



Para publicación inmediata: 11/24/2015

GOBERNADOR ANDREW M. CUOMO

ALERTA EL GOBERNADOR CUOMO A NEOYORQUINOS CONTRA ESTAFAS DURANTE LA TEMPORADA DE COMPRAS PARA LAS FIESTAS

El Gobernador Andrew M. Cuomo instó hoy a los neoyorquinos a protegerse contra el robo de identidad y a estar alerta contra las estafas en Viernes Negro (Black Friday), Ciberlunes (Cyber Monday) y durante toda la temporada de compras para las fiestas.

“Esta época de dar infortunadamente es vista por los ciberladrones y estafadores como una excelente oportunidad para aprovecharse de compradores incautos”, **dijo el Gobernador Cuomo**. “Animo a todos los neoyorquinos a mantenerse alerta y extremar precauciones al hacer sus compras en esta época de fiestas para evitar convertirse en víctimas de estas prácticas inmorales”.

El Viernes Negro y el Ciberlunes marcan el arranque oficial de la temporada de compras para las fiestas. Aunque estos días deben ser oportunidades para lograr gangas, también son una temporada activa para los estafadores. Los defraudadores se aprovechan de la temporada de compras para las fiestas para estafar a los consumidores y robarles su dinero y su identidad.

El Secretario de estado de New York Cesar A. Perales dijo: “El robo de identidad y otros tipos de estafas sin escrúpulos son más comunes en esta época del año, y estos consejos y lineamientos ayudarán a hacer que esta temporada festiva sea menos estresante y más gratificante para los neoyorquinos. Queremos concientizar a los neoyorquinos de sus derechos como consumidores y darles valiosos consejos para que puedan tomar precauciones contra los estafadores que utilizan la época festiva como una oportunidad para robarles su dinero”.

Margaret Miller, directora de Informática del Estado de New York, dijo: “La tecnología de hoy hace que las compras en línea sean increíblemente convenientes, con sólo oprimir el botón del mouse o deslizar el dedo en la pantalla. Aunque estas tecnologías hacen que las transacciones sean mucho más fáciles para el consumidor, también vuelven el cibercrimen mucho más fácil para un “hacker”. Los neoyorquinos deben extremar precauciones al conectarse a internet en esta época festiva, y aprovechar estos consejos para protegerse”.

Ted Potrikus, presidente y director general del Consejo de Venta al Detalle del Estado de New York dijo: “Las tiendas al detalle de New York, grandes y pequeñas, están listas para dar servicio a los compradores, desde las calles principales a los centros comerciales y a sus sitios web, con excelentes productos, precios y servicios. Asegúrense de comprar a comerciantes en los que confíen, conserven sus recibos por si necesitan hacer una devolución, ¡y no duden en consultar a un empleado de la tienda si tienen cualquier pregunta! ¡Esperamos verlos en las excelentes tiendas que hay en cada rincón del Estado de New York!”.

De acuerdo con la Comisión Federal de Comercio, los consumidores a nivel nacional reportaron más de \$1.7 mil millones en pérdidas por fraudes y robo de identidades en 2014. El Centro de Denuncias para Crímenes por Internet del Buró Federal de Investigaciones recibió reportes de más de 14,000 neoyorquinos en 2014, que denunciaron más de \$47 millones en pérdidas por cibercrimes. En el Estado de New York los consumidores presentaron más de 3,000 denuncias por robo de identidad durante la temporada festiva del año pasado, de noviembre de 2014 a enero de 2015. La línea de ayuda de la División de Protección al Consumidor también recibe cientos de llamadas durante la temporada festiva de consumidores que piden ayuda para evitar volverse víctimas de una estafa.

