SERIE DE BIENESTAR FINANCIERO DE GREENPATH

ROBO DE IDENTIDAD

Ayudando a la comunidad a tener una mejor vida financier

GreenPath™
financial wellness

ÍNDICE

¿Qué es el robo de identidad? 2

Cómo ocurre el robo de identidad 3

Cómo los ladrones de identidad usan su información 6

Cómo protegerse 6

¿Es usted víctima del robo de identidad? 9

Tome medidas si roban su identidad 10

Controle su crédito para no convertirse en víctima. 13

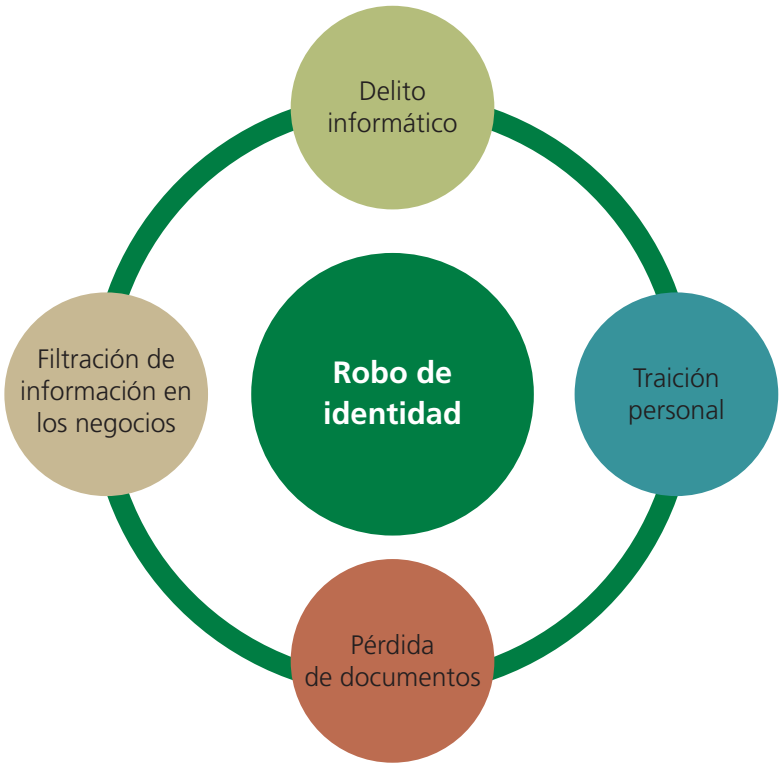
PONGA A PRUEBA SUS CONOCIMIENTOS

Busque este ícono en todo el manual para ver información importante.

¿QUÉ ES EL ROBO DE IDENTIDAD?

Desafortunadamente, la mayoría de las personas no se hacen esta pregunta sino hasta después de ser víctimas del robo de identidad. El robo de identidad es un delito grave y que cada vez es más frecuente. Un ladrón de identidad toma parte de su información personal o financiera y la utiliza haciéndose pasar por usted, robándole y realizando transacciones financieras en su nombre sin que usted lo sepa. Un ladrón puede cargar artículos a la cuenta que usted tiene o abrir nuevas cuentas, tarjetas de crédito u otras cuentas fraudulentas en su nombre. Cada año, millones de estadounidenses se ven afectados por este delito, el cual puede ocurrir de muchas formas diferentes:

- Delito informático: Ocurre cuando le roban sus datos durante sus actividades en línea.
- Traición personal: Ocurre cuando un amigo, pariente, empleado o un extraño roba sus datos.
- Pérdida de documentos: Ocurre cuando pierde su billetera o cartera, chequera o tarjetas de crédito o cuando le roban su correo o la basura.
- Filtración de información en los negocios: Ocurre cuando le roban sus archivos personales y los explotan desde un lugar en el que usted realizó actividades comerciales.



Por más que deseemos confiar en que nuestra información personal está segura, no es prudente asumir que lo está. Estas son las medidas que puede tomar para proteger su identidad.

