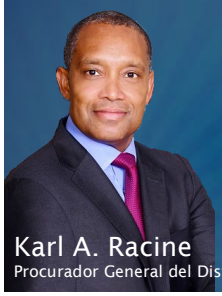

Karl A. Racine
Procurador General del Distrito de Columbia

Procuraduria General Alerta al consumidor: Protección de datos y privacidad

Muy a menudo, nos enteramos de que vendedores, bancos o profesionales médicos sufrieron una "filtración de datos" que compromete nuestra información personal. Es posible que haya recibido una carta donde se le notifica que un hacker robó su número de Seguro Social, número de cuenta de tarjeta de crédito o fecha de nacimiento.

Desafortunadamente, los consumidores que fueron objeto del robo de información sensible corren un mayor riesgo de sufrir robo de identidad, fraude u otras estafas como el "phishing" (fraude mediante correo electrónico), donde el estafador se hace pasar por un remitente de confianza. Puede proteger su privacidad en línea e información personal poniendo en práctica hábitos seguros en Internet y reconociendo situaciones en las que puede exponer su información personal a estafadores. Si roban su identidad, hay pasos que puede seguir para minimizar cualquier daño a su crédito o reputación.

¿Cuáles son algunas de las estafas en línea que debo conocer?

El fraude con subastas en línea representa tres cuartos de todas las quejas registradas ante el Centro de Quejas por Crímenes en Internet del FBI. Hay diferentes tipos de fraudes con subastas en línea, pero por mucho la más común es pagar por bienes que nunca recibió. Esté pendiente de las ofertas que parecen muy buenas como para ser verdaderas.

Recibe un correo electrónico que pareciera venir de su banco, en el que se le advierte sobre el robo de su identidad y le piden que inicie sesión y verifique la información de su cuenta. Es probable que esto sea "phishing", donde un estafador se hace pasar por un remitente de confianza que solicita la verificación de su información personal, como su número de Seguro Social, contraseña o PIN. Estos correos electrónicos son fraudulentos, ya que los negocios legítimos no solicitarán esta información por correo electrónico. Los estafadores electrónicos que tengan éxito pueden utilizar su información para acceder a sus cuentas o suplantarlo en línea, lo cual puede resultar en un daño importante para su crédito y en pérdidas financieras.

Las estafas con el "IRS" (Servicio de Impuestos Internos) se están haciendo más comunes, particularmente entre las personas que presentan su declaración de impuestos de manera electrónica. Puede recibir un correo electrónico que pareciera ser del IRS donde le piden que "actualice su presentación electrónica del IRS" y que haga clic en un enlace en el correo electrónico. O, su contador recibe un correo electrónico donde se le solicita que actualice la información de presentación electrónica de sus clientes. Estas estafas están diseñadas para obtener los nombres de usuario, las contraseñas y la información de identificación de las personas que declaran en línea, de tal modo que los ladrones puedan presentar declaraciones falsas y robar su reembolso de impuestos.

La carta "nigeriana" involucra a alguien que se hace pasar por un ciudadano extranjero que necesita ayuda para transferir dinero y ofrece pagarle un monto a usted. Borre estos correos electrónicos, ya que responderlos puede ocasionar que vacíen su cuenta bancaria y roben su información personal.

Póngase en contacto con la Procuraduría General
441 4th Street, NW, Washington, DC 20001
Tel.: (202) 727-3400 Fax: (202) 347-8922 TTY: (202) 727-3400
Correo electrónico: dc.oag@dc.gov
LÍNEA DIRECTA DEL CONSUMIDOR — (202) 442-9828

MANTÉNGASE CONECTADO:

www.oag.dc.gov

¿Cómo evito exponer mi información sensible y privada en línea?

- Utilice solo sitios "seguros" para comprar o al proporcionar información sobre usted. Estos sitios tienen el ícono de un "candado" en la barra de estado y sus direcciones (o URL) comienzan con "https".
- No haga clic en los enlaces integrados en correos electrónicos o en sitios a los que lo transfieran, a menos que conozca al remitente o el sitio web.
- Esté pendiente de los correos electrónicos no solicitados en los que el remitente le pida proporcionar información personal, como su número de Seguro Social o número de cuenta, o le pida hacer clic en un enlace o abrir un archivo adjunto. No dé este tipo de información, o direcciones o números telefónicos, inclusive en las redes sociales, y trate de no hacer clic en enlaces que no reconozca.
- Utilice contraseñas "largas y fuertes" en los sitios en línea: utilice letras minúsculas y mayúsculas, números y caracteres especiales para crear contraseñas que tengan por lo menos de 8 a 10 caracteres. No utilice contraseñas que contengan el nombre, la fecha de nacimiento o la dirección de usted o de sus familiares. No utilice la misma contraseña para varios sitios. Por último, debe cambiar su contraseña de manera regular.
- Asuma que cualquiera puede ver su información, fotos o datos si utiliza una red inalámbrica pública. Asegúrese de que las redes inalámbricas de su hogar estén protegidas con contraseñas, o mejor aún, que estén encriptadas, para evitar accesos no autorizados.
- Utilice programas de seguridad y antivirus en todas sus computadoras y dispositivos, como teléfonos inteligentes y tabletas, y actualice esos programas cuando se lo indiquen. Por lo general, las versiones actualizadas contienen parches de seguridad que ayudan a protegerlo en contra del malware (programas diseñados para robar su información personal de sitios que de otra manera son seguros).
- Reconozca que las fotos, los videos, los mensajes de texto y otros datos almacenados en una computadora o en un teléfono pueden respaldarse en otro lugar, en lo que se conoce comúnmente como la "nube". Debe leer las políticas de privacidad de su proveedor de servicios para asegurarse de que este acepta tomar medidas razonables de seguridad para mantener la privacidad de la información en la nube.
- Sea cauteloso con los juegos y programas "gratuitos" que se ofrecen en Internet. "Gratis" a menudo significa que usted está dando información personal a cambio de utilizar el producto.

