Sección 2: Robo de Identidad

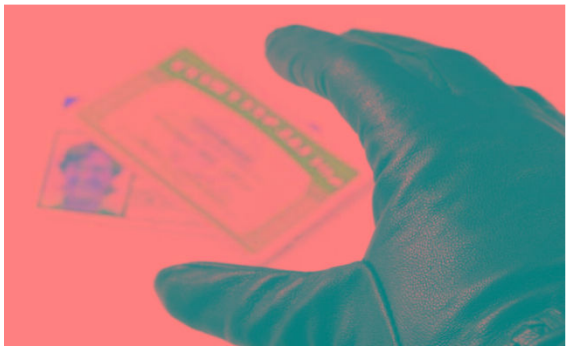
Introducción

El robo de identidad es uno de los delitos de más rápido crecimiento en el mundo hoy y puede ser uno de los problemas más costosos que enfrentan los consumidores. Los consumidores reciben casi todos los días ofertas que suenan demasiado buenas para ser verdad. La mayoría de esas ofertas solían llegar por correo o por teléfono, pero hoy en día, también llegan por correo electrónico e Internet. Los estafadores no tienen fronteras nacionales y, de hecho, pueden estar ubicados en otros países pero "haciendo negocios" en los Estados Unidos.

¿Qué es el robo de identidad?

El robo de identidad significa que alguien utiliza su información personal (su nombre, número de seguro social, número de tarjeta de crédito u otros datos similares) sin su permiso. Por lo general, las personas que roban su identidad utilizan esta información para alquilar un apartamento, obtener un teléfono celular, obtener otra tarjeta de crédito o realizar otras acciones en su nombre. Por supuesto, pueden usar lo que han comprado ilegalmente, y usted recibe las facturas.

Según la Comisión Federal de Comercio, cada año se roba la identidad de unos 9 millones de personas sólo en los Estados Unidos. Puede que conozca a alguien que haya sido una víctima. Puede tomar cientos de dólares y muchas horas de su tiempo para corregir el problema. Mientras tanto, su historial de crédito y su reputación se ven afectados. Puede que incluso no consiga un trabajo, alquile un apartamento o se le niegue un préstamo o una beca debido a la información negativa que se ha reunido sobre usted, aunque no tenga nada que ver con el problema. Algunas víctimas incluso han sido arrestadas por un crimen porque alguien más usó sus nombres.



¿Cómo lo hacen?

Los ladrones de identidad utilizan varios enfoques diferentes para obtener información sobre ti. Estos incluyen:

Bucea en el basurero y buzones. Revuelven en su basura buscando facturas u otros papeles con su información personal. Es posible que ladrones saquen cosas de su buzón como extractos de cuenta, información de impuestos, o nuevos cheques.

Copiar tarjetas. Roban los números de las tarjetas de crédito o de débito con un dispositivo especial al procesar su tarjeta.

Fingir Identidad. Fingen ser bancos, el IRS o alguna otra organización y le envían un correo electrónico o una carta (o incluso hacen una llamada telefónica) pidiendo información personal. También pueden duplicar sitios web creíbles para obtener esa información.

Cambiar su dirección. Completan una tarjeta de cambio de dirección, creando una nueva dirección para usted para que puedan recibir sus estados de cuenta. Una vez que tengan los estados de cuenta, podrán acceder a su cuenta.

Robar. Roban billeteras, carteras, móviles, o otra tecnología portátil.

Piratería. Pueden piratear su computadora u otro sistema informático, incluyendo escuelas, compañías de tarjetas de crédito y otros lugares que mantienen información personal.

Desafortunadamente, alguien puede usar su información personal durante meses antes de que usted se entere. Imagina las facturas y los honorarios que pueden acumularse en su contra antes de que se entere.

¿Cómo se sabe que pasó?

Pistas que alguien ha robado su información

- Hay retiradas en su cuenta bancaria que no puede explicar.
- No recibe cuentas ni otros correos.
- Vendedores rechazan sus cheques.
- Cobradores le llaman por deudas que no son suyas.
- Encuentra cuentas y cargas desconocidas en su reporte de crédito.
- Proveedores médicas facturan por servicios que no usó.
- Su plan de salud rechazó su reclamación médica legítima porque la historia muestra que alcanza su límite.
- Seguro médico no le cubre porque su historia médica muestra una condición que no la tiene.
- El Servicio de Rentas Internas (IRS) notifica a usted que más de una declaración de ingresos fue declarada por usted o tiene ingresos por un empleador que no trabaja.
- Recibe un aviso que su información fue arriesgada por un filtración de datos en una compañía que no tiene cuenta ni hace negocios.

Cómo protegerse del robo de identidad

Desafortunadamente, no puede protegerse completamente de ser una víctima, pero hay varias cosas que puede hacer para minimizar el potencial.

- Use las contraseñas de su tarjeta de crédito, banco y cuentas de teléfono celular. Evite las contraseñas que son información que otros puedan conocer -- su fecha de nacimiento, dirección, número de seguro social o números de teléfono. Además, utilice contraseñas que sean una combinación de letras y números y las cambie frecuentemente.

- Ponga su información personal en un lugar seguro, como una pequeña caja fuerte o caja de seguridad, para evitar fácil acceso a la caja. Lleve sólo la información de identificación y las tarjetas de crédito/débito que necesite cuando salga.

- Triture todos los papeles con su información personal antes de tirarlos a la

basura. Asegúrese de triturar ofertas de tarjetas de crédito, cheques de tarjetas de crédito enviados por la compañía de su tarjeta, formularios de seguros y otros papeles con su nombre e información personal.