Un delincuente comprará mercadería en línea con credenciales robadas y se las hará enviar a un hotel. El delincuente rastrea el estado de la entrega en línea y se reúne con el conductor en el estacionamiento del hotel cuando llega, de modo que la entrega no se puede rastrear hasta una persona o número de habitación. El delincuente luego vende la mercadería inmediatamente.

CÓMO OCURRE EL ROBO DE IDENTIDAD

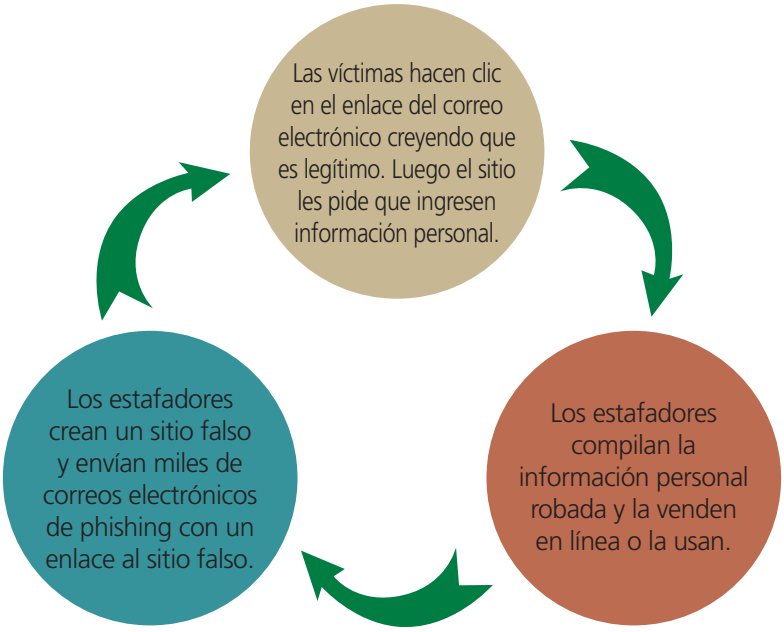
Un ladrón de identidad obtiene parte de su información personal sin que usted lo sepa y la utiliza para cometer fraude o robo. Algunos ejemplos de la información que quieren los ladrones:

Los ladrones de identidad robarán su información personal de varias formas. Los ladrones harán lo siguiente:

- Robar billeteras, carteras, mochilas, portafolios, monederos y teléfonos inteligentes.
- Robar su correo, tanto entrante como saliente.
- "Hurgar en la basura", lo cual ocurre cuando se registra la basura de su casa o del trabajo para buscar información personal.
- Robar su vehículo, en el cual está su registración y la tarjeta del seguro.
- Robar en su casa o en su negocio.
- Estafarlo por correo electrónico, haciéndose pasar por empresas legítimas, agencias guber namentales o personas necesitadas.
- Espiar en los cajeros automáticos para ver los PIN. También se le denomina "mirar por encima del hombro".
- Robar los números de su tarjeta de crédito mediante una "lectura rápida", lo cual ocurre cuando se procesa su tarjeta usando un dispositivo pequeño que almacena información y que puede leer la banda magnética del reverso de las tarjetas de crédito.

Otra forma de verificar que está en un sitio web seguro es buscar el candado en la parte inferior del explorador o en la barra de tareas. El candado cerrado indica que el sitio es seguro y que hay una conexión cifrada. Si el candado está abierto o no bloqueado, significa que la conexión no es segura y que no debe ingresar ninguna información personal.

PHARMING	
Qué es:	El pharming es un proceso que roba información de usuarios ingenuos de Internet.
Consta de dos componentes principales:	1. Los estafadores del pharming dirigen a los usuarios a sitios web comerciales fraudulentos y captan los datos personales que los usuarios ingresaron. 2. El pharming es más peligroso que el phishing ya que los delin cuentes pueden robar la información personal de los usuarios de Internet que están totalmente desprevenidos con respecto a su vulnerabilidad.
Qué puede hacer usted:	1. Borrar mensajes de correo electrónico desconocidos y no descargar archivos adjuntos ni hacer clic en enlaces incluidos en el correo electrónico. 2. No enviar información personal ni financiera por correo electrónico. 3. Verificar que está en un sitio web seguro y cifrado. Un sitio seguro generalmente está designado por una URL que comienza con "https", en donde la "s" quiere decir seguro.