A través de su Unidad de Asistencia al Consumidor, la División recibe las denuncias de los consumidores, intenta mediar cuando es apropiado y deriva las denuncias a la agencia federal, estatal o local que esté facultada por la ley para tomar las acciones apropiadas. Entre otras cosas, la Unidad de Asistencia al Consumidor media y resuelve denuncias relacionadas con reembolsos y devoluciones de productos, disputas relacionadas con tarjetas de crédito y mitigación del robo de identidad. Para maximizar sus posibilidades de aprovechar excelentes ofertas y minimizar el riesgo de estafas y robo de identidad, los consumidores deben hacer sus compras con tiendas reconocidas y practicar hábitos seguros en línea. La División de Protección al Consumidor del Estado de New York y la Oficina de Servicios de Tecnologías de la Información del Estado de New York ofrecen los siguientes consejos:

Investigue.

- **Sólo haga compras con comerciantes y sitios web que conozca y en los que confíe.** No visite un sitio haciendo clic en un enlace que le llegó por correo electrónico, que encontró en un blog o que vio en un anuncio. Podría llegar a un sitio web que sea igual al verdadero, pero que sea un duplicado bien hecho. Si tiene dudas sobre la legitimidad o seguridad de una tienda o de un sitio web, es mejor no arriesgarse.
- **Cuídese de los anuncios engañosos.** Asegúrese de que entiende la oferta y de leer la letra pequeña. No confíe en gangas extraordinarias a menos que se asegure de que son legítimas poniéndose en contacto con el comerciante y haciéndole preguntas antes de hacer una compra.
- **Piénselo dos veces antes de hacer clic en enlaces que lleguen por correo electrónico o en anuncios emergentes.** Cuando reciba ofertas no solicitadas por correo electrónico o aparezcan anuncios emergentes que parezcan de

tiendas legítimas, tenga mucha cautela respecto a su origen. Además de la posibilidad de que contengan un virus, estos anuncios pueden ser estafas para robarle su dinero o venderle productos de imitación..

- **Lea las políticas de reembolsos, tiempos de entrega y manejo/envío de la tienda.** Antes de hacer cualquier compra, pregunte por las políticas de la tienda. Verifique en qué condición deben estar las mercancías para poder devolverlas y si la tienda cobra una cuota por reposición.
- **Esté alerta de posibles estafas con donativos para caridad.** Piénselo bien antes de hacer clic en correos electrónicos que pidan donativos. Haga su contribución visitando el sitio web de confianza de la organización caritativa, nunca a través de un enlace en un correo electrónico.

Proteja su información de identificación personal.

- **Proteja su computadora y sus dispositivos móviles.** [Mantenga actualizados sus programas antivirus y antispyware, así como su cortafuegos.](#) Tenga cuidado con las descargas gratuitas; lo barato puede salir caro. Los protectores de pantalla, tarjetas electrónicas y otras descargas gratuitas de la temporada pueden tener virus.
 - **No use redes inalámbricas públicas para trámites bancarios o compras en línea.** Su información personal nunca debe ser transmitida a través de conexiones inalámbricas inseguras en espacios públicos.
 - **Proteja la red inalámbrica Wi-Fi de su casa.** Asegúrese de controlar quién tiene acceso como administrador, y que todos los usuarios de su red inicien sesión con una contraseña sólida. La configuración de cifrado debe estar habilitada y ser fuerte.
 - **Proteja sus compras.** Busque las letras “https” al principio de la dirección de internet. La “s” es de seguro, e indica que la comunicación con la página web está cifrada, protegiendo así su información.
 - **Tome precauciones con las contraseñas que use para sus cuentas en línea.** Utilice contraseñas diferentes para sus diferentes cuentas en línea, especialmente para la que están vinculadas con su información financiera. Genere contraseñas largas y complejas que incluyan letras mayúsculas y minúsculas, caracteres especiales y números. Por lo general se recomienda una contraseña con al menos 10 caracteres. Piense en cambiar sus contraseñas cuando termine la temporada de compras para las fiestas. Asegúrese de cerrar la sesión en un sitio web después de terminar su transacción en línea.
 - **Evite las ofertas no solicitadas.** Al comprar en línea, escriba el nombre del sitio que desea visitar en lugar de hacer clic en ofertas que lleguen por correo electrónico o que aparezcan en anuncios emergentes, dado que estos presentan el riesgo de robo de identidad y fraude.
- Si un correo electrónico le pide su información personal o financiera, es muy probable que sea una estafa.**

