

La computadora y el Internet han cambiado el mundo. Ahora podemos trabajar, aprender, jugar, hacer vida social, hacer compras y manejar nuestra vida diaria en línea, sin salir de la comodidad de nuestra casa.

Pero no toda comunicación en línea es de confianza. Hay gente que usa el Internet para molestar u hostigar a otros en el anonimato, para dañar sistemas de computación o datos o hasta para cometer delitos.

Afortunadamente, puede tomar unos pasos sencillos que le ayudarán a evitar convertirse en víctima. Si sabe a qué atenerse, toma precauciones y usa útiles de protección, podrá disfrutar de los beneficios del Internet y también mantener a su familia, sus datos de computadora y a usted mismo seguros y sin peligro.

## Riesgos potenciales para los usuarios de Internet

Dependiendo de cómo utiliza el Internet, podría estar tomando riesgos innecesarios. Podría correr el riesgo de ser víctima de robo de identidad (cuando le roban y usan su información personal, como para obtener nuevas cuentas de crédito); robo o daño de datos; o amenazas contra su seguridad personal (también llamado ciberacecho o ciberintimidación).

Las que siguen son algunas de las formas con las que los delincuentes y estafadores encuentran a sus víctimas en línea:

- **Phishing**—se dice del intento de “engañarlo” para que revele su información confidencial y personal con el envío de correo electrónico falso que parece provenir de un comercio legítimo.
- **Spam (correo basura)**—correo electrónico y mensajes instantáneos no deseados que ofrecen venderle mercadería dudosa o le prometen beneficios financieros si le da dinero a quien se los envía.
- **Malware**—programación maliciosa (espía, troyana, virus y gusanos) que puede ser instalada en su computadora de forma remota y que permite que la persona que controla estos programas maliciosos le robe, dañe o borre sus expedientes o demás datos.
- **Operaciones que no son seguras**—Los sitios sin medidas de seguridad para la aceptación de pagos o compañías que almacenan información sobre tarjetas de débito o crédito sin los resguardos apropiados le pueden dar a los delincuentes la oportunidad de interceptar su información personal.

• **Sitos de redes sociales**—Los usuarios podrían correr riesgo si revelan demasiada información personal o si hacen arreglos para reunirse personalmente con personas que sólo conocen en línea. Ciertos sitios de redes sociales hasta podrían poner en peligro su información personal confidencial.

## Cómo proteger su computadora y los datos

El acceso a su información personal se puede obtener de muchas formas. Por fortuna, también hay muchas maneras de protegerse.

- **Use una barrera de control de acceso (firewall).** Se trata de un obstáculo virtual entre su computadora y el Internet. Todo lo que entra o sale de su computadora debe pasar por la barrera que impide el acceso a lo que no cumple ciertos criterios específicos de seguridad. Antes de comprar equipos o programación de barrera, verifique si su sistema operativo (OS, siglas en inglés) ya los tiene incluidos y si están en funcionamiento. (Mac OS X o Windows Vista son dos sistemas operativos comúnmente usados.)
- **Instale programas contra virus.** Estos programas escudriñan todo lo que entra a su computadora y buscan los virus conocidos. Como se crean nuevos virus continuamente, usted debe actualizar su programa antivirus de forma regular.
- **Instale programas contraespías.** Los programas espías vigilan las actividades que realiza en su computadora y reúnen información sin su conocimiento. Los programas contraespías los bloquean o los anulan. Algunos productos antivirus contienen características contraespías.
- **Use un filtro contra spam.** La mayoría de los proveedores de Internet (ISP, siglas en inglés) y programas de correo electrónico ya traen un filtro automático contra *spam* que reduce la cantidad de mensajes no solicitados que logra entrar a su bandeja de entrada. Elimine sin abrir cualquier *spam* o “correo basura” que logra traspasar el filtro.
- **Realice actualizaciones frecuentes.** Las compañías de informática y software actualizan sus programas con frecuencia para incluir protección contra las amenazas de seguridad más recientes. Por lo que, con sólo actualizar su sistema operativo y programación siempre que se publiquen versiones nuevas, tendrá una medida de seguridad adicional. Active las actualizaciones automáticas de medidas de seguridad, si están disponibles, para recibir una alerta cuando se publican.
- **Formule contraseñas resistentes.** La contraseña

se debe componer de letras, números y símbolos escogidos al azar. Nunca se debe usar información personal, como su fecha de nacimiento, dirección o el nombre de su mascota. Use por lo menos ocho caracteres en sus contraseñas; las más largas son más difíciles de deducir o descifrar.

• **Asegure su red inalámbrica.** Si deja la red “abierta” cualquiera dentro del alcance de su señal de wi-fi puede obtener acceso y posiblemente capturar los datos que envía y recibe. Asegurar la red puede ser tan simple como crear una contraseña resistente para su enrutador y encenderle la herramienta de codificación que ya tiene incorporada.

## Nota especial sobre computadoras anticuadas

Si tiene una computadora anticuada, es posible que ya no reciba actualizaciones y “remiendos” de seguridad, y el fabricante posiblemente ya no ofrezca apoyo para ese modelo. Las nuevas versiones de navegadores tienen características importantes de seguridad que podrían no operar en sistemas anticuados. Las barreras de control de acceso son relativamente nuevas y ya vienen activadas por el fabricante en las computadoras nuevas, pero podrían no estar activadas en las más antiguas. Como resultado, una computadora más antigua con conexión de Internet continua de alta velocidad podría correr el riesgo de sufrir infracciones de seguridad y privacidad.

