Cómo hacerle frente al COVID-19

Evite el robo de identidad y el fraude de cuentas ligados a la pandemia

Durante la lucha continua del país contra las dificultades de la pandemia, los estafadores y ladrones de identidad se están aprovechando de la crisis. Se dirigen a los consumidores que están buscando información, recursos, alivio financiero, asistencia para la vivienda y tratamiento para COVID-19.

Esta publicación advierte al consumidor sobre los fraudes más comunes de los que se debe cuidar, ofrece consejos para protegerse y explica qué puede hacer si resulta como víctima.

Robo de identidad y fraude de cuentas

El robo de identidad y el fraude de cuentas están estrechamente relacionados. El robo de identidad se refiere más específicamente al uso de información robada para abrir y abusar de nuevas cuentas bajo el nombre de la víctima, mientras que el fraude de cuentas en general se refiere al uso indebido de la información personal de alguien para acceder y abusar de sus cuentas existentes (también conocido como fraude de "adquisición de cuentas").

Tanto el robo de identidad como la adquisición de cuentas son delitos que pueden tener consecuencias significativas. Por lo general, las víctimas sufren algún tipo de pérdida financiera. Pero además las consecuencias pueden ir más allá de lo monetario e incluir otros efectos, tal como cargos criminales erróneos o errores médicos que podrían resultar fatales.

Fraudes ligados a la pandemia

Los casos de fraude de cuentas y robo de identidad vienen en aumento durante los últimos años, pero la crisis de COVID-19 ofrece a los delincuentes una oportunidad para explotar las circunstancias únicas que presenta esta pandemia global. El miedo y la incertidumbre generalizados, en combinación con programas de socorro de reciente creación y la introducción de vacunas a nivel nacional, crearon oportunidades para estafadores y ladrones.

Algunas de las estafas más destacados son:

Fraude de beneficios de desempleo: La

información personal obtenida de compañías de informes de crédito, bancos y compañías de tarjetas de crédito, sistemas de seguro médico y otras fuentes a través de una filtración de datos o robo de identidad anteriores se utiliza para robar miles de millones en beneficios de seguro de desempleo. Los estafadores presentan reclamaciones utilizando identidades robadas, y las víctimas a menudo se enteran sólo cuando se les rechaza o retrasa su propia reclamación, o cuando presentan su declaración de impuestos.

Robo de pagos de estímulo: De manera que los pagos federales de estímulo les llegaran a los beneficiarios, el IRS lanzó un portal en línea (ya cerrado) donde las personas calificadas que no habían presentado su declaración de impuestos en 2018 o 2019 podían ingresar información básica de identificación personal (nombre, dirección, fecha de nacimiento, números de Seguro Social [SSN], de cuenta bancaria, de licencia de conducir o de identificación emitidos por el estado, etc.) y registrarse para recibir los pagos de estímulo. Los estafadores que pudieron obtener esta información básica la utilizaron para reclamar los cheques de las víctimas. Esa herramienta se cerró, pero los delincuentes seguramente encontrarán nuevas formas de interceptar el dinero de las víctimas.

Fraude relacionado con la vacunación: El proceso de vacunación contra COVID-19 permite que los impostores obtengan datos confidenciales (información personal, y números de cuentas de Medicare y seguro médico, etc.) haciéndose pasar por personal de atención médica o de agencias gubernamentales que, entre otras cosas, programan citas de vacunación. Los datos robados se usan para cometer una variedad de fraudes financieros y de seguros. (Lea la alerta de fraude del Department of Health and Human Services, con advertencias específicas sobre COVID y vacunas: *https://oig.hhs.gov/fraud/consumer-alerts/fraud-alert-covid-19-scams/*.)

Fraude de asistencia de alquiler: Sabiendo que en Estados Unidos millones de personas corren el peligro de ser desalojados y de ejecuciones hipotecarias por haber perdido su empleo en la pandemia, los estafadores llaman y envían correos electrónicos y mensajes de texto a sus potenciales víctimas; fingen ser parte de una agencia o programa que proporciona asistencia monetaria para pagar hipotecas o alquiler, asistencia legal, u otro servicio o ayuda para no perder sus viviendas.

