaciones para proteger y asegurar su información confidencial y mantenerse alerta ante amenazas cibernéticas intensificadas

La gobernadora Kathy Hochul advirtió hoy a los neoyorquinos sobre las estafas de organizaciones benéficas y el aumento de las amenazas a la seguridad cibernética relacionadas con la invasión de Ucrania por parte de Vladimir Putin. La División de Protección al Consumidor del estado de Nueva York se enteró de solicitudes fraudulentas de dinero de ayuda caritativa para apoyar a las víctimas de la guerra. Se alienta a los consumidores a evaluar cuidadosamente cualquier solicitud de dinero y verificar las organizaciones benéficas antes de donar dinero o suministros. La gobernadora Hochul también alienta a los neoyorquinos a estar atentos cuando publican información confidencial en línea en medio de un aumento en las amenazas de seguridad cibernética mediante la utilización de las recomendaciones de seguridad del Departamento de Impuestos y Finanzas. Esto sigue a la formación de la Gobernadora del Centro de Operaciones Conjuntas de Seguridad (JSOC, por sus siglas en inglés), que sirve como centro para los esfuerzos cibernéticos conjuntos locales, estatales y federales.

"Nueva York es el hogar de la población ucraniana más grande de los Estados Unidos, y los neoyorquinos siempre ofrecen una mano para ayudar a los necesitados", **dijo la gobernadora Hochul.** "Sin embargo, debemos ser cautelosos con aquellos que intentan cometer fraude, aprovechándose de la bondad de los demás. En su generosidad para ayudar a nuestros amigos y familiares ucranianos, recuerde que si algo parece sospechoso, es probable que lo sea. Anime a sus amigos y familiares, especialmente a sus seres queridos mayores, para que estén alertas en línea".

Cada vez que ocurren desastres, los estafadores se aprovechan de la sensibilidad de las personas que quieren ayudar. La invasión de Ucrania brinda una oportunidad para

que los estafadores establezcan organizaciones benéficas falsas o se hagan pasar por víctimas de guerra convincentes. Otros diseñan sitios web para imitar el sitio oficial de una organización benéfica legítima a fin de robar el dinero o la información personal de los donantes desprevenidos.

El secretario de Estado, Robert J. Rodríguez, sostuvo: "Los neoyorquinos son conocidos por ser solidarios y generosos con los necesitados. Mientras la guerra en Ucrania continúe, los estafadores seguirán apareciendo usando tácticas emocionales y solicitudes falsas en un intento de estafar a los consumidores. Animo a los neoyorquinos a proteger sus buenas intenciones y a que siempre investiguen a las organizaciones benéficas antes de donar para asegurarse de que el dinero que tanto les costó ganar llegue a quienes necesitan su apoyo desesperadamente".

La comisionada interina de Impuestos y Finanzas, Amanda Hiller, dijo: "La crisis global en Ucrania intensificó la preocupación por los ataques cibernéticos, por lo que todos debemos estar atentos para evitar que la información confidencial caiga en las manos equivocadas, haya ataques de denegación de servicio y otras consecuencias negativas".

El director ejecutivo de la Oficina de Servicios de Tecnologías de la Información (ITS, por sus siglas en inglés), Angelo "Tony" Riddick, mencionó: "Innumerables neoyorquinos con las mejores intenciones han hecho donaciones a organizaciones benéficas para apoyar a las personas de Ucrania, y están marcando la diferencia. Desafortunadamente, esta generosidad también crea nuevas oportunidades para que exploten los ciberdelincuentes. Para protegerse y garantizar que su generosa donación siempre llegue a manos de aquellos que realmente necesitan ayuda, la ITS les pide a los neoyorquinos que sigan estas prácticas recomendadas y permanezcan atentos a las recientes amenazas en línea y estafas cibernéticas".

La comisionada de la Oficina de Seguridad Nacional y Servicios de Emergencia (DHSES, por sus siglas en inglés), Jackie Bray, dijo: "Cada neoyorquino tiene un papel que desempeñar cuando se trata de asegurar su información personal y protegerse de las amenazas cibernéticas. Sabemos que, en momentos de necesidad, los malos están buscando aprovecharse de aquellos que intentan ayudar. Si está tratando de apoyar a la gente de Ucrania a través de donaciones en línea o digitales, permanezca alerta y siga estas prácticas recomendadas para asegurarse de que sus donaciones sean auténticas y que su información permanezca segura".

El senador estatal Kevin Thomas señaló: "Habla mucho de nuestros vecinos que tantos neoyorquinos hayan tomado medidas para ayudar al pueblo ucraniano. Desafortunadamente, también creó una excelente oportunidad para que los estafadores exploten esta crisis para beneficio personal. Insto a los neoyorquinos permanecer alerta y a tomar precauciones adicionales para garantizar que sus generosas contribuciones se destinen a causas legítimas".