## Cómo proteger su privacidad frente al mercadeo en línea

El resguardo de su información personal cuando está conectado al Internet no sólo lo protege a usted de las personas deshonestas, si no que le reduce la exposición a ciertos estorbos, por ejemplo, los mensajes comerciales indeseables.

Una forma simple pero efectiva para mantener su privacidad es revelar lo menos posible sobre sí mismo en sitios que no conoce hasta haber decidido que sí desea establecer una relación. Siempre que complete un formulario, se registre en un concurso en línea, o ingrese información electrónica de cualquier forma, la misma podría ser usada para propósitos de comercialización por la compañía cuyo sitio está visitando, o por terceros que compran la información. Lea la “política de privacidad” en los sitios que visita para asegurarse de que no van a vender ni canjear su información de contacto.

También puede tomar pasos para manejar las llamadas “cookies” que pueden ser colocadas en el disco duro de su computadora después

que usted visita un sitio web. Se utilizan, por ejemplo, para informarle al sitio patrocinador acerca de las páginas que visitó y lo que puso en su carrito de compras. Esa información se registra cada vez que usted visita el sitio y las compañías a veces la utilizan en sus esfuerzos comerciales. Si no desea que el sitio que visita retenga su información o que lo reconozca cuando vuelva a visitar, fije al navegador para que borre las cookies automáticamente siempre que salga del mismo. También puede fijarlo de tal forma que no acepte cookies, pero así podría restringir su visita a ciertos sitios.

Para limitar la cantidad de mensajes no deseados que le envían a su dirección electrónica principal, puede crear una dirección alterna para ciertas actividades en línea. Puede elegir entre muchos servicios gratuitos de correo electrónico.

Ignore o borre completamente el *spam*. No responda, ni siquiera para que lo retiren de la lista de suscriptores, porque su respuesta confirmaría que su dirección está vigente.

Las compañías legítimas tendrán una política sobre privacidad que cita con claridad cuándo y cómo podrán usar su información. Salga del sitio si no está satisfecho que su privacidad será protegida. Busque logos de marca de confianza, como TRUSTe, que certifican las políticas de privacidad confiables.

Si tiene hijos, no les permita revelar su información privada en los sitios que visitan. (La ley COPPA, Children’s Online Privacy Protection Act, requiere que los sitios obtengan el consentimiento de sus padres para recopilar o usar cualquier información personal de niños menores de 13 años.)

## Cómo proteger a sus hijos en línea

Los niños sacan mucho provecho del Internet, pero no toda la comunicación ni el contenido es apropiado para niños pequeños o adolescentes. Para ayudar a asegurar que la experiencia de sus hijos en línea sea positiva y segura, demuestre un interés activo en sus actividades por Internet.

Lea los blogs favoritos de sus hijos (una especie de bitácora de Internet), y visite y hágase “amigo” de ellos en sus sitios de redes sociales. Hable con ellos sobre la información que puede compartirse y la que se debe mantener secreta. Explíqueles por qué no es apropiado que se encuentren solos con alguien que “conocen” por Internet. También deben saber que no deben compartir sus contraseñas de las redes sociales y demás sitios con sus amigos. Las cuentas podrían ser comprometidas y les podrían robar la información personal.

Manténgase en comunicación con sus hijos; anímelos a compartir con usted las dudas y experiencias que han tenido en Internet. Asegúreles que no serán castigados y que no les quitará el acceso a Internet si le cuentan que reciben amenazas o comunicación inapropiada, incluso intimidación. Y explíqueles por qué está mal que intimiden a los demás.

Informe a las autoridades apropiadas sobre comportamiento hostil o predatorio, entre otros, autoridades escolares, policía local, o CyberTipline en [www.cybertipline.com](http://www.cybertipline.com) o 800-843-5678.

Hable con ellos sobre los riesgos de usar el Internet, y fije reglamentos claros sobre lo que sus hijos pueden hacer y los sitios que pueden visitar en línea. Existen programas especiales diseñados para manejar el uso de Internet que lo pueden ayudar a mantener a sus hijos más seguros. Obtenga información sobre útiles para la seguridad familiar en [kids.getnetwise.org/tools](http://kids.getnetwise.org/tools).

## Más consejos y útiles

Las que siguen son otras formas adicionales para aumentar su seguridad y privacidad en línea:

- **Haga copias** de seguridad de sus expedientes de forma regular (al menos una vez por semana).
- **Fije su sistema** operativo para que actualice automáticamente. Puede optar por que actualice en horarios convenientes cuando no esté usando la computadora.
- **Borre** el disco duro antes de vender, donar o deshacerse de la computadora.
- **Asegúrese** que el sitio sea seguro. Verifique que lleve la codificación SSL ("https://" y no sólo "http://") en la barra de direcciones del navegador y que aparezca en el marco de la ventana del navegador un candado cerrado o llave entera. Nunca ingrese información sobre tarjetas de débito o de crédito o números de cuentas de banco a menos que verifique primero lo anterior. La mayoría de los sitios web legítimos usan codificación SSL para que se pueda comprar en línea sin peligro.
- **Al hacer compras** en línea es más seguro usar una tarjeta de crédito que una de débito. La responsabilidad por el uso no autorizado de una tarjeta de crédito es de \$50, pero puede ser mucho más alta por una de débