Fiscal General de Nueva York
Letitia James

Estimados neoyorquinos:

Su identidad está en riesgo. Por internet, por teléfono, e incluso en persona, para los estafadores es más fácil que nunca robarse su información personal y usarla para cometer fraudes.

El robo de identidad afecta a millones de personas cada año. Los estafadores solicitan tarjetas de crédito en su nombre, reciben sus beneficios médicos, e incluso usan su número del seguro social para cometer fraudes tributarios, lo que daña su calificación crediticia y le cuesta tiempo y dinero para arreglarlo.

Puede proteger su información personal y prevenir la mayoría de los tipos de robo de identidad con un poco de diligencia, y estamos listos para explicarle cómo hacerlo.

Para ver más información sobre cómo mantener segura su identidad, o qué hacer si cree que alguien ha robado su identidad, visite nuestro sitio de internet en ag.ny.gov.

Atentamente,

Letitia James

Recursos

Oficina de Fraudes al Consumidor, Oficina de la Fiscal General del Estado de New York

Report scams or file a complaint.

(800) 771-7755 / ag.ny.gov

Comisión Federal de Comercio de EE. UU.

Denuncie las estafas y el robo de identidad.

877- 382-4357 / ftc.gov

Informes crediticios anuales

Para consultar o congelar sus informes de crédito.

877-322-8228 / annualcreditreport.com

Principales agencias de informes crediticios

Experian:
(888) 397-3742 / experian.com

TransUnion:
(800) 888-4213 / transunion.com

Equifax
(800) 685-1111 / equifax.com

Innovis
innovis.com

Proteja su identidad

Consejos para mantener su identidad a salvo

Oficina de la Fiscal General del estado de Nueva York
Letitia James

Proteja su información personal

Aunque por lo general es seguro proporcionar su nombre o su número de teléfono, decirle a alguien su fecha de nacimiento, número de seguro social o cualquier número de cuenta puede exponerlo al robo de identidad. También debe abstenerse de divulgar cualquier información que use con respuesta de "respaldo" en caso de olvidar su contraseña de un sitio de internet.

Nunca le proporcione su información personal a alguien que lo contacte al azar: a menos que usted sea quien se comunicó, existe la posibilidad de que se trate de un intento de phishing.

El "phishing" es un intento de lograr que la víctima proporcione información personal, como su nombre de usuario, contraseña o número de tarjeta de crédito. Los estafadores pueden comunicarse con usted por mensaje de texto, teléfono o correo electrónico, y con frecuencia se hacen pasar por representantes de una agencia gubernamental, un banco o una compañía reconocida. Le exigirán su información personal para resolver algún problema o emergencia, o le dirán que solo necesitan "confirmar su información" antes de que puedan darle algo.

Ninguna de esas organizaciones se comunicaría de esa manera para algo importante. Si tiene alguna duda llame a la compañía, a sus números publicados, para confirmar si se trata de ellos. Algunos intentos de phishing le dirán que vaya a un sitio de internet o que abra un archivo adjunto. ***No descargue archivos adjuntos ni haga clic en enlaces de personas que no conoce.*** Pueden contener virus que infecten su computadora y roben su información personal.

Mensajes sospechosos

Incluso si un mensaje parece provenir de una fuente de confianza, como un familiar o una compañía reconocida, podría ser un intento de phishing: los estafadores podrían haber tomado el control de la cuenta, o haber creado una cuenta nueva con un nombre similar. Si recibe un mensaje que no suena como algo que escribiría el remitente, que contiene solamente un enlace o un archivo adjunto sin explicación alguna, o que le parece sospechoso por cualquier otro motivo, revise cuidadosamente el campo "De:" para asegurarse de que es de la dirección correcta, o llame al remitente para verificar que realmente proviene de él. Esto puede ocurrir en redes sociales con la misma facilidad que por correo electrónico o mensaje de texto, así que no confíe en un mensaje sospechoso solamente porque proviene de un "amigo".

