Cómo proteger su identidad

Resguarde su identidad aplicando algunas prácticas de seguridad en línea y limitando el acceso a su información personal.

El robo de identidad ocurre cuando alguien roba su información personal, o identidad, para cometer fraude. Esto puede incluir información como su nombre, número de Seguro Social, tarjetas de crédito o información de su cuenta bancaria. Los ladrones pueden utilizar este tipo de información para alquilar apartamentos, obtener préstamos, abrir cuentas en su nombre, o poner cargos en sus cuentas, sin su permiso.

El robo de identidad, el fraude y la extracción de datos afectan cada año a decenas de millones de personas en los Estados Unidos. Es por ello que es importante ser muy cauteloso con su información de identificación, tanto en línea, como en el mundo real.

REVISE SU INFORME DE CRÉDITO

Cada año revise su informe de crédito de cada una de las tres compañías nacionales de informes de crédito (Equifax, Experian y TransUnion) en el sitio web gratuito **annualcreditreport.com** (En inglés). Si ve algo incorrecto o sospechoso en su informe, comuníquese inmediatamente con la compañía de informes de crédito y con la compañía que proporcionó dicha información. Si le preocupa algún robo de identidad que haya sufrido en el pasado, o que pueda ocurrir en el futuro cercano, podría congelar o colocar una alerta de fraude en su expediente de crédito. Para obtener más información, vea el Módulo 7: "Cómo comprender los informes y puntajes de crédito".

También puede socilitar ser excluido o "opt out" de recibir ofertas de crédito o seguros, también conocidas como ofertas "prescreened" o preverificadas. Esto puede prevenir que ofertas de seguros o créditos, dirigidas a usted, caigan en manos de extraños. Las mismas podrían ser luego utilizadas para sacar préstamos fraudulentos en su nombre. Excluya su nombre de cualquier oferta preverificada, tomando la opción "opt out" por teléfono llamando al (888) 567-8688, o en línea en **optoutprescreen.com** (En inglés). Elija ser excluido por cinco años de las ofertas preverificadas tomando la opción de "5 años", o haga su solicitud por correo para ser permanentemente excluido de éstas. Aunque usted haya optado por no recibir ofertas, aún podrá solicitar crédito cuando quiera comunicándose directamente con el prestamista, o en línea.

LIMITE EL ACCESO A SU INFORMACIÓN

No lleve su tarjeta, ni el número del Seguro Social en su cartera o bolso; guárdelos en un lugar seguro en casa.

Excluya su nombre de muchas listas de correo de mercadeo directo, registrándose en la página de la Direct Marketing Asociation (Asociación Nacional de Mercadeo Directo), utilizando la forma disponible en **dmachoice.thedma.org** (En inglés). Esto reducirá los chances de que ladrones puedan robar su información.

Excluya su nombre permanentemente de la mayoría de las listas de telemercadeo registrando su número de teléfono celular o residencial en el "Do Not Call Registry" o "Registro No Llamar", llamando al (888) 382-1222 o visitando **donotcall.gov**.

Nunca entregue su información personal a alguien que llame y se la pida, aun cuando la persona diga que llama de su institución financiera. Si desea confirmar que la llamada es auténtica, cuelgue y llame a dicha entidad financiera, a un número de teléfono en el que confíe, como el que aparece en su estado de cuenta o en el reverso de su tarjeta de crédito.

Use una trituradora de papel, tijeras, o sus manos para destruir todos los papeles que contengan información de identificación o números de cuentas, antes de tirarlos a la basura. También corte las tarjetas de crédito o débito viejas o canceladas.

Proporcione su número de Seguro Social sólo cuando sea absolutamente necesario. A menudo, cuando alguien se lo pide, usted no está obligado a darlo.

Proteja cierta información como el apellido de soltera de su madre, que a menudo se usa para verificar su identidad con las instituciones financieras. Sea cauteloso acerca de dónde pueda aparecer en internet, no lo comparta en las redes sociales.

PRACTIQUE LA SEGURIDAD EN LÍNEA

Hay muchas cosas que puede hacer para proteger su información personal en línea.

Memorice todas sus contraseñas. Nunca las anote ni las lleve consigo (¡Ni siquiera en un pedazo de papel pegado a su computadora!).

Asegúrese de que las contraseñas sean largas e incluyan mayúsculas, minúsculas y números. No incluya palabras que se puedan encontrar en un diccionario, o nombres y fechas que puedan ser asociados a usted (Nombres y fechas de nacimiento de sus hijos, por ejemplo).

Lo más recomendable es tener una clave diferente para cada cuenta. Si le resulta muy difícil recordar tantas contraseñas, cree contraseñas separadas, que sean más largas, y difíciles de adivinar, para sus cuentas financieras.

No entregue su información financiera, ni personal en la Internet, a menos que usted sea el que haya iniciado el contacto, o conozca con certeza con quién está tratando.

Tampoco comparta información de identidad en línea, a menos que el sitio esté protegido con algún programa de codificación, y así nadie pueda interceptarla. **La dirección de un sitio web seguro debe comenzar con "https", nunca "http"**. También tendrá el símbolo de un candado (🔒). Un sitio web seguro no es necesariamente un sitio legítimo. No baje la guardia solo porque aparezcan "https" y el símbolo del candado.

No utilice una red Wi-Fi pública cuando envíe información personal o financiera. Si utiliza una computadora pública, como en la biblioteca, nunca le dé permiso al navegador para que guarde su contraseña, cierre siempre la sesión de cualquier sitio web en el que haya ingresado, y cierre el navegador antes de retirarse de la computadora.

Proteja su teléfono y tableta con contraseña. Muchas personas utilizan aplicaciones en sus aparatos móviles que guardan sus contraseñas para iniciar automáticamente las sesiones, dando así acceso fácil a los ladrones a su información personal. Una contraseña sirve para garantizar que nadie pueda acceder a la información confidencial que esté almacenada en su dispositivo y usarla para entrar en su cuenta bancaria o tarjeta de crédito.

No responda correos electrónicos donde le soliciten información personal bancaria. ¡Aún si el mensaje tiene el logotipo de una compañía! **Las instituciones financieras nunca le solicitarán información personal en un correos electrónico**.