Estos son sólo algunos de los muchos tipos de fraude y robo de identidad surgidos desde el comienzo de la pandemia. Hay varios más que explotan datos robados (o revelados involuntariamente); angustia, confusión, esperanza y necesidad; programas de asistencia que se ven abrumados; y las propias prácticas del consumidor con respecto a la seguridad de su datos.

Protección de sus datos

La mejor forma de evitar ser víctima de fraude es por medio de su propio compromiso a la protección de su información personal. Algunos de los datos personales que se pueden utilizar para cometer robo de identidad y fraude incluyen su nombre, dirección, número de Seguro Social (SSN), fecha de nacimiento, apellido materno y números de cuenta (tarjeta de crédito, cuenta bancaria, Medicare, seguro, licencia de conducir, etc.).

Estos son algunos consejos para mantener sus datos personales privados:

Número de Seguro Social (SSN): No lleve consigo su tarjeta del Seguro Social; memorice el número. Baje la voz al dar su número de Seguro Social u otra información confidencial en bancos, consultorios médicos u otros lugares públicos.

Tarjetas de crédito, bancarias y otras: Lleve sólo las tarjetas que necesita ese día; si pierde o le roban su billetera o bolso, habrá menos cuentas en peligro. Siempre cuide su billetera o bolso. En restaurantes, no cuelgue el bolso en su silla.

Solicitudes de información: Nunca responda a solicitudes de información personal a menos que usted haya iniciado el contacto o esté absolutamente seguro de que conoce a la empresa o persona con la que está tratando. Para verificar que la solicitud es legítima póngase en contacto con la entidad

solicitante llamando al número que figura en su estado de cuenta o en un directorio o sitio web de confianza. No haga clic en enlaces ni abra archivos adjuntos de remitentes que no reconozca (verifique con cuidado la dirección de correo electrónico del remitente).

Documentos: Cierre con llave su buzón de correo postal. Deposite el correo de salida que contenga cheques o datos personales en un buzón del servicio postal: no lo deje en el buzón de su casa o en el vestíbulo de su apartamento. En su casa, oculte la información confidencial, como estados de cuentas bancarias y de tarjetas de crédito, registros de seguro, etc., donde los visitantes o trabajadores no los vean. Antes de descartar documentos y correo que contengan su número de Seguro Social, números de cuenta y otra información personal, tritúrelos o rómpalos en pedacitos.

Redes sociales: Elimine su información personal en cuentas de redes sociales y revise la configuración de privacidad para asegurarse que su perfil no sea visible al público. No publique fotos de su tarjeta de vacunación COVID-19, ya que muchos que lo hicieron terminaron víctimas de robo de identidad.

Números de identificación personal (PIN, siglas en inglés) y de inicio de sesión: En los cajeros automáticos (ATM, siglas en inglés), proteja el teclado al introducir los números PIN de tarjetas de crédito y débito. No anote los nombres de usuario y contraseñas de la cuenta. En su lugar, utilice un administrador de contraseñas en línea ("online password manager") para almacenar sus credenciales de inicio de sesión de diferentes sitios; sólo tendrá que recordar una contraseña para acceder a todas las demás. (Haga una búsqueda en línea de "best password managers" [mejores administradores de contraseñas] para encontrar información y opiniones sobre sus opciones.)

Crédito. La colocación de una "congelación" ("freeze") en su archivo de crédito impide que se emita un nuevo crédito a su nombre. Congelar y descongelar sus informes es gratis. Obtenga más información en *Congele su crédito* (*https://www.consumer-action.org/spanish/articles/freeze_your_credit_file_sp*).

Detección de fraude y robo de identidad

Cuanto antes se entere de un fraude de cuentas o robo de identidad, más pronto podrá detener el daño. Mejore la probabilidad de darse cuenta de actividad sospechosa adoptando estas prácticas:

Regístrese para recibir alertas de fraude. Muchos acreedores e instituciones financieras ofrecen enviarle mensajes de correo electrónico o de texto para ayudarle a detectar actividades no autorizadas en su cuenta.

Esté al tanto de su correo. Si no recibe facturas, estados de cuenta de tarjetas de crédito y demás correo que esté esperando, puede ser que un delincuente se haya hecho cargo de sus cuentas y haya cambiado la dirección donde recibe facturas. Del mismo modo, si recibe correo postal que no esperaba, como una tarjeta de crédito nueva o rechazos de crédito o préstamos que no solicitó, facturas o avisos que no reconoce, cartas (o llamadas) de cobradores de deudas, etc., es posible que alguien esté usando su identidad para abrir cuentas nuevas.