PHISHING	
Qué es:	El phishing es una práctica que usan los estafadores para "pescar" contraseñas confidenciales y datos financieros del "mar" de usuarios de Internet que manejan correo electrónico.
Consta de dos componentes principales:	1. La falsificación de IP ocurre cuando los ladrones crean una réplica exacta de un sitio web existente. 2. El envío de correo no deseado ocurre cuando usted recibe correo electrónico no solicitado o también conocido como correo basura.
Qué puede hacer usted:	1. Esté atento a dónde entra en Internet. ¿Está en el sitio que creyó que estaba? 2. No sea complaciente con respecto a la seguridad. 3. No deje que la comodidad se anteponga a la seguridad.

Tenga cuidado cuando haga clic en un enlace para ir a un sitio web. Siempre debe verificar la dirección después de entrar al sitio o antes de hacer clic en el hipervínculo. Por ejemplo, si alguien falsificara un sitio, por ejemplo, www.google.com, este podría aparecer como www.lygoogle.com en la barra de direcciones luego de hacer clic en el enlace. La idea es replicar el sitio, por lo tanto, no basta con mirar el contenido del sitio en la pantalla para poder determinar que es falso. La mejor forma de evitar esto es escribiendo directamente el sitio web en la barra de direcciones en vez de hacer clic en cualquier enlace que probablemente podría estar robándole información.

CÓMO LOS LADRONES DE IDENTIDAD USAN SU INFORMACIÓN

Los ladrones de identidad usarán su información personal de varias formas. Los ladrones pueden hacer lo siguiente:

- Usar sus números de tarjetas de crédito y débito existentes para comprar mercadería y luego revenderla fácilmente.
- Abrir cuentas de crédito nuevas. Usar las cuentas y no pagar las facturas, sin embargo, las cuentas del delincuente aparecerán en su informe de crédito.
- Establecer un servicio telefónico o inalámbrico a su nombre.
- Abrir cuentas bancarias y girar cheques sin fondo.
- Pedir préstamos y comprar bienes de consumo, por ejemplo, un vehículo a su nombre.

CÓMO PROTEGERSE

Casi todos somos vulnerables al robo de identidad ya que hay mucha información disponible para todos. Si alguna vez solicitó una tarjeta de crédito, una línea de crédito o un préstamo, si fue a la universidad o tuvo un trabajo, si tuvo una cuenta de ahorro o cuenta corriente o si tuvo seguro médico con un empleador, usted está en riesgo.

Puede minimizar su riesgo mediante una gestión minuciosa de su información personal y siendo consciente del problema de manera continua. Hay muchas formas de protegerse del robo de identidad:

Su número de Seguro Social: la llave al castillo

- No lleve consigo su número de Seguro Social.
- Mantenga su tarjeta de Seguro Social en un lugar seguro, por ejemplo, la caja fuerte de su casa.
- Brinde su número de Seguro Social solo cuando sea absolutamente necesario (por ejemplo, si su empleador lo necesita para declarar el salario y los impuestos).
- Controle cada año su declaración de beneficios e ingresos del Seguro Social para prevenir fraudes.
- Nunca escriba el número de Seguro Social en los cheques.
- Haga las siguientes preguntas si alguien le solicita su número de Seguro Social (las respuestas que reciba lo ayudarán a determinar si sigue negociando con dicha persona):
  - ¿Para qué lo necesita?
  - ¿Cómo lo usará?
  - ¿Cómo lo protegerá contra un posible robo?
  - ¿Qué sucede si no se lo doy?
  - ¿Qué ley me obliga que le dé mi número de Seguro Social?