La asambleísta Nily Rozic indicó: "Los estafadores prueban nuevos métodos para engañarlo todo el tiempo, incluso durante una crisis internacional. Mientras los neoyorquinos se unen para apoyar a Ucrania en su momento de necesidad, es crucial que los consumidores cuenten con las habilidades y el conocimiento para garantizar que no se aprovechen de su generosidad. Agradezco a la gobernadora Hochul por garantizar que los neoyorquinos no sean estafados por su amabilidad".

Los estafadores suelen ponerse en contacto a través de las redes sociales, correos electrónicos no solicitados, llamadas telefónicas o mensajes de texto. Pueden solicitar que les envíen dinero a través de una aplicación de pago como Cash App, Venmo o Zelle, que les transfieran el dinero a una cuenta bancaria en el extranjero o enviar tarjetas de regalo prepagas. Muchas estafas recientes incluyen solicitudes de donaciones en criptomonedas, como Bitcoin o Ethereum. Los estafadores son creativos y seguirán pensando en nuevas formas de defraudar a las personas, por lo que los consumidores siempre deben estar atentos.

Para evitar que el dinero de las donaciones caiga en manos equivocadas, la División de Protección al Consumidor del estado de Nueva York recomienda tomar las siguientes precauciones:

- **Verificar la solicitud.** Los estafadores se hacen pasar por amigos, familiares o personas con intereses románticos con mayor frecuencia en las redes sociales y solicitan donaciones; es fácil copiar la foto y la información biográfica de otra persona y crear una cuenta falsa en línea. Si recibe una solicitud no solicitada de ayuda para una donación en línea, incluso si parece ser alguien que conoce, conéctese directamente con la persona a través de una vía de comunicación diferente para verificar la solicitud. No haga clic en ningún enlace ni complete formularios antes de verificar la fuente. Si la solicitud proviene de alguien que conoció recientemente en línea, lo más probable es que sea una estafa y debe tener especial cuidado.
- **Investigar a la organización benéfica.** No confíe solo en un sitio web de una organización benéfica. Antes de hacer una donación a cualquier organización benéfica, realice una búsqueda en línea utilizando el nombre del grupo y términos de búsqueda como "revisión" y "estafa". La Comisión Federal de Comercio recomienda consultar con give.org, charitynavigator.org,charitywatch.org o candid.org para ver informes y calificaciones de organizaciones benéficas. También puede consultar con el Servicio de Impuestos Internos (IRS, por sus siglas en inglés) para verificar si una organización benéfica está registrada. La Oficina de la Fiscalía General (OAG, por sus siglas en inglés) también recomienda revisar el Registro de organizaciones benéficas para obtener informes financieros antes de donar para asegurarse de que la organización benéfica sea fiscalmente sólida.
- **Resistir antes las tácticas de alta presión.** Si bien la situación es urgente, los consumidores deben resistirse a ser presionados para donar de inmediato. Con frecuencia, los estafadores lo presionan para que done de inmediato, lo que

hace que pase por alto las señales de alerta en su historia. Tenga cuidado con los correos electrónicos directos de "víctimas" y abogados que emplean historias desgarradoras, insistiendo en que done de inmediato. No done dinero por teléfono a vendedores telefónicos no solicitados; en su lugar, pídale a la persona que llama que le envíe materiales escritos sobre la organización benéfica y dónde donar, si así lo desea.

- **Mantener la información personal en privado.** Nunca proporcione su número de seguro social, número de tarjeta de crédito o tarjeta de débito u otra información de identificación personal en respuesta a una solicitud de una organización benéfica no solicitada. Si realiza una donación en línea, asegúrese de que su conexión a Internet sea segura antes de continuar con las solicitudes de donación.
- **Preguntar cómo se invertirá el dinero.** Los consumidores quieren saber que su dinero va directamente a las víctimas. Una organización benéfica genuina debería poder informarle qué parte de su donación irá directamente al programa en lugar de las tarifas administrativas.

- **Donar mediante cheque o tarjeta de crédito.** Nunca done dinero en efectivo, tarjetas de regalo, criptomonedas o cualquier otra moneda que sea difícil de rastrear. Haga su contribución mediante un cheque o una tarjeta de crédito para asegurarse de tener un registro de la donación. Haga los cheques a nombre de la organización benéfica, no de una persona. Si elige donar a través del sitio web de una organización benéfica, verifique que este sea seguro y que su computadora esté equipada con la última protección antivirus.

