Agarra la onda...
¡cuida tu dinero!
¿Debo prestar atención?

ROBO DE IDENTIDAD

Como operan los ladrones

¡Y AHORA EMPIEZA LA PESADILLA!

¡Seguridad ante todo!

SI ERES UNA VÍCTIMA

¡Privacidad, por favor!

Probablemente has oído hablar del robo de identidad. O tal vez tú o alguien que conoces hayan sido víctimas de este crimen. Pero, ¿qué es exactamente el robo de identidad?

Bueno, se refiere a cuando alguien roba tu información personal y la utiliza para obtener una tarjeta de crédito, rentar un departamento, conseguir un empleo o cometer un delito. Estas personas no sólo se hacen pasar por ti, sino que también te responsabilizan de pagar por los gastos que incurren usando tu nombre.

Es decir que aunque no hayas hecho nada malo, podrías tener que pagar las consecuencias de sus acciones. Estas consecuencias podrían ser el tener que pagar por cosas que no compraste, que rehúsen otorgarte préstamos para comprar un coche o pagar por tu educación, no poder obtener un empleo o hasta ser arrestado. En el mejor de los casos, te causará estrés y una serie de molestias al tratar de probar tu inocencia a tu compañía de tarjetas de crédito. En el peor de los casos, podrías pasar años tratando de reparar tu historial crediticio, laboral y tu reputación.

Universidad de California
Agricultura y Recursos Naturales

Robo de identidad

Es uno de los delitos de mayor incidencia en los Estados Unidos; el robo de identidad afecta a 9 millones de estadounidenses anualmente, según la FTC. En conjunto, las víctimas de robo de identidad perderán más de $5,000 millones de dólares tan sólo en este año. Ser adolescente no quiere decir que estés a salvo. De hecho, corres un mayor riesgo. Puesto que la mayoría de adolescentes no cuentan con un historial de crédito, los ladrones pueden abrir cuentas nuevas a tu nombre y ni siquiera te enterarás. Si esto te pasara a ti, podrían pasar años sin que lo supieras y te enterarías cuando trates de obtener un préstamo. Puesto que estás empezando a establecer tu historial crediticio, todo tu futuro financiero corre riesgo. Y, si no cuentas con una licencia de conducir, un ladrón puede usar tu número de Seguro Social para solicitar una y tú no te enterarás sino hasta que acudas a solicitar tu propia licencia y te sea negada.

¿Qué tan serio es el riesgo que corro?

Esta prueba te ayudará a saber qué tan serio es el peligro de que te conviertas en víctima de robo de identidad.

☐ Nunca ☐ A veces ☐ Siempre 1. ¿Qué tan seguido tiras o reciclas documentos que tienen tus datos personales, como recibos de compras, ofertas preaprobadas para tarjetas de crédito o la factura de tu teléfono celular?

☐ Nunca ☐ A veces ☐ Siempre 2. ¿Qué tan seguido utilizas tu nombre completo en los perfiles que aparecen en la Internet para que tus amigos puedan encontrarte?

☐ Nunca ☐ A veces ☐ Siempre 3. ¿Cuántas veces, después de usar la computadora de otra persona, sólo cierras el navegador en lugar de salirte por completo del sistema de correo electrónico, de las páginas de tu banco o de las redes sociales?

☐ Sí ☐ No ☐ No viene al caso 4. Reviso la actividad de mi cuenta de tarjeta de débito por lo menos una vez a la semana para asegurarme que nadie ha usado mi cuenta ilegalmente.

☐ Sí ☐ No ☐ No viene al caso 5. He incluido mi número de Seguro Social en un formulario de salud, solicitud de empleo o se lo he dado a un representante de un equipo deportivo, sin preguntar para que lo necesitan.

☐ Sí ☐ No ☐ No viene al caso 6. Llevo siempre conmigo mi tarjetas de crédito, débito o chequera cada vez que salgo, por si acaso.

☐ Sí ☐ No ☐ No viene al caso 7. He compartido mis contraseñas y números de cuentas con algunas personas muy cercanas a mi, porque sé que puedo confiar en ellas.