Número de seguro social

Una compañía muy rara vez necesita pedirle su número del seguro social. Si lo hacen, pregunte para qué lo necesitan, especialmente si no se trata de una agencia gubernamental, un empleador, un banco o una institución financiera. ***Y, de nuevo, nunca se lo dé a alguien que lo contacte sin previo aviso.***

Use un cortafuegos, actualice su sistema operativo

Navegar por internet puede exponer a su computadora a virus. Mantenga su sistema operativo y su programa antivirus actualizados, y tenga activo su cortafuegos para mantenerse seguro.

Elija contraseñas fuertes

Si usa internet, necesitará contraseñas fuertes, y necesitará varias de ellas. Una contraseña fuerte cumple los siguientes criterios:

- Es larga. Debe tener por lo menos ocho caracteres, pero mientras más, mejor.
- No puede ser adivinada por alguien que lo investigue, así que no use fechas de nacimiento o nombres de familiares.
- Es algo que usted puede recordar. Puede ser útil combinar palabras largas y poco comunes ("bateriaengrapadora").
- Solamente se usa una vez. Si repite una contraseña y alguien la averigua una vez, puede obtener acceso a todas sus cuentas.

Administradores de contraseñas

Los navegadores modernos tienen "administradores de contraseñas" que pueden recordar sus contraseñas por usted: solamente descargue un administrador y todo lo demás se hace automáticamente. Mantenga la contraseña de su administrador lo más segura posible: si un estafador obtiene acceso a ella, podrá obtener acceso a todas sus cuentas.

Proteja sus dispositivos con contraseña

Trate los teléfonos celulares y las cuentas de computadora igual que las cuentas de un sitio de internet: asígneles contraseñas únicas y fuertes.

Contraseñas predefinidas

Algunos dispositivos, como su enrutador o módem, tienen una contraseña predefinida. Las contraseñas predefinidas casi nunca son seguras, así que debe cambiarlas de inmediato.

Cambie sus contraseñas con regularidad

Incluso si sigue este consejo, mientras más tiempo usa una contraseña, más probable será que alguien malintencionado la consiga: la seguridad de los sitios de internet puede ser vulnerada. Siempre cambie una contraseña si el sitio de internet correspondiente es vulnerado, y cambie las contraseñas con regularidad para mantenerse seguro.

Proteja sus conexiones

Un sitio de internet o red Wi-Fi con poca seguridad puede exponer su información personal. Nunca realice transacciones personales o financieras en una red pública, y asegúrese de que un sitio de internet es "seguro" antes de darle información delicada. Los sitios de internet seguros comenzarán con **"https://"** en lugar de **"http://"**

Borre la información innecesaria

Destruya todos los registros de información personal cuando ya no los necesite. Triture los documentos físicos como recibos, declaraciones de impuestos y registros financieros o médicos; borre o desactive las cuentas digitales y borre los archivos digitales. Recuerde que incluso los archivos borrados pueden seguir en su disco duro, así que necesitará software de seguridad especial para borrar toda su información personal si se deshace de una computadora vieja.

Revise sus estados de cuenta

Revise cuidadosamente los estados de cuenta de sus tarjetas de crédito y cuentas bancarias para detectar actividades que usted no autorizó.

Revise cuidadosamente sus facturas médicas y su seguro de salud para asegurarse de que recibió los tratamientos descritos.

Informes crediticios

Todos tenemos derecho a recibir una copia gratuita al año de nuestro informe crediticio de cada una de las principales agencias de informes crediticios. Si ve cuentas o consultas que usted no inició o que no reconoce, podría significar que alguien más está usando su identidad. Puede solicitar informes de diferentes agencias en diferentes épocas del año para obtener una cobertura regular en annualcreditreport.com o llamando al (877) 322-8228.

Robo de identidad de niños

Las identidades de los niños son las robadas con más frecuencia, en ocasiones por familiares con malas calificaciones crediticias. Proteja la información personal de sus hijos como protegería la de usted. Recuerde hacer preguntas y actuar de inmediato si sus hijos reciben llamadas de cobranza u ofertas de crédito en su nombre, si les niegan beneficios porque alguien más está usando su número, o si recibe avisos del IRS sobre impuestos vencidos.