Contraseñas: que sean impenetrables

- Sea inteligente al elegir una contraseña. No use información que se identifique fácilmente, por ejemplo: el nombre de soltera de su madre, su dirección, fecha de nacimiento o número telefónico. Los expertos dicen que para crear una contraseña fuerte debe seguir los siguientes criterios:
  - Que tenga por lo menos ocho caracteres.
  - Que sea significativamente distinta de las contraseñas anteriores.
  - Que contenga una combinación de letras en minúscula y mayúscula, números y caracteres.
  - Que no contenga una palabra completa.
  - Que no contenga su nombre de usuario o nombre real.
- Guarde sus contraseñas en un lugar seguro, por ejemplo, en una caja fuerte de la casa. No las escriba ni las lleve consigo.

Tecnología: esté alerta

- Pague sus cuentas en línea. Las probabilidades de robo de identidad son menores cuando paga sus cuentas en línea que cuando las paga en un lugar físico.
- Actualice el software de protección de virus de forma periódica en la computadora de su casa.
- Evite usar la función de inicio de sesión automático que ofrecen los servicios en línea en los que se guarda el nombre de usuario y la contraseña.
- Lea las políticas de privacidad.
- Use un buscador seguro para proteger la privacidad de sus transacciones en línea.
- No descargue los archivos de extraños ni haga clic en hipervínculos de personas que no conoce. Si recibe un correo electrónico de un amigo con solo un enlace o si algo le parece extraño, comuníquese con su amigo antes de hacer clic en algo o de ingresar cualquier información personal en el correo electrónico ya que podría haber sido hackeado.
- Evite usar la función de inicio de sesión automático que se ofrece para los servicios en línea.
- Coloque un código de contraseña en su teléfono inteligente.

En la casa: gestione su información personal

- Compre una trituradora de corte cruzado y destruya facturas, ofertas de crédito preaprobados y demás documentos con información personal.
- No deje información personal a plena vista en lugares donde las personas que viven con usted, sus parientes o empleados externos puedan verla.
- Manténgase al tanto de sus finanzas, especialmente de las fechas de vencimiento de las facturas.

- Informe cualquier cargo discutible en sus facturas.
- No ponga su número de tarjeta de crédito o número de cuenta en los cheques cuando pague sus facturas por correo.
- Firme y active de inmediato las tarjetas de crédito nuevas. Corte y deseche las tarjetas de crédito vencidas.
- Proteja su correo. Si es posible, lleve todo el correo saliente a la oficina postal o a un buzón del servicio postal azul que sea oficial.
- Si es posible, proteja la basura guardando los cestos de basura en un área cerrada.
- Haga una copia de todas sus tarjetas personales, financieras, del seguro y de identificación que lleva en la billetera y guárdelas en un lugar seguro en su casa.
- Solicite un informe de crédito una vez al año de cada una de las principales oficinas de informe de crédito, Equifax, Experian y TransUnion, a fin de verificar que la información sea exacta.
- Revise los estados financieros periódicamente y cierre cualquier cuenta que no use.

Cuando salga

- Lleve solo la información que realmente necesite. Deshágase de cualquier información innecesaria que esté en su billetera y que lo identifique.
- Cuide siempre su tarjeta del cajero automático, su número de identificación personal (PIN) y los comprobantes del cajero.

En el trabajo: Ponga en práctica la seguridad y cuestione todo.

- Si viaja por negocios y usa su computadora portátil cuando está en la habitación del hotel, apáguela al salir de la habitación.
- Fije una pantalla de privacidad a su computadora portátil para evitar los ojos fisgones de aquellos que se sientan a su lado.
- Desconecte siempre la Internet inalámbrica en su computadora portátil cuando no la use. Esta medida puede disuadir a los "gemelos malvados", que simulan ser puntos de acceso y que envían señales fuertes para robar contraseñas e información personal.

En resumen, asegúrese de proteger lo que puede controlar de la mejor manera posible. El mejor ataque es una buena defensa. Esté atento al robo de identidad, controle de cerca su información y denuncie de inmediato cualquier actividad sospechosa.

¿ES USTED VÍCTIMA DEL ROBO DE IDENTIDAD?

A veces se puede enterar de que ha sido víctima de robo de identidad en el momento más inoportuno. Por ejemplo, una oportunidad laboral perdida, un rechazo de préstamo o incluso un arresto pueden ser la primera pista de que ha sido víctima de robo de identidad.