☐ Sí ☐ No ☐ No viene al caso 8. Utilizo programas para compartir archivos o información para obtener música y películas gratis.

Busca la clave de puntuación en la página 3

CONFIDENCIAL

Clave de puntuación

Pregunta 1: Nunca = 1 punto; A veces = 2 puntos; Siempre = 3 puntos
Tirar a la basura o reciclar información privada no es suficiente. Los ladrones de identidad por lo general buscan entre la basura información que les pueda servir para robar tu identidad. Es mejor hacer trizas todo documento que contenga información personal usando una trituradora de papel de corte cruzado.

Pregunta 2: Nunca = 1 punto; A veces = 2 puntos; Siempre = 3 puntos
Incluir información como tu nombre completo y fecha de nacimiento en sitios de redes sociales (o cualquier otro sitio) incrementa tu riesgo de robo de identidad. Es mejor usar un sobrenombre y dejarles saber a tus amigos el nombre que escojas.

Pregunta 3: Nunca = 1 punto; A veces = 2 puntos; Siempre = 3 puntos
Si sólo cierras el navegador, no estás haciendo lo suficiente para protegerte. Muchos sitios te mantienen conectado hasta que te sales del sistema. Así que la siguiente persona que use la computadora podría tener acceso a tus cuentas privadas. Aunque es mejor acceder a información privada en tu propia computadora, lo mejor que puedes hacer cuando uses una computadora ajena es finalizar la sesión en todos los sitios a los que te conectaste y borrar los archivos temporales del navegador antes de retirarte de la computadora ajena.

Pregunta 4: Si = 1 punto; No = 3 puntos; N/A=1 punto
Al revisar tu cuenta cuidadosamente podrás darte cuenta de inmediato si alguien te ha robado tu información bancaria. Entre más pronto lo notes, menor será el costo. Si te das cuenta en un periodo de dos días y notificas a tu banco, sólo tendrás que pagar un máximo de $50 dólares. Si notificas a tu banco en un periodo de 2 a 60 días, podrían cobrarte hasta $500 dólares. Si lo notificas hasta después de 60 días, podrías ser responsable de la cantidad total que los ladrones gasten, lo que podría alcanzar miles de dólares.

Pregunta 5: Sí = 3 puntos; No = 1 punto; N/A=1 punto
Los amantes de lo ajeno pueden usar tu número de Seguro Social para abrir cuentas de crédito, solicitar una licencia de conducir y hasta para obtener un empleo. Son pocas las ocasiones en las que se requiere legalmente el número de Seguro Social. Así que, antes de dárselo a alguna persona, pregunta ¿para qué lo necesita? ¿Qué hará con él? ¿De qué manera lo protegerá? Para más información, lee “Una nota sobre tu número de Seguro Social” en la página 6.

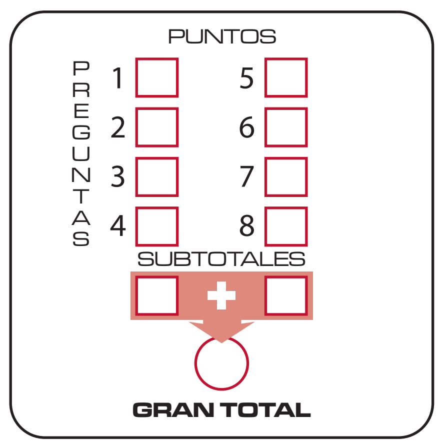
Pregunta 6: Si = 3 puntos; No = 1 punto; N/A=1 punto
Llevar contigo tus tarjetas de crédito y débito y tu chequera cuando no las necesitas aumenta tus posibilidades de perderlas o de que te las roben. Si vas a ir al cine o a cenar, lleva contigo la cantidad de dinero que planeas gastar. Esto no sólo mantendrá tus cuentas de banco y tarjeta de crédito a salvo, sino que también podría ayudarte a gastar menos dinero.

Pregunta 7: Sí = 3 puntos; No = 1 punto; N/A=1 punto
Desafortunadamente los malhechores que roban la identidad a adolescentes por lo general son personas que las víctimas conocen, incluyendo a familiares de confianza. Así que lo mejor es mantener tus contraseñas y la información de tus cuentas en secreto.

Pregunta 8: Sí = 3 puntos; No = 1 punto; N/A=1 punto
Aunque los programas que comparten información parecen ser una opción económica para obtener cosas que quieres, estos también le dan acceso a otros usuarios a tu computadora y archivos. Aún cuando organices tu computadora para “compartir archivos”, los usuarios también podrían obtener tus fotografías, estados de cuentas, contraseñas, en otras palabras, ¡todo! Cuando esto ocurre, los archivos de información compartida pueden terminar costándote mucho dinero y tiempo.

Tu puntuación

Escribe la puntuación para cada pregunta en los recuadros de abajo. Obtén el subtotal de cada columna. Suma ambos subtotales para obtener tu puntuación total.



¿Qué significa tu gran total?

8 - 13 puntos: Tu riesgo de sufrir robo de identidad parece bajo, pero aún así, hay que ser siempre cautelosos. Sigue leyendo para saber si puedes encontrar algunas otras maneras de mantener tu identidad a salvo.

14 - 19 puntos: Tu riesgo de sufrir robo de identidad es moderado. Esta información puede ayudarte a encontrar maneras de reducir tu riesgo aún más.

20 - 24 puntos: Tu riesgo de sufrir robo de identidad es alto, pero no es demasiado tarde para protegerte. La información incluida en esta prueba te da buenas ideas sobre los cambios que puedes adoptar para protegerte. Para más información sobre cómo proteger tu identidad, lee el resto de este boletín.

Cómo operan los ladrones

Los ladrones de identidad básicamente tienen dos objetivos. El primero, obtener información privada. Segundo, desean usar esta información para su propio beneficio. ¿Cómo obtienen acceso a información que se supone es privada? Robando la correspondencia o tarjetas de crédito y hurgando en la basura. Sigue leyendo para que te enteres acerca de las muchas maneras en las que un ladrón puede robarte tus datos personales.

Duplicado de tarjetas: Quizás este sea el método más usado para defraudar con tarjetas de crédito. Básicamente se da cuando le entregas tu tarjeta de crédito a un mesero, cajero o recepcionista en un consultorio médico y copian la información de tu cuenta. Los maleantes también pueden colocar un lector de tarjetas de crédito en el deslizador de tarjetas del cajero automático. La información de tu cuenta queda grabada cuando retiras dinero de tu cuenta. Protégete revisando habitualmente la actividad de tu cuenta.

Hurgar en los contenedores de basura: Los ladrones literalmente se echan un "clavado" en los contenedores y botes de basura y reciclables y hasta en las pilas de desperdicio en el vertedero de basura. Todo lo que necesitan encontrar es un aviso de tarjeta preaprobada a tu nombre. Pero muchas veces encuentran mucho más. Haz trizas todos los documentos que contengan datos personales.

Programas espías para computadoras: Los programas espías o *spyware* pueden ser descargados a tu computadora cuando visitas ciertos sitios en la Internet o llevas tu computadora a reparar. Estos programas permiten a los estafadores registrar tu actividad en la Internet y todo lo que allí escribes, inclusive números de cuentas y contraseñas. Puedes protegerte instalando programas que detectan virus o programas espías en tu computadora y mantenerlos actualizados.

Cambio de dirección: Los ladrones pueden ir a la oficina postal y llenar un formulario para que tu correspondencia les sea enviada directamente a su dirección. También pueden llamar a tu institución financiera y decirles que te has mudado. Tanto los bancos como las cooperativas de ahorro y crédito por lo general envían cartas a ambas direcciones así que está atento a la llegada de este tipo de correspondencia. Si no te has mudado pero recibes una carta del banco diciendo que tu dirección ha cambiado, ¡llámalos de inmediato!

Continúa en la página 5

Cómo operan los ladrones (cont.)