- NUNCA dé ninguna información personal por teléfono, a través del correo, en Internet, en un correo electrónico o en persona a menos que usted haya iniciado el contacto y esté seguro de con quién está tratando. ¡Recuerde que el IRS, su banco, la compañía de su tarjeta de crédito y otros lugares donde hace negocios no necesitan pedirle que por la información!

- Evite cortar y pegar o hacer clic en los enlaces web de los correos electrónicos, a menos que esté seguro de que es un enlace válido. Sólo se introducen datos personales en sitios web seguros.

- Ponga su correo saliente de los Estados Unidos en un buzón de correo o llévelo a la oficina de correos en lugar de ponerlo en el buzón de la casa. Cualquiera puede pasar a recogerlo. Si va a salir de casa por la noche, haga que la oficina de correos retenga su correo hasta que usted regrese.

- Tenga cuidado con las ofertas o organizaciones sin ánimo de lucro. Las investigue que sean reputadas y legítimas.

- Solicite una copia de su informe crediticio a las tres principales agencias de crédito para controlar su historial de crédito. Se le permiten tres por año sin costo. Muchos proveedores financieros con los que ya trata también le proporcionarán la información de sus informes crediticios como parte de sus servicios.

Proteger su futuro

- **Revise su administración del dinero y el proceso de pagar las cuentas.** Las lagunas o debilidades en la forma en que administra su dinero y sus cuentas a menudo son la forma en que se roba su identidad o información.
- **Mejore su plan de protección personal contra fraude.** Averigüe cómo ocurrió el fraude y cambie su comportamiento al respecto.
- **Tenga un fondo de emergencia.** Es posible que necesite acceder a su fondo de emergencia para cubrir la disrupción y restablecer todo de sus cuentas.

Pasos a seguir si se es víctima

- Presente una queja ante la Comisión Federal de Comercio. Su sitio web es www.ftc.gov y contiene números de teléfono, formularios e información general.

- Póngase en contacto con la división de fraude de las tres oficinas de crédito y pídales que pongan una alerta de fraude en sus archivos de crédito. Si alguien roba su identidad, tiene derecho a quitar la información fraudulenta de su informe crediticio. A esta acción se le llama bloqueo. Cuando se bloquea la información, no aparecerá en su informe crediticio y las empresas no podrán intentar cobrar la deuda. Si tiene un Informe de robo de identidad de la FTC, las agencias de crédito deben cumplir con su solicitud de bloquear esta información.
    - Equifax, 1-800-525-6285, www.equifax.com
    - Experian, 1-888-397-3742, www.experian.com
    - TransUnion, 1-800-680-7289, www.transunion.com

- Contacte con su policía local o con la policía de la ciudad donde tuvo lugar el robo de identidad.

- Contacte con sus instituciones financieras, proveedores de crédito, o cuentas de servicios para verificar que ellos no se han visto afectadas. Solicite una copia gratis de su reporte de ChexSystems, que recopila la información de sus cuentas de crédito. Para obtener su reporte, contacte ChexSystems al 1-800-428-9623.

- Llame a los departamentos de fraude de todos los negocios que tienen actividad fraudulenta. Presente una copia de la queja con la policía y la FTC a las compañías para verificación.

- Revise su proceso de pago de facturas. Es posible que deba restablecer cualquier opción de pago que tenga implementada si necesita bloquear o cerrar cuentas. Si el fraude causa una interrupción importante en su flujo de efectivo, es posible que deba comunicarse con los deudores para analizar las opciones para los pagos retrasados.

Revisión de la lección

Compare los siguientes términos con los escenarios. Ponga la letra del término correcto en el espacio en blanco delante del escenario.

A. Cambiar la dirección B. Copiar Tarjetas C. Robar D. Piratería

E. Fingir Identidad F. Pretextos G. Bucea en el basurero

___1. John tira todas las copias de sus facturas y estados de cuenta de sus tarjetas de crédito a la basura. Recibe una llamada de la compañía de su tarjeta de crédito preguntándole si ha estado en Cancún recientemente y ha comprado una gran cantidad de equipo de buceo. John nunca ha viajado fuera de los Estados Unidos. ¿Qué término describe cómo un ladrón obtuvo la información de la tarjeta de crédito de John?

___2. Kaden recibió un correo electrónico pidiéndole que confirmara la información de su tarjeta de crédito y luego hizo clic en el enlace del correo electrónico que lo dirigía a un sitio que le pedía que llenara los espacios en blanco con su nombre, número de seguro social y su número de tarjeta de crédito. El sitio se parecía al de la organización legítima, así que cumplió con la petición. Poco después de proporcionar la información, recibió una factura de la compañía de su tarjeta de crédito con varias compras que no había hecho. ¿Qué término describe lo que le pasó a Kaden?

___3. La abuela de Mary pagó su almuerzo con una tarjeta de crédito. El camarero le devolvió la tarjeta y ella firmó el recibo. Un mes después, aparecieron varios cargos en la cuenta de la tarjeta de crédito de su abuela que ella no había hecho. ¿Qué término describe lo que hizo la camarera?

___4. Kurt es un nerd de las computadoras con habilidades excepcionales. Es capaz de acceder a ordenadores que pertenecen a otras personas. Obtiene los números de cuenta bancaria y de tarjeta de crédito del Sr. Ling y los usa para ordenar artículos de Amazon.com. ¿Qué término describe lo que Kurt está haciendo?