Algunas de las formas más comunes de saber si es víctima son:

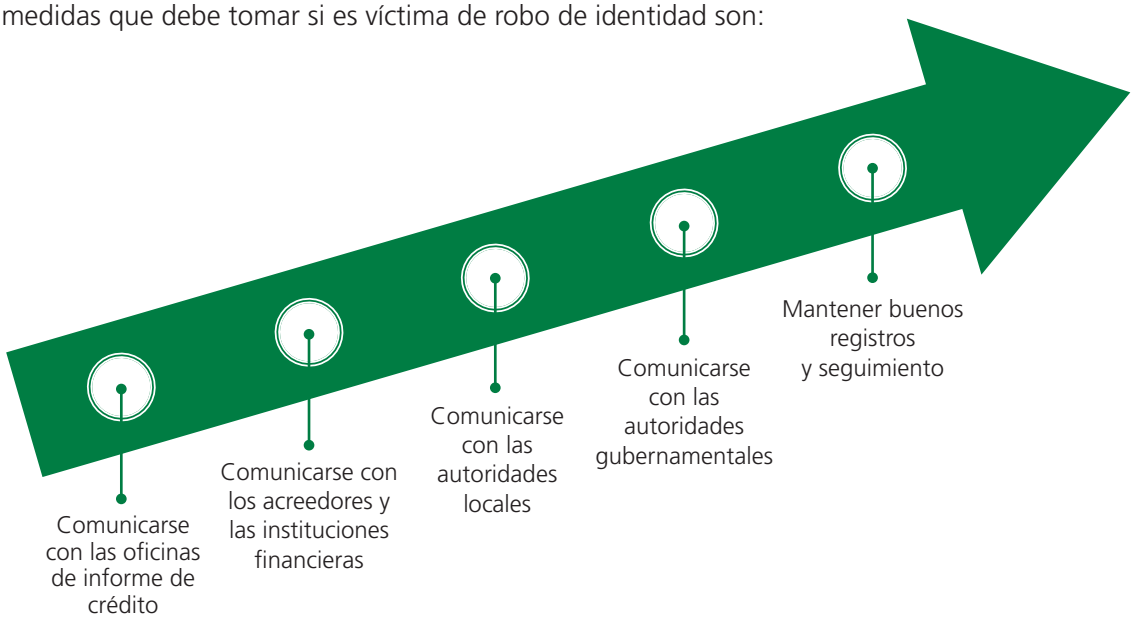
- Percatarse de cobros o retiros inexplicables de su cuenta corriente o de ahorros
- No recibir facturas u otro correo, lo cual puede indicar que un ladrón hizo un cambio de dirección y su correo ahora se envía a la dirección designada por el ladrón.
- Recibir tarjetas de crédito que no solicitó.
- No ser aceptado para un crédito sin motivo aparente.
- Recibir llamadas de cobro de acreedores y cobradores de deudas por facturas que no son suyas.
- Encontrar imprecisiones en sus informes de créditos que no son resultado de error humano.

Un ladrón robó una solicitud de préstamo hipotecario de la cartera de una consultora que asistía a una feria comercial. La consultora había estado completando la solicitud durante el tiempo libre de la feria comercial y luego de terminarla, el ladrón se la arrebató.

TOME MEDIDAS SI ROBAN SU IDENTIDAD

Si fue víctima de robo de identidad, debe averiguar cuántos de sus registros están en peligro. Algunos de los lugares donde se encuentran sus registros son más comunes que otros. Las bases de datos más conocidas son: Las oficinas de informe de crédito, la policía local y estatal y la división de vehículos automotores. También es posible que su información personal aparezca en las listas de vigilancia federal debido a la actividad delictiva del robo de identidad, en las listas de actividades bancarias fraudulentas o en direcciones desconocidas asociadas a su número de Seguro Social.

