BUREAU OF CONSUMER PROTECTION Consumer Facts

Protecting Wisconsin Consumers for 75 Years

Resguardar su información

Cuatro maneras básicas para proteger su información personal y reducir el riesgo del robo de identidad:

- Sepa con quién está compartiendo información.
- Guarde y elimine su información de una manera segura.
- Haga preguntas antes de decidir compartir su información personal.
- Mantenga seguridad apropiada en su computadora y otros dispositivos electrónicos.

Además, los pasos en seguido pueden ayudarle a proteger su identidad:

- **Resguarde su número de seguro social –** No mantenga su tarjeta de Seguro Social con usted y no utilice su número de seguro social como clave o contraseña a menos que la institución financiera, negocio u otra compañía con la que esté tratando se lo requiera en absoluto. Ya que las tarje tas de medícate también usan su número de seguro social como número de identifaciòn de seguro, so lo lleve su tarjeta de medicare cuando seci necesario.

- **Triture, triture, triture –** Invierta en un triturador de papeles – un modelo barato es suficiente – y úselo. Triture facturas, recibos y estados de cuenta. Destruya las etiquetas en las botellas de prescripción antes de tirarlas. También triture cualquier otro papel que contenga información personal o financiera, tarjeta de crédito o oferta de seguro, y que usted no desea guardar.

- **Proteja su correo –** Si usted se va de casa aunque sea por unos días, pídale a un vecino, amigo o familiar que le recoja el correo o pídale a la oficina de correo local que mantenga su correo hasta que usted vuelva. Cuando envíe algo por correo, especialmente si contiene un cheque u otra documentación personal, mándelo desde algún lugar seguro – en lugar de dejárselo a un cartero o peor, a un ladrón de identidad. Si usted está comprando cheques de su institución financiera, recogalos en persona en vez de que se los envíen.

- **No comparta su información –** Los ladrones de identidad obtienen mucha información simplemente preguntándonos qué quieren. Se comunican con nosotros por teléfono, correo electrónico, o correo postal haciéndose pasar por nuestro propio banco, compañía de crédito o incluso el IRS. Nos piden que “verifiquemos” información como nuestros números de cuentas, de seguro social o claves. Las compañías o agencias legítimas no hacen esto, por lo que si le piden esta información, lo más probable es que sea un ladrón de identidad. Nunca dé su información personal a menos que usted sea el que haya iniciado la comunicación.

- **No comparta demasiada información en los redes sociales –** Si publica demasiada información personal, un ladrón de identidad puede encontrar información sobre su vida, usarla para contestar preguntas de seguridad en sus cuentas, y acceder su dinero e información personal. Considere limitar el

número de personas que pueden acceder su página de red social a un grupo chico. Nunca publique su nombre completo, número de seguro social, fecha de nacimiento, dirección, número de teléfono o número de cuenta en los sitios de acceso público.

- **Active autenticación de dos factores si se le ofrece –** La autenticación de dos factores es una capa adicional de seguridad que combina algo que tienes, un testigo físico, como una tarjeta o un código, con algo que sabe, algo memorizado, tal como un número de identificación personal (PIN) o una contraseña.

- **Ponga un fin a las ofertas de tarjetas de crédito pre-aprobadas –** A menos que usted esté realmente comprado una tarjeta de crédito, ponga un fin a las ofertas de tarjetas de crédito pre-aprobadas. Son muy fáciles de encontrar en su buzón y pueden ser fácilmente utilizadas por los ladrones de identidad para obtener una tarjeta de crédito en su nombre. Usted puede pedir que remuevan su nombre de las listas de mercadeo de las agencias calificadoras de crédito llamando al número gratuito 1-888-5OPTOUT (888-567-8688) o visitando el sitio www.optputprescreen.com.

- **Verifique sus facturas y estados de cuentas –** Si un ladrón de identidad ataca, es posible que primero lo note en su facturas o estados de cuenta bancarios. Si puede, lo mejor es revisar sus estados de cuenta bancarios y facturas en línea, donde la mayoría de las transacciones son visibles dentro de unos días. Controle sus facturas y estados de cuenta bancarios por cargos no autorizados tan pronto como lleguen. Informe cualquier problema tan pronto como sea posible. Si su factura o estado de cuenta no llega a la hora normal, llame y pregunte al respecto; ya que llegar tarde podría ser otra indicación de robo de identidad.

- **Preste atención a la seguridad en el Internet –**Asegúrese de tener la seguridad a de cuada en su computadora. Installe un firewall, antivirus y protección contra spyware. Elija sus contraseñas con cuidado y hágalas únicas. Los expertos recomiendan utilizar una contraseña que tiene por lo menos ocho caracteres, con una mezcla de números, símbolos y letras mayúsculas y minúsculas. No haga “clic” en las ventanas emergentes ni abra correos electrónicos y archivos adjuntos de personas que usted no reconoce ni confía. Tenga cuidado con los correos electrónicos de phishing de compañías que se nacen pasar por compañías legitimas. Verifique las preferencias de seguridad de su navegador para asegurarse de que no estén a un nivel mínimo. Además, verifique si el sitio Web es seguro. Por lo general, “https” y/o candados pequeños en la esquina de abajo a la derecha significan que el sitio es seguro.

- **Lea las declaraciones de privacidad –** En la era de la información, hay un gran mercado de información personal. Algunas de las compañías con las que hacemos negocios comparten o incluso venden su información personal a otros. Antes de comprar en línea, lea la política de privacidad de la empresa. También, lea la declaración de privacidad que la compañía de tarjeta de crédito le envía. En algunos casos, podría impedir que la compañía comparta toda o parte de su información simplemente contactándolos.

- **Revise su informe de crédito con frecuencia –**Obtenga su informe de crédito gratis de cada una de las tres agencias principales de informes de créditos cada ano. Los informes de crédito contienen una amplia cantidad de información sobre la historia financiera de los consumidores, y revisarlos con frecuencia es una de las mejores maneras de protegerse contra el robo de identidad. Si usted encuentra en su informe una cuenta bancaria o de tarjeta de crédito que usted piensa que no es suya, podría significar que un ladrón de identidad las ha abierto en su nombre. Usted puede obtener una copia gratuita de su informe de crédito de Equifax, Experian, y TransUnion llamando al número gratuito 1-877-322-8228 o por Internet al www.annualcreditreport.com/cra/index.jsp.

- **Elimine su información personal de una manera segura –** Antes de tirar una computadora, borra toda la información personal que contenga. Utilice un programa de limpieza para borrar todo el contenido del disco duro. Antes de tirar un dispositivo móvil, revise el manual, el sitio web del proveedor de servicio, o el sitio web del fabricante del dispositivo para información sobre como borrar permanentemente su información, y como guardar o transferir información a un nuevo dispositivo. Saca el módulo de identidad del suscriptor (Tarjeta de SIM) del dispositivo móvil. Borre el directorio de contactos, lista de llamadas hechas y recibidas, mensajes de voz y texto hechos y recibidos, carpetas de organización, historia de búsqueda de internet, y las fotos.

Para obtener más información, o para presentar una queja, visite nuestra página web o contacte al Departamento de Protección al Consumidor.

Departamento de Protección al Consumidor
2811 Agriculture Drive
PO Box 8911
Madison WI 53708-8911

E-MAIL: DATCPWisconsinPrivacy@wi.gov

WEBSITE: datcp.wi.gov

(800) 422-7128

FAX: (608) 224-4677

TTY: (608) 224-5058

I:\dtcp\common\Fact Sheets\IDTheftSafeguardsSPANISH626 02/19-G