- **No responda a correos electrónicos no solicitados que le pidan su contraseña, su NIP u otra información delicada por correo electrónico.** Una organización legítima nunca iniciará el contacto con usted por redes sociales o correo electrónico, ni le pedirá información personal o financiera. Si el correo

electrónico parece ser de su banco o de su compañía de tarjetas de crédito, comuníquese directamente con ellos.

- **Pague con tarjeta de crédito.** Al comprar en línea o en una tienda, asegúrese de usar una tarjeta de crédito y no de débito. Las tarjetas de crédito están cubiertas por la Ley de Facturación Justa de Crédito, que le da mayores protecciones contra cargos fraudulentos y le permite impugnar con más facilidad un artículo en su estado de cuenta si es que no lo recibe. Piense en utilizar una tarjeta de crédito exclusivamente para sus compras en línea, para que sólo una tarjeta se vea afectada si la tienda en línea o la procesadora de tarjetas de crédito sufre una fuga de datos. Si paga en efectivo, conserve sus recibos.

Lleve registros.

- **Tenga un archivo.** Guarde los registros de sus transacciones en línea, incluyendo la descripción del producto, el precio, las condiciones, las garantías, el recibo electrónico y los correos electrónicos enviados y recibidos del comerciante.
- **Esté alerta a cargos pequeños en sus estados de cuenta.** Los “hackers” usan cargos pequeños como pruebas de validación. Cualquier cargo desconocido podría ser una señal de que la tarjeta ha sido comprometida.

Actúe si cree que ha sido víctima de un ciberdelito.

- **Comuníquese con sus instituciones financieras.** Notifique inmediatamente a su banco, a su compañía de tarjetas de crédito y a cualquier otro lugar en el que tenga cuentas y notifíqueles que alguien podría estar utilizando su cuenta de manera fraudulenta.
- **Cambie sus contraseñas.** Si ha sido atacado por “hackers”, es posible que hayan robado las contraseñas de sus otras cuentas. Cambie primero las contraseñas de sus cuentas críticas, empezando por su cuenta de correo electrónico y siguiendo con sus cuentas financieras y otras cuentas críticas. Es importante comenzar con las cuentas de correo electrónico, ya que generalmente el cambio de contraseña de sus demás cuentas se envía a su correo electrónico.
- **Suspenda sus cuentas de crédito.** Comuníquese con los tres principales burós de crédito, Experian, Equifax y TransUnion, y solicite un reporte de crédito y la colocación de una alerta de fraude y una suspensión de crédito en su cuenta.
- **Comuníquese con su departamento de policía local.** Presente una denuncia para que haya un registro oficial del incidente.

Para más información, o para presentar una denuncia contra un negocio, visite el sitio web de la División de Protección al Consumidor del Departamento de Estado de New York en <http://www.dos.ny.gov/consumerprotection/> o póngase en contacto con la línea de ayuda de la División al (800) 697-1220. La línea de ayuda al consumidor está abierta de lunes a viernes, excepto por los días feriados federales, de 8:30 a.m. a 4:30 p.m.

Siga a la División de Protección al Consumidor en redes sociales en Twitter [@NYSConsumer](#) y [Facebook](#)

Para ver más consejos sobre seguridad en línea, incluyendo alertas en tiempo real sobre riesgos emergentes, consejos diarios y mucho material informativo de fácil comprensión, visite la Oficina de Servicios de Tecnologías de la Información en línea en <http://www.its.ny.gov/>

Siga a la Oficina de Servicios de Tecnologías de la Información en Twitter [@NYStateCIO](#) y [Facebook](#)

###

Noticias adicionales disponibles en www.governor.ny.gov
Estado de New York | Executive Chamber | press.office@exec.ny.gov | 518.474.8418