

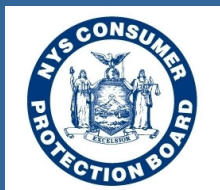
Lo Qué Deben Saber los Consumidores

- ◆ **Proteja Sus Datos Personales:** Evalúe las páginas de Internet que visite, y no entre información personal en los sitios web que no son seguros. Lea las reglas de privacidad para averiguar lo que el sitio web hará con su información personal
- ◆ **Transmita los Datos Financieros y Personales vía Sitios Web Seguros:** Los sitios web con conexión segura serán precedidas por "https." Dependiendo del programa que utilice, una cerradura o el símbolo clave intacto aparecerán en la porción más baja de su navegado. Cerciórese que "https" y la cerradura cerrada o llave intacta aparecen
- ◆ **No se Deje Caer en Estafas:** Quedese atento a tentativas para conseguir su información personal por medio de mensajes de spam y phishing

Envios spam inundan el Internet con muchas copias del mismo mensaje para forzar el mensaje en personas que de otro modo no decidiría recibirlo. La mayoría de spam son anuncios comerciales que muchas veces son para productos dudosos y esquemas para hacerse rico pronto

Phishing ocurre cuando alguien manda un mensaje electrónico a un usuario reclamando falsamente ser una empresa legítima y establecida con intento a estafar al usuario a rendir información privada que será utilizada para propósitos de robo de identidad

- ◆ **Evite Descargar Spyware:** No haga clic libremente en ofertas para productos de software de ningún-costo tales como los juegos, la música, salvapantalla o filtros aún anti spam. Eduque a otros usuarios de su computadora que sigan esta regla
- ◆ **Tenga Cuidado con Transacciones Financieras por Internet:** Cerciórese que la institución bancaria es legítima y los depósitos son financiados federalmente. Aprovechese de todos los programas de seguridad su banco ofrese, aún opcional



Lo Qué Deben Saber los Consumidores

- ◆ **Entienda las Limitaciones de la Seguridad de la Tecnología Radiofónica:** Los criminales pueden robar los datos transmitidos radiofónicamente sobre una red no garantizada por controlando la charla, los mensajes instantáneos y el correo electrónico. Los criminales pueden establecer también las redes de "pícaro" que imitan los que son seguros. Siempre verifique las calidades de una red antes de conectar. No transmita sus datos sensibles en un sitio público a menos que usted lo confíe, incluso si la transmisión sea cifrada
- ◆ **No Se Vuelva en una Víctima de Robo de Identidad por Medio del Internet:** Utilice contraseñas difíciles y cambielas regularmente. Cierre su computadora cuando usted no la utilice. Deshágase de las computadoras viejas apropiadamente. Si usted es una víctima, tome medidas
- ◆ **El Conocimiento de la Infracción de la Seguridad:** Si los datos que usted ha transmitido a un negocio en línea han sido robados, sepa cuales son sus derechos acerca de la notificación bajo la ley del Estado de Nueva York y otros remedios disponibles por el Acto Justo de la Cobertura del Crédito
- ◆ **Sea un Usuario Informado Sobre la Tecnología:** Controle todo uso de la computadora, especialmente el de los niños. Edúque a los niños acerca del uso apropiado de la computadora y del Internet. Si utiliza una computadora para el tratamiento de textos, salve archivos con frecuencia
- ◆ **Tenga Cuidado al Hacer Compras por el Internet:** Cerciórese de hacer compras de sitios web acreditados que utilizan codificación. Busque comprobación de terceros partidos. También revise las reglas de privacidad de la página de Internet y utilice una tarjeta de crédito dedicada para permitir un revisió fácil de compras. Nunca utilice una tarjeta de débito
- ◆ **Límite Spam:** Utilice las protecciones ofrecidas por su proveedor de servicios de Internet, como un filtro autónomo. No responda a spam ni para vengarse – éste sólo tendrá como resultado más spam.

Un servicio a la comunidad de la

**Junta de Protección al Consumidor del
Estado de Nueva York**

5 Empire State Plaza, Suite 2101, Albany, New York 12223