Si sospecha que se encontró con un intento fraudulento de recibir donaciones, puede presentar una queja ante la División de Protección al Consumidor del estado de Nueva York en https://dos.ny.gov/file-consumer-complaint.

La Línea Gratuita de Asistencia al Consumidor de la División está disponible de lunes a viernes (excepto en los feriados estatales) de 8:30 a. m. a 4:30 p. m. llamando al 1-800-697-1220. Para encontrar más información y consejos, siga a la División de Protección al Consumidor en las redes sociales en Twitter (@NYSConsumer) y Facebook (www.facebook.com/nysconsumer).

En medio de una mayor preocupación internacional sobre la seguridad cibernética, el Departamento de Impuestos y Finanzas del estado de Nueva York también comparte una serie de consejos críticos para ayudar a los contribuyentes a proteger su información privada durante la temporada de impuestos y durante todo el año:

Tener cuidado con los correos electrónicos no solicitados y las llamadas telefónicas que solicitan información personal. Nunca comparta información personal, como su número de seguro social, en respuesta a un correo electrónico o una llamada telefónica no solicitada. Si el correo electrónico o la llamada dicen ser de una empresa con la que hace negocios, llámelos directamente para confirmar que el

contacto sea legítimo. Los estafadores suelen usar tácticas de miedo y amenazas relacionadas con la deuda tributaria para que comparta su información personal y financiera.

Proteger los dispositivos móviles. Aplique actualizaciones de software que corrijan las vulnerabilidades conocidas tan pronto como estén disponibles. Use funciones de seguridad integradas en su dispositivo, como un código de acceso, y use programas que encripten datos y eliminen contenido de forma remota si el dispositivo se pierde o lo roban.

Tener cuidado con los puntos de acceso a redes wifi. Los puntos de acceso inalámbricos públicos no son seguros, lo que significa que es fácil para los ladrones cibernéticos ver lo que está haciendo en su dispositivo móvil mientras está conectado. Limite lo que hace cuando usa redes wifi públicas y evite iniciar sesión en cuentas confidenciales.

Conocer las aplicaciones. Revise detenidamente los detalles y las especificaciones de una aplicación antes de descargarla. Revise y comprenda la política de privacidad de cada aplicación móvil. Tenga en cuenta que la aplicación puede solicitar acceso a su ubicación e información personal.

Tener cuidado con la información que se comparte en las redes sociales. Evite publicar su fecha de nacimiento, número de teléfono, domicilio o imágenes que identifiquen su trabajo o pasatiempos. Una razón: este tipo de información se puede usar para determinar las respuestas a las preguntas de seguridad que se usan para restablecer las contraseñas y lo convierte en un objetivo de los estafadores que quieren acceder a sus cuentas e información personal.

Usar contraseñas seguras. Cree contraseñas distintas para todas sus cuentas. Cuando se trata de contraseñas, trate de usar una con al menos 14 caracteres, el estándar actual de la industria. Use una combinación de letras (mayúsculas y minúsculas), números y símbolos. Considere frases de contraseña en las que use las primeras letras de una frase memorable para crear una contraseña compleja que sea difícil de adivinar. Cambie regularmente sus contraseñas y frases de contraseña.

Variar las preguntas de seguridad. No utilice las mismas preguntas de seguridad en varias cuentas. Seleccione preguntas de seguridad cuyas respuestas no se puedan adivinar o encontrar buscando en las redes sociales o en Internet.

Utilizar la verificación en dos pasos para acceder a las cuentas. Para mejorar la seguridad de las cuentas en línea, siempre que sea posible solicite una contraseña y un código de seguridad adicional para verificar su identidad cuando inicie sesión.

Tener cuidado con el *phishing*. No haga clic en enlaces, no descargue archivos y no abra archivos adjuntos en correos electrónicos de remitentes desconocidos. Abra los

archivos adjuntos solo cuando los esté esperando y sepa lo que contienen, incluso si conoce al remitente.

Es importante revisar periódicamente los pasos necesarios para proteger su información confidencial.

Denunciar. Si es víctima o cree que puede ser víctima de un robo de identidad relacionado con los impuestos, infórmenos de inmediato. Haremos un seguimiento de su información para ayudar a mantenerla privada y protegida. Visite la página web Informe sobre fraudes, estafas y robo de identidad del Departamento de Impuestos.

El Departamento de Impuestos utiliza encriptación avanzada, *firewalls*, sistemas de detección de intrusos y otras medidas de seguridad para proteger nuestros sistemas y datos confidenciales, pero los contribuyentes también deben adoptar un enfoque proactivo para protegerse en línea.

###