Engaños por Internet (*Phishing*): Seguramente has recibido un correo electrónico engañoso. Estos correos electrónicos aparentan ser de carácter oficial de un banco o de una tienda cibernética pidiéndote que actualices la información de tu cuenta; pero, cuando lo haces, tu información va directamente al ladrón. El *phishing* puede también darse por teléfono, cuando el ladrón se hace pasar por un funcionario bancario que llama para hablar de tu cuenta. Si crees que el mensaje electrónico o las llamadas son legítimas, llama siempre al teléfono que aparece en el reverso de la tarjeta. Quien quiera que conteste el teléfono podrá conectarte al departamento indicado.

Cosecha de contraseñas (*Pharming*): Es similar a *phishing*. El *pharming* pretende sacarte, con engaños, información sobre tu cuenta o para ingresar a ella por Internet. Los ladrones crean sitios Web falsos diseñados de tal manera que parecen bancos o tiendas cibernéticas y adquieren nombres de dominio similares a las direcciones de sitios auténticos. Así que, cuando accidentalmente llegas a escribir la página incorrecta, terminas en el sitio falso. Cuando ingresas en esa página, los ladrones se apoderan de tu nombre de usuario y contraseña. Si necesitas ingresar a una cuenta, hazlo directamente a través del sitio Web de la compañía, no a través del enlace recibido en un correo electrónico.

Saqueo inalámbrico: Si utilizas una conexión de Internet inalámbrica para tu computadora o teléfono celular, puedes ser atacado. Los ladrones buscan conexiones no protegidas y luego interceptan tu información. Con frecuencia el ladrón es el que se sienta al lado tuyo en una cafetería o en un coche en el estacionamiento. Lo mejor es simplemente evitar acceder a información personal si estas usando una conexión no protegida.

Robo: Al despojarte de tu cartera o tu bolso, un ladrón puede tener acceso inmediato a una tonelada de información. Estos ladrones tienen, por lo general, toda una red establecida para manejar el contenido de tu bolso o billetera; así que en pocos minutos pueden usar tu tarjeta de crédito o vaciar tu cuenta de banco. Un ladrón también puede robar la correspondencia que sale o llega al buzón de tu casa, lo cual le puede dar un acceso inmediato a información de tus cuentas u ofertas de tarjetas de crédito preaprobadas. Llama a tu banco u otras instituciones financieras importantes si sospechas que han robado tu información. Nunca lleves en la cartera o billetera tu número o tarjeta de Seguro Social. Mantén tu tarjeta en un lugar seguro y sácala sólo cuando sea necesario, como cuando te contraten para un nuevo empleo. Te será de gran ayuda mantener una lista de los documentos y tarjetas que llevas en tu billetera o bolso para saber a que compañías llamar si te roban.

Mirar de reojo: Un ladrón puede obtener información directamente de ti mirando de reojo cuando tecleas los números de tu tarjeta telefónica o al escucharte darle a un amigo tu dirección. Asegúrate de mirar a tu alrededor para asegurarte de que nadie te escucha antes de hablar sobre información personal. Aún mejor, no compartas tu información personal en público.

¡Y ahora empieza la pesadilla!

Una vez que robe tu información, el ladrón puede venderla a alguien más o usar tu nombre para:

- ☐ Establecer una línea de crédito u obtener un préstamo
- ☐ Pedir conexión a un servicio de teléfono
- ☐ Solicitar un servicio público
- ☐ Hacer cargos a tu tarjeta de crédito
- ☐ Obtener una licencia de conducir
- ☐ Obtener servicios médicos
- ☐ Recibir beneficios públicos del gobierno
- ☐ Rentar un departamento
- ☐ Obtener un trabajo
- ☐ Vaciar tus cuentas bancarias
- ☐ Escribir cheques de tu cuenta
- ☐ Evitar una infracción de tránsito u otros cargos criminales

Recuerda: desconéctate siempre de los sitios Web que visites.

Una nota sobre tu número de Seguro Social

Te sorprenderá cuántas personas te pedirán tu número de Seguro Social: escuelas, bancos, posibles empleadores, consultorios, solicitudes para alquilar una vivienda, para cuentas de servicios públicos, etc. Cuando alguien te pida tu número de Seguro Social:

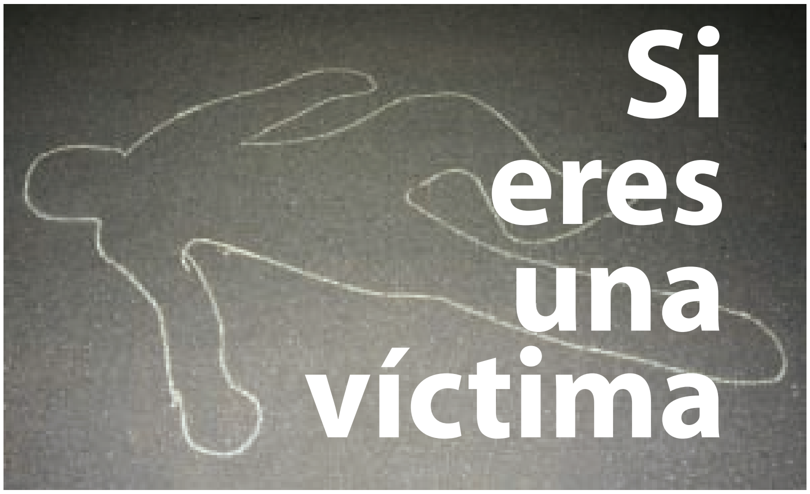
- pregúntale para qué lo necesita
- cómo piensa usarlo
- cómo lo protegerá
- qué pasa si no se lo das

Aunque a los empleadores e instituciones financieras se les requiere por ley usar tu número de Seguro Social, en muchas ocasiones podrás dejar este espacio en blanco. En la mayoría de las solicitudes de trabajo, en lugar de escribir tu número de Seguro Social, sólo escribe "available upon hire" (disponible al momento de ser contratado).

¡Seguridad ante todo!

19 formas fáciles de proteger tu identidad

1) Usa contraseñas en tu computadora portátil, celular y PDA.
2) Usa contraseñas que contengan una mezcla de letras, números y símbolos (de ser permitido).
3) No compartas tus contraseñas con nadie.
4) Has trizas las solicitudes de préstamos y tarjetas de crédito que te llegan por correo.
5) Protege tus números personales como teléfonos, direcciones, cuentas bancarias, Seguro Social, fecha de nacimiento, identificación de estudiante, etc., hasta de los amigos o familiares de confianza que no necesitan saber este tipo de información.
6) Usa una trituradora de papel de corte cruzado para destruir documentos que contengan números personales.
7) Revisa con regularidad tus estados de cuentas para verificar que nadie haya hecho cargos no autorizados.
8) No escribas tu número de cuenta al respaldo de los cheques que deposites o cambies.
9) Usa los programas *firewall*, antivirus y antiespías en tu computadora.
10) No incluyas información personal en tu blog o páginas de redes sociales.
11) No almacenes información personal en computadoras que compartas con otras personas.
12) Limpia el disco duro de una computadora que pienses regalar.
13) Verifica la información sobre privacidad de un sitio Web para saber si tu información va a ser compartida con otros.
14) Nunca pierdas de vista tus tarjetas de crédito o débito.
15) Nunca des tu información personal o contraseñas por teléfono cuando te encuentres en un lugar público.
16) Nunca le des tus números de cuenta a un representante de telemercadeo que te llame (a no ser que tú hayas pedido que te contactara).
17) No utilices tu teléfono celular para dar información privada como números de tarjetas de crédito.
18) No te sientas intimidado si un maestro, entrenador, un líder de un grupo juvenil u otro adulto de confianza te pide información privada como tu número de la licencia de conducir o tu Seguro Social. No les des esa información y pídeles que hablen con tus padres o tutor legal.
19) A partir de los 18 años, solicita una copia gratuita de tus reportes de crédito. Puedes hacerlo visitando www.annualcreditreport.com



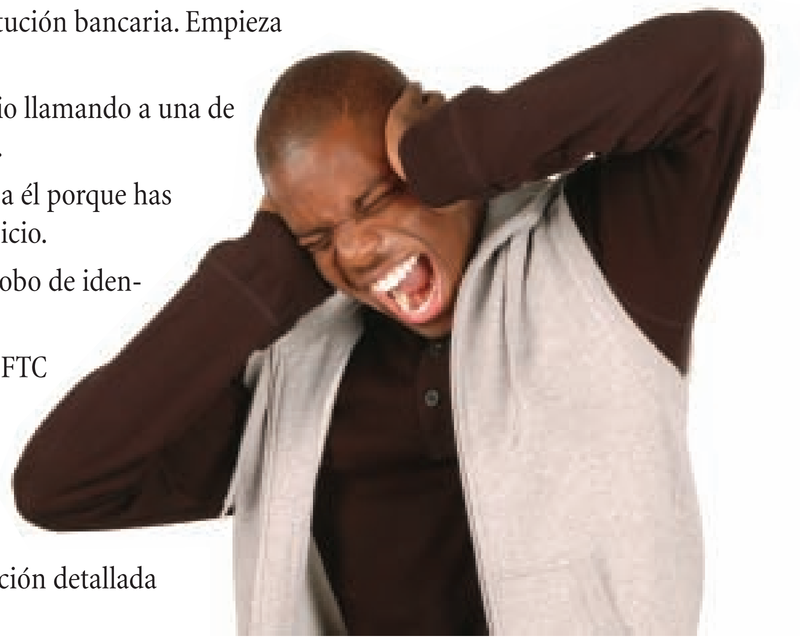
Si eres una víctima

¿Sabías que… ?

- El 15 por ciento de todos los robos de identidad son cometidos por amigos cercanos o miembros de la familia de la víctima.
- El 29 por ciento de las víctimas de robo de identidad tienen entre 18 y 29 años de edad.
- Las víctimas de robo de identidad dedican un promedio de 330 horas durante un lapso de 4 a12 meses reparando su récord.

Si te roban la identidad, actúa de inmediato para reducir el daño que le puedan hacer a tu historial crediticio o para evitar la pérdida de dinero de tus cuentas bancarias. Pide ayuda a un adulto de confianza o a tu institución bancaria. Empieza con estos cinco pasos:

1. Coloca una alerta de fraude en tu historial crediticio llamando a una de las tres agencias principales de reportes de crédito.
2. Obtén gratis un reporte de crédito. Tienes derecho a él porque has colocado una alerta de fraude en tu historial crediticio.
3. Cancela las cuentas que han sido afectadas por el robo de identidad.
4. Envía un reporte a la Federal Trade Commission o FTC (Comisión Federal de Comercio) en www.ftc.gov/idtheft
5. Presenta un reporte policial. Entrega a la policía una copia de la queja entregada a la FTC.



También puedes visitar estos sitios que tienen información detallada sobre los pasos a seguir:

http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html

http://www.justice.gov/criminal/fraud/websites/idtheft.html

Agarra la onda…¡cuida tu dinero! Es una serie de 4 boletines preparados con los jóvenes en la mente. Los temas y contenido se basan en resultados de una encuentra hecha entre jóvenes. La meta de estos boletines es ayudar a 1) identificar sus hábitos de gastar y ahorrar, 2) entender la importancia de ahorrar a largo plazo, y 3) implementar planes de ahorro que estén de acuerdo a su estilo de vida. Cualquier comentario sobre estos boletines puede dirigirse a: Consumer Economics Department, University of California, 135 Building C Highlander Hall, UC Riverside, Riverside, CA 92521. Autores: Shirley Peterson, Margaret Johns, Charles Go, Susan Cortz; Equipo de desarrollo: Grupo de trabajo Agarra la Onda…¡cuida tu dinero! de UCCE; diseñador gráfico: Kerry Decker, Universidad de California, Riverside. 2008. Traducción: Servicio de Información en Español, UC ANR, Myriam Grajales-Hall, directora.