Verifique inmediatamente sus estados de cuenta financieros y facturas. Revise con atención los diversos estados de cuenta financieros y de crédito, y verifique que no haya alguna actividad no autorizada. Infórmele de inmediato a la compañía sobre cualquier actividad sospechosa.

Revise sus informes de crédito con regularidad. Obtenga copias gratuitas de cada una de las tres principales compañías de informes crédito (Equifax, Experian y TransUnion) en *AnnualCreditReport.com* o llamando al 877-322-8228. (Hasta el 20 de abril de 2022, puede recibir informes gratuitos semanalmente, en lugar de una vez por año, si los solicita.) Verifique que en sus informes de crédito no haya cuentas que no reconoce.

Cuestione los rechazos de crédito. Si sabe que tiene buen crédito y se le niega una solicitud de préstamo nuevo, puede haber un problema. Revise

sus informes de crédito y verifique que no contengan actividad que no sea suya que esté dañando su crédito.

Cómo reparar el daño

Si descubre que fue víctima de fraude de cuentas o robo de identidad, tome estas medidas:

■ Visite el sitio web de la Federal Trade Commission (FTC) sobre el robo de identidad (*https://www.identitytheft.gov/*) para crear un un Reporte de Robo de Identidad y recibir un plan de recuperación.

■ Considere presentar un informe con su departamento de policía local (si un acreedor lo requiere; si puede identificar al ladrón o tiene detalles específicos que puedan ayudar en la investigación; o si usaron su identidad en un encuentro con la policía). Obtenga una copia del informe policial como prueba de ser víctima. Si el robo de identidad ocurrió en línea, reporte el delito al Internet Crime Complaint Center (IC3) de la FBI (centro para quejas sobre delitos en internet) (*https://www.ic3.gov/*).

■ Póngase en contacto con el departamento de seguridad o fraude de cada empresa para disputar cualquier transacción fraudulenta y cerrar cuentas abiertas o utilizadas sin su conocimiento. Pida una carta que confirme que la cuenta fraudulenta no es suya, que no es responsable de ella, y que fue (o será) eliminada de su informe de crédito. Pregunte si necesita además presentar una solicitud o declaración por escrito. (De ser necesario, pida las solicitudes fraudulentas y demás registros comerciales de cualquier transacción relacionada con el robo de identidad, ya que podrían ayudarle a demostrar que se falsificaron.)

■ Notifique a **Equifax** (*https://www.equifax.com/personal/identity-theft-protection/*), **Experian** (*https://www.experian.com/help/identity-theft-victim-assistance.html*) o **TransUnion** (*https://www.transunion.com/blog/identity-protection/know-report-identity-theft*) sobre el robo de identidad para que puedan agregar una alerta de fraude a sus informes. (Cualquiera de estas compañías que notifique compartirá la información con las otras dos.)

■ Si sospecha que le robaron sus beneficios o reembolso de impuestos, comuníquese con la agencia correspondiente (oficina estatal de desempleo, IRS, etc.) para informarle sobre el problema y averiguar qué pasos adicionales debe tomar para recuperar la pérdida.

■ Para el resto de sus cuentas, incluso si no se infringieron, cree nuevos números de identificación personal (PIN) y contraseñas que sean fuertes (difícil de advinar) y únicos (que no se comparten con ninguna otra cuenta).

Acerca de Consumer Action

www.consumer-action.org

A través de educación y defensa, Consumer Action promueve derechos y políticas sólidas a favor del consumidor que impulsan equidad y prosperidad financiera para los consumidores subrepresentados en todo el país.

Asesoramiento y asistencia al consumidor: Envíe quejas sobre asuntos del consumidor a: *https://complaints.consumer-action.org/forms/english-form/complaint_form/* o llame al 415-777-9635. (Las quejas en español pueden presentarse a: *https://complaints.consumer-action.org/forms/spanish-form/*.)

Nuestra línea directa acepta llamadas en chino, inglés y español.

Consumer Action creó esta guía como parte de su proyecto educativo COVID-19 Educational Project.

WELLS FARGO

Fondos proporcionados por Wells Fargo.