

W I S C O N S I N

# Office of Privacy Protection

*Safeguarding Information for Your Future*

## Protección al Robo de Identidad Diez consejos útiles para mantenerte Seguro en la Escuela

### **Protege tu número de Seguro Social**

No cargues con tu Tarjeta de Seguro Social y no uses el número como NIP (Número de Identificación Personal) ó como código de acceso al menos de que tu Institución Financiera u otro negocio lo requiera.

### **Protege tu Correo**

Cuando envíes algo por correo, particularmente si envías un cheque ó cualquier otra información personal, envíala desde un lugar seguro – no lo pongas en un buzón de correo que esté abierto. Si ordenaste cheques a tu Institución Financiera ó Banco, será mejor que los recogas en sus oficinas en lugar de pedir que te los manden por correo. Finalmente, mantén seguro el correo que recibes hasta que lo puedas triturar.

### **Detén las ofertas de Crédito pre-aprobadas.**

Al menos de que relamente estés buscando obtener una tarjeta de Crédito, el mejor que pongas un alto a las ofertas de tarjetas de crédito preaprobadas. Estas llegan a tu buzón y pueden ser usadas facilmente por ladrones de identidad con el fin de obtener una Tarjeta en tu nombre. Puedes pedir que tu nombre sea removido de las listas de oficinas de crédito de mercadeo llamando gratis al: 1-888-5OPTOUT (888-567-8688) ó visitando su página de internet: [www.optoutprescreen.com](http://www.optoutprescreen.com).

### **Solicita un Estado de cuenta de tu Seguro Social.**

La Administración del Seguro Social, envía anualmente un estado de cuenta para todos los ciudadanos estadounidenses que cuentan con una tarjeta y que han sido empleados y despues de que haya cumplido 25 años de edad. Hasta ese momento, no recibirá un estado de cuenta al menos de que usted lo solicite. Si sospecha que ha sido victima de robo de identidad o algo ha ocurrido con su número de seguro social, puede solicitar un estado de cuenta de seguro social antes de que haya cumplido 25 años. Revise el estado de cuenta para que se asegure de que los totales de su sueldo e información personal es correcta y reporta en caso de que haya alguna inconsistencia. Solicite un estado de cuenta al 1-(800)772-1213 ó en la página de internet: [www.socialsecurity.gov](http://www.socialsecurity.gov).

### **Tritura, tritura, tritura**

Invierte en una trituradora – un modelo sencillo que normalmente no son caros te podrá servir, úsalo. Tritura los estados de cuenta, los recibos, y las ofertas de Tarjeta de crédito que normalmente tirabas a la basura. También tritura cualquier otro documento que contenga información personal o financiera, como estados de cuenta bancarios que no guardas.

### **Toma en cuenta lo que estás bajando en tu computadora.**

Todo lo que bajas en tu computadora tiene un riesgo. Virus, “spyware” y otros programas de computación pueden estar dentro de lo que bajas. Al menos de que realmente estés seguro de lo que estás bajando y la fuente de esa información, no lo hagas, particularmente si lo que vas a bajar es gratis.

### **Ten cuidado con los Foros (bloggs)**

Nunca incluyas ninguna información personal que te pueda identificar, más que tu nombre sin apellidos. Esto incluye tu fecha de nacimiento, tu dirección, y número de teléfono.

### **Asegúrate de tener siempre un buen programa de seguridad y actualízalo frecuentemente.**

Con el fin de mantenerte seguro cuando visitas una página de internet, tienes que tener programas de “corta-fuego” (firewall), anti-virus y anti-espía. Sin esta protección un ladrón de identidad puede obtener información personal como tu número de seguro social, tu cuenta bancaria y número de tarjeta de crédito si es que compras en sitios de internet o pagas tus cuentas por esta vía. Hay programas gratis disponibles si es que no puedes comprar algunos de los que se ofrecen en el mercado, por ejemplo vea Grisoft’s gratis AVG anti-virus y Ewido programa anti-espía visitando sus páginas de internet en el sitio: <http://free.grisoft.com>.

### **No creas en los pescadores de contraseñas en la red (Phishing)**

Ellos nos contactan por teléfono, por correo electrónico o por correo regular, haciéndose pasar por nuestro banco, por nuestra compañía de Tarjeta de crédito y algunas veces por la oficina de hacienda pública (IRS) y nos piden que “verifiquemos” información como números de cuenta bancaria, número de seguro social ó contraseñas. A esto se le llama “pescadores de contraseñas” (phising) y los ladrones de identidad son tan buenos para eso, que convencen a muchas personas de que la página de internet falsa es una página de internet auténtica y real. Las compañías y/o agencias legítimas no piden información personal para identificarte vía telefónica ó por internet, por lo tanto si alguien te pide esta información, es más seguro que se trate de un ladrón de identidad quien te la esté pidiendo. Nunca des tu información personal al menos de que haya sido tú quien inició el contacto. Cuando tengas dudas, investiga el número real ó la dirección de página en internet a través de otra fuente de información y contáctalos para verificar si lo que recibiste fué legítimo.

### **Usa contraseñas que no sean fáciles de adivinar.**

Asegúrate de que tus contraseñas no sean fáciles de adivinar. Nombres, direcciones, cumpleaños y aún nombres de mascotas y amigos, pueden ser fácilmente utilizados por aquellos que te conocen aunque sea de forma casual. Si quieres mantenerte seguro contra el robo de identidad, usa contraseñas que sean más largas y sin sentido para otras personas más que para tí.

**Si crees que tu identidad ha sido robada, contacta a la Oficina de Protección a la Privacidad de Wisconsin al número 1-800-422-7128 ó mándanos un correo electrónico a: [WisconsinPrivacy@datcp.state.wi.us](mailto:WisconsinPrivacy@datcp.state.wi.us). Para más información, visite nuestra página de internet: [www.privacy.wi.gov](http://www.privacy.wi.gov)**