¿Cómo sé si mi identidad ha sido comprometida?

- Es posible que reciba un aviso escrito de una filtración de datos, el cual es obligatorio si usted es residente del D.C. y si su información personal sensible fue comprometida. La notificación debe identificar el tipo de información que fue comprometida, como nombres, direcciones, información de tarjeta de débito o crédito, números de Seguro Social, direcciones de correo electrónico o contraseñas. Si la filtración afecta a más de 1,000 residentes del D.C., la ley del Distrito exige que se informe sobre la filtración a las agencias nacionales de información crediticia.
- Es posible que reciba una alerta de fraude de parte de su compañía de tarjeta de crédito, o vea actividad sospechosa en su estado de cuenta bancario o estado de cuenta de su tarjeta de crédito o encuentre retiros en un estado de cuenta bancario que no recuerda haber hecho.
- Es posible que reciba facturas inesperadas o llamadas de cobro por bienes o servicios que nunca compró.
- Se le niega un crédito debido a información negativa en su informe crediticio que no es exacta; por. ej. una deuda impaga que no contrajo o de la que nunca recibió la factura.

Póngase en contacto con la Procuraduría General
441 4th Street, NW, Washington, DC 20001
Tel.: (202) 727-3400 Fax: (202) 347-8922 TTY: (202) 727-3400
Correo electrónico: dc.oag@dc.gov
LÍNEA DIRECTA DEL CONSUMIDOR — (202) 442-9828

MANTÉNGASE CONECTADO:

www.oag.dc.gov

¿Qué debo hacer si me entero de que mi información personal fue comprometida?

Si sabe que ha ocurrido una actividad fraudulenta y han robado su identidad:

- Cancele cualquier cuenta bancaria o de tarjeta de crédito que considere que ha sido comprometida o que fue abierta de manera fraudulenta.
- Considere colocar un bloqueo de seguridad sobre sus informes crediticios ante las tres agencias nacionales de información crediticia: Equifax, Experian o TransUnion. El bloqueo de seguridad "bloquea" por completo la aprobación de cualquier crédito, préstamo o servicio en su nombre sin autorización adicional. Si es víctima de robo de identidad, la ley del Distrito prevé que usted puede obtener un bloqueo de seguridad sin costo alguno y que cualquier otro bloqueo de seguridad no debe constarle más de $10.
- Considere buscar y revisar servicios de control crediticio que le dan actualizaciones regulares sobre cuentas de crédito nuevas o cambios sospechosos.
- Obtenga un informe crediticio gratuito de parte de una de las principales agencias de información crediticia. Las solicitudes de informes gratuitos con base en un reclamo por fraude se pueden hacer en línea en www.annualcreditreport.com o llamando al (877) 322-8228 o se pueden hacer directamente a las agencias de información crediticia:

TransUnion	**Experian**	**Equifax**
P.O. Box 6790 Fullerton, CA 92834-6790	P.O. Box 9532 Allen, TX 75013	P.O. Box 740241 Atlanta, GA 30374-0241
(800) 680-7289 transunion.com	(888) 397-3742 experian.com	(800) 525-6285 equifax.com

- Presente una denuncia policial ante el Departamento de la Policía Metropolitana del D.C. y obtenga una copia de la denuncia tan pronto como esté disponible.

Controlar de manera diligente su información personal siempre es beneficioso.

Esté pendiente de revisar sus documentos financieros. Revise detenidamente sus estados de cuenta bancarios y de tarjetas de crédito e infórmele al banco o la compañía de tarjetas de crédito sobre cualquier transacción no autorizada o desconocida.

Controle de manera periódica los informes crediticios para ver si hay alguna actividad inusual y revise la exactitud de los montos. Toda persona tiene derecho a un informe crediticio gratuito por año de parte de cada una de las tres principales agencias de información crediticia.

¿Qué debo hacer si soy víctima de una estafa de *telemarketing*?

Puede presentar una queja ante la Oficina de Protección al Consumidor de la Procuraduría General del Departamento de Columbia llamando a nuestra línea directa al (202) 442-9828, correo electrónico (consumer.protection@dc.gov), o escribiendo a la **Oficina de Protección al Consumidor** de la Procuraduría General.

También puede presentar una queja ante la Comisión Federal de Comercio, ubicada en 600 Pennsylvania Avenue, NW, Washington, D.C. 20580; (877) 832-4357; www.ftc.gov.

Póngase en contacto con la Procuraduría General
441 4th Street, NW, Washington, DC 20001
Tel.: (202) 727-3400 Fax: (202) 347-8922 TTY: (202) 727-3400
Correo electrónico: dc.oag@dc.gov
LÍNEA DIRECTA DEL CONSUMIDOR — (202) 442-9828