Si usted es víctima de robo de identidad, actúe rápidamente y restablezca su buen nombre. Las medidas que debe tomar si es víctima de robo de identidad son:



PASO 1: Comunicarse con las oficinas de informe de crédito	• Solicitar a las oficinas de informe de crédito, Equifax, Experian y TransUnion, que coloquen una alerta de fraude en su informe de crédito. • Revisar sus informes de créditos minuciosamente. • Extender la alerta de fraude más allá de los 90 días estándar a siete años escribiendo a cada una de las agencias e incluyendo una copia del informe policial que presentó.
PASO 2: Comunicarse con los acreedores y las instituciones financieras	• Cerrar cualquier cuenta que haya sido manipulada o abierta en forma fraudulenta. • Pedir a la empresa el formulario de disputas de fraudes, en caso de que esté disputando imprecisiones en sus cuentas existentes.

PASO 2: Comunicarse con acreedores e instituciones financieras (continuación)	• Si robaron sus cheques o si los usaron indebidamente, suspenda el pago de cualquier cheque pendiente. • Cree nuevos números de identificación personal (PIN) para sus cuentas nuevas y guárdelos en un lugar seguro.
PASO 3: Comunicarse con las autoridades locales	• Presente un informe policial ante el departamento de policía local donde ocurrió el robo de identidad.
PASO 4: Comunicarse con las autoridades gubernamentales	• Comisión Federal de Comercio (FTC, por sus siglas en inglés): Presente una queja comunicándose con la Línea directa de robo de identidad: *www.ftc.gov*. • Administración de Seguro Social (SSA, por sus siglas en inglés): Si aparentemente alguien está usando o usó su número de Seguro Social. • Servicio postal de los EE. UU.: Si se está adulterando o robando su correo. • Comuníquese con el Departamento estatal de Vehículos Automotores para denunciar la perdida de la licencia de conducir.
PASO 5: Mantener buenos registros y seguimiento	• Documente todas sus acciones, incluyendo el tiempo y dinero que dedicó para arreglar el problema de su identidad. En algunos estados, cualquier persona que sea hallada culpable de robo de identidad financiera deberá pagar un resarcimiento a la víctima de cualquier pérdida financiera, incluidos los salarios perdidos. • Guarde copias de la correspondencia y de los documentos relacionados con el robo y anote todas las llamadas telefónicas, incluidas la fecha y la hora de su llamada y el nombre y cargo de la persona que lo ayudó. • Haga el seguimiento por escrito de todas las llamadas telefónicas. • Obtenga nuevamente una copia de su informe de crédito en unos meses para verificar que se hayan hecho sus correcciones y modificaciones y para corroborar que no haya ocurrido una nueva actividad fraudulenta.

Afortunadamente, hay medidas que se pueden tomar ante el robo de identidad. Si usted gestiona su información personal con cautela y en forma continua, puede protegerse del robo de identidad en el futuro.

A un consumidor muy cauto le robaron la identidad y no tenía idea de lo que le había sucedido. Siempre trituraba los documentos antes de desecharlos. Entregaba su correo saliente en la oficina postal. Aun así, cuando controló su informe de crédito, se encontró con $15,000 por cobros no autorizados en las tarjetas de crédito que no usaba habitualmente. Por eso es importante revisar de manera periódica los resúmenes mensuales de los acreedores y sus informes de crédito para corroborar que no haya imprecisiones.

Robo de identidad y las leyes que lo protegen

La resolución de los problemas que ocurren por el robo de identidad puede llevar mucho tiempo y ser frustrantes. Según la ley federal, hay protecciones para corregir informes de crédito y errores de facturación. También hay una ley federal que lo protege para no ser contactado por cobradores por deudas que no son suyas. También se han promulgado leyes federales específicamente dirigidas contra el robo de identidad.

Ley de Transacciones de Crédito Justas y Correctas (FACT, por sus siglas en inglés) de 2003

- Esta ley le da a todo consumidor el derecho a acceder a su informe de crédito cada año en forma gratuita.
- Exige a los comerciantes que retiren los cinco últimos dígitos de un número de tarjeta de crédito de los comprobantes de la tienda.
- Crea y establece un sistema nacional de detección de fraudes y alerta a los consumidores.
- Crea una Norma de eliminación según la cual toda persona que mantenga o posea de otra forma información del consumidor para un fin comercial debe destruirla correctamente antes de eliminarla.

Ley de Disuasión del Uso y Robo de Identidad de 1998

- Esta ley federal establece que es un delito federal transferir o usar el medio de identificación de otra persona sin un motivo legítimo y con intención de cometer un delito.

Ley de Aumento de Sanciones por el Robo de Identidad

- Esta ley determina penas mayores para los ladrones de identidad.
- Crea el delito de "robo de identidad agravado" que se castiga con hasta dos años de presión cuando se comete en relación con otros delitos.

Ley de Facturación Justa de Crédito

- Esta ley le otorga derechos particulares cuando se trata de errores de facturación.

Ley de Transferencia Electrónica de Fondos

- Esta ley establece procedimientos para resolver errores en los estados de cuenta con las transferencias electrónica de fondos.

Ley de Informes de Crédito Justos

- Esta ley está diseñada para promover la precisión, equidad y privacidad de la información en los expedientes de cada Agencia de Informe del Consumidor (CRA), cuya forma más común es la oficina de informe de crédito.

Ninguna ley federal limita sus pérdidas si alguien roba sus cheques y falsifica su firma. No obstante, una ley estatal podría protegerlo. Comuníquese con su banco estatal o con su agencia de protección del consumidor para obtener más información.

CONTROL DE SU CRÉDITO PARA NO SER VÍCTIMA

El control de su crédito debe ser un componente clave de su plan financiero personal.

Es importante que entienda la información de su informe de crédito, independientemente de su situación financiera. Esta información afecta directamente su capacidad de obtener una tarjeta de crédito, comprar un automóvil o una vivienda, alquilar un departamento o incluso conseguir un trabajo nuevo. Dos de las mejores razones para revisar su informe de crédito hoy es asegurarse de que su informe de crédito sea exacto y protegerse de fraude o robo de identidad.

Puede crear su propio sistema de monitoreo continuo y gratuito obteniendo uno de sus informes de crédito gratuitos cada cuatro meses.

Por ejemplo:

1. En enero, solicite su informe de Experian de *annualcreditreport.com*.
2. Luego en mayo solicite su informe de TransUnion.
3. Finalmente, en septiembre, solicite su informe de Equifax antes de comenzar nuevamente el proceso en enero.

Como las tres oficinas tienen la misma información, usted podrá monitorear la actividad en sus informes de crédito e identificar los puntos discutibles.

OFICINAS DE CRÉDITO				
Para solicitar su informe de crédito:	teléfono:	Sitio web:	Domicilio:	Para informar fraude, llame a:
Experian	888-EXPERIAN	www.experian.com	PO Box 9532 Allen, TX 75013	888-EXPERIAN
TransUnion	800-916-8800	www.transunion.com	PO Box 1000 Chester, PA 19022	800-680-7289
Equifax	800-685-1111	www.equifax.com	PO Box 74024 Atlanta, GA 30374	800-525-6285

Cuando se trata de su información personal, las palabras precaución y prudencia están a la orden del día.

Un viajero de negocios se registró en un hotel y usó su tarjeta de crédito personal por error. No se dio cuenta del error sino hasta después de que el empleado había pasado su tarjeta e impreso el número de cuenta completo. Entonces su tarjeta se procesó para pagar la estadía del hotel. En los cinco días siguientes, se compró más de $1,500 de mercadería en forma fraudulenta con su tarjeta de crédito personal. El fraude fue descubierto por el emisor de la tarjeta de crédito, quien identificó actividad no habitual en la tarjeta y la canceló. Es importante verificar que cualquier documento que tenga un número de tarjeta de crédito completo o número de cuenta termine en una trituradora y no se deje a la vista de cualquier persona.

NOTAS

NOTAS

36500 Corporate Drive
Farmington Hills, MI 48331
248-553-5400 fax: 248-553-8970
www.greenpath.org

GreenPath™ financial wellness

Accel™ members financial counseling

Search *greenpath*