• Cuando haga compras en línea, busque vendedores minoristas en línea reconocidos o sitios que otras personas hayan usado a su satisfacción. Observe el ángulo inferior derecho de la ventana del explorador. Si ve una imagen pequeña de un candado, se encuentra en un sitio seguro. Si no la ve, busque otro comercio en línea para realizar su compra. Asimismo, verifique las políticas de privacidad del sitio. Aléjese de sitios que no declaran, específicamente, que no darán a conocer su información a otras empresas.

• Proteja su información personal cuando llene formularios de cualquier tipo. Pregunte a los empleados o a otra persona si es absolutamente necesario proveer información como el número del seguro social o de la licencia de conducir. Toda persona que exija el número de su seguro social, por ejemplo, la compañía de seguros, debe explicarle la política de privacidad de la empresa y cómo mantendrán la seguridad de la información.

• Si recibe mensajes de correo desconocidos, puede ser de alguien que busca aleatoriamente suplantar la identidad ("phishing") de posibles víctimas de este delito. No abra ni haga clic en ninguna parte del mensaje del correo electrónico; solo use el botón Eliminar para borrar el mensaje y luego vacíe la papelera del correo.

• Para disminuir las llamadas de ventas no deseadas, inscríbase en el National Do Not Call Registry (Registro Nacional No Llame).

El sitio web es **www.donotcall.gov.** Si no usa Internet, puede registrarse por teléfono, llamando al 1-888-382-1222. Los teléfonos móviles también se pueden registrar. Usted permanecerá en la lista No Llame hasta que solicite que lo eliminen.

• Todos los años solicite los informes de créditos gratuitos y verifique si existió alguna actividad sospechosa. Si encuentra algo sospechoso, avise de inmediato a la empresa de la tarjeta de crédito o al acreedor.

Si alguien ya está usando su identidad

Comuníquese con el departamento de fraudes de cualquiera de las tres oficinas de referencias de créditos (credit bureaus) e infórmeles. (A su vez, ellos informarán a las otras dos). Solicite que se coloque una "alerta de fraude" en su expediente, junto con una nota donde se solicite a los acreedores que lo llamen antes de abrir nuevas cuentas o cambiar las existentes.

Equifax: 1-800-525-6285
Experian: 1-888-397-3742
TransUnion: 1-800-680-7289

Asegúrese de buscar más información sobre robo de identidad y otros enlaces en **www.ct.gov/dcp.** Busque "identidad".

State of Connecticut
Department of Consumer Protection
165 Capitol Avenue
Hartford, CT 06106

Número de teléfono gratuito:
1-800-842-2649

www.ct.gov/dcp

Department of
CONSUMER PROTECTION

FOLLETO INFORMATIVO

Proteja su buen nombre

¡Protéjase del robo de identidad!

ESTADO DE CONNECTICUT

Departamento de Protección del Consumidor

El robo de identidad está en auge

Se estima que cada año, 10 millones de estadounidenses son víctimas del robo de identidad.

Esto incluye una cantidad de distintos delitos contra la privacidad, que incluyen el robo del número del seguro social, de tarjetas de débito o crédito, y hasta de tarjetas para llamar por teléfono.

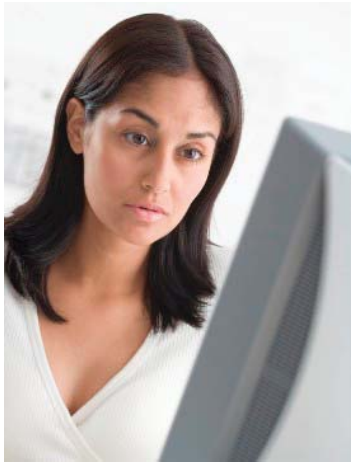
Proteger totalmente su identidad es casi imposible. No obstante, es útil saber cómo se puede poner en riesgo la propia identidad. Algunas medidas simples pueden ser de utilidad para usted.

Cómo puede suceder

Una gran parte del robo de identidad todavía se produce como perjuicios favorecidos por la oportunidad, y los ladrones cambian constantemente sus trampas.

Obviamente, Internet abrió nuevas oportunidades para el robo al permitir que los ladrones envíen datos robados desde y hacia cualquier lugar en el mundo, como también que los recuperen.

En las estafas populares participan prestamistas falsos que tientan con tasas muy bajas a solicitantes que no vacilan en dar sus datos personales.



Para otras estafas se usan llamadas por teléfono o mensajes de correo electrónico que el delincuente realiza en nombre de un banco o un organismo de gobierno, y pide a quien los recibe que verifique y provea la información de una una cuenta.

Una cartera perdida o robada que contenga una tarjeta de seguro social permite que el delincuente rápidamente abra cuentas bancarias y de ahorros ficticias, y hasta solicite una tarjeta de crédito. A partir de allí, el timador no demorará en gastar el máximo permitido en la tarjeta.

Maneras de protegerse

No existe una protección que garantice totalmente que usted nunca será víctima de alguna forma de robo de identidad. No obstante, puede tomar medidas para proteger su privacidad, muchas de las cuales son bastante simples.

• Destruya los registros y estados de cuenta privados. Rompa o destruya estados de cuenta de las tarjetas de crédito, solicitudes u otros documentos que contengan información financiera privada.

• Vacíe rápidamente su buzón de correo, para que nadie tenga la oportunidad de robar su correo. No deje correo para retirar en el buzón (por ejemplo, facturas pagadas que incluyan números de cuenta), para evitar que cualquier transeúnte lo tome. Coloque el correo para enviar en un buzón del U.S. Postal Service (Servicio Postal de EE. UU.).

• No lleve siempre la tarjeta del seguro social. Llévela solo cuando vaya a necesitarla. Lo mismo se aplica a las tarjetas de Medicare y Medicaid. Déjelas en un lugar seguro cuando no necesite usarlas.

• No escriba el número de seguridad social en sus cheques. Como regla general, tampoco incluya en los cheques el número de la licencia de conducir.

• Nunca deje los recibos del cajero automático (ATM) o de la tarjeta de crédito cuando retire efectivo o haga una compra.

• En lo posible, pague en efectivo. Si paga con tarjeta, preste atención a qué hacen los empleados y meseros con ella cuando registran su compra.