Estimados neoyorquinos:

En línea, en el correo, incluso en persona — su identidad puede estar en riesgo.

El robo de identidad afecta a millones de personas cada año. Los estafadores adquieren nuestras historias de crédito, obtienen beneficios médicos, incluso usan nuestros números de seguro social para un empleo.

Es importante tomar medidas para proteger su información personal, al igual que proteger a sus seres queridos y propiedad personal. No comparta su información con extraños, colóquela bajo llave en casa y protéjala en línea con contraseñas seguras. Evite llevar información con usted cuando salga de su casa.

Para averiguar más acerca de cómo mantener segura su identidad o qué debe hacer si cree que su identidad ha sido robada, vaya a nuestro sitio web: www.ag.ny.gov.

Atentamente.

Letitia James

Letitia James

Fiscal General del Estado de Nueva York
The State Capitol
Albany, New York 12224
1-800-771-7755
www.ag.ny.gov

Recursos

Oficina del Fiscal General de la Oficina del Estado de Nueva York
Oficina de investigación de fraudes del consumidor (Consumer Frauds Bureau)
800-771-7755
www.ag.ny.gov

Informes de crédito anual
www.annualcreditreport.com
877-322-8228

Agencias de elaboración de informes de crédito principales
Experian
888-397-3742
www.experian.com
TransUnion:
800-888-4213
www.transunion.com
Equifax
800-685-1111
www.equifax.com
Innovis
www.innovis.com/InnovisWeb/

Comisión de comercio federal de EE. UU. (U.S. Federal Trade Commission)
877-382-4357
www.ftc.gov

PROTEJA SU IDENTIDAD

Identity Protection: Spanish

OFICINA DEL ESTADO DE NUEVA YORK
del
FISCAL GENERAL

MANTENGA SEGURA SU IDENTIDAD

Asegure su información personal

Cierta "información de identificación personal" como los números de seguro social, fechas de nacimiento y números de cuenta pueden dar a los ladrones de identidad lo que necesitan para obtener una tarjeta de crédito, un empleo e incluso beneficios médicos en su nombre. Es por eso que es importante proteger esta información cuidadosamente.

Llamadas y correo no solicitados

Nunca dé su información personal a alguien que se ponga en contacto con usted sin haberlo solicitado. Independientemente de si ellos llaman, le envían un correo electrónico o se acercan a usted en persona, no dé su información personal a personas que no conoce o con quienes no se puso en contacto.

No sea víctima de un "engaño cibernético"

Un engaño cibernético (Phishing) es un intento para hacer que una víctima dé su información personal como su nombre de usuario, contraseña o número de tarjeta de crédito. Los estafadores enviarán mensajes de texto, correo electrónico o llamarán, identificándose como su banco o una agencia del gobierno. Ellos le dirán que necesitan "confirmar su información" para "verificar su cuenta".

Las instituciones financieras legítimas no se comunicarán con usted para obtener información importante. Si no está seguro, llame al banco por medio de números publicados, para verificar si en realidad necesitan su información. No haga clic en vínculos incluidos en correos electrónicos de personas que no conoce.

Número de Seguro Social

Agencias gubernamentales, empleadores, instituciones bancarias o financieras — hay un número limitado de instituciones que requieren su número de seguro social. Pregunte por qué lo necesitan. **Y, una vez más, nunca lo dé a alguien que se ponga en contacto con usted sin haberlo solicitado.**

Limite lo que lleva con usted

Es mejor mantener los documentos como sus tarjetas de seguro social en casa en un lugar seguro. Lleve con usted solo las tarjetas de crédito y bancarias que necesita.

Cree contraseñas seguras

Si usa Internet, necesita contraseñas seguras y necesitará varias. Una contraseña segura es una que:

- no se puede adivinar fácilmente (por ejemplo su cumpleaños, el nombre de un ser querido, el nombre de una mascota);
- tiene múltiples formas de caracteres (números, letras mayúsculas y minúsculas, símbolos);
- tiene al menos 8 dígitos de longitud;
- es diferente de sus otras contraseñas.

Use contraseñas en:

- Redes de internet inalámbricas: Ponga una contraseña a sus propias redes; evite realizar negocios personales y financieros en redes públicas.
- Cada computadora individual y cada cuenta en la computadora deben estar protegidas con una contraseña.
- Correo electrónico: Si usa su correo electrónico para comprar, pagar facturas o realizar transacciones bancarias, existe mucha información personal que se puede acceder con el clic de un botón.
- Teléfonos inteligentes: Estos son ventanas portátiles a su mundo. Use una contraseña segura, en caso de que se pierda, se lo roben o incluso lo preste alguien que ande merodeando.

Use sitios web seguros

Los sitios web seguros "cifran" la información cuando la envían.

Si usted transmite información personal o financiera, observe estas señales:

- **S para Seguro:** Busque una "S" al principio del nombre del sitio. Un sitio seguro empezará con https://.
- **Certificado de seguridad:** Muchos navegadores usan el icono de un candado, otros usarán el nombre del sitio resaltado en color antes de la URL (el nombre del sitio en el que ha iniciado sesión). Cuando hace clic en este, le indicará el nombre del propietario del certificado, el cual debe ser igual que el del sitio en el que se encuentra.

Destruya registros innecesarios

Destruya documentos importantes antes de tirarlos, incluyendo cualquier registro que contenga información de identificación personal como registros médicos y financieros, recibos, declaraciones de impuestos, incluso solicitudes de tarjetas de crédito.

Supervise los estados de cuenta

- Revise cuidadosamente los estados de cuenta del banco y de la tarjeta de crédito en relación con cualquier actividad que usted no haya autorizado.
- Facturas médicas y seguro médico — revíselos cuidadosamente para asegurarse de que en realidad recibió el tratamiento descrito.

Informes de crédito

Cada persona tiene derecho a recibir una copia gratuita de su informe de crédito cada año, de cada una de las agencias de elaboración de informes de crédito. Si observa cuentas o consultas que usted no inició o no reconoce, esto podría indicar que alguien más está usando su identidad. Solicite un informe de cada una de las principales agencias de elaboración de informes de crédito. Puede programarlas en diferentes momentos del año. www.annualcreditreport.com o 877-322-8228.

Robo de identidad infantil

Las identidades de los niños son las que se roban con más frecuencia, algunas veces por parte de miembros de la familia que tienen malas calificaciones de crédito. Proteja la información personal de sus hijos como lo haría con la suya. Asegúrese de hacer preguntas y tomar medidas si reciben llamadas de cobro de facturas u ofertas de crédito a su nombre, se les niegan beneficios porque alguien más está usando su número o reciben avisos de IRS sobre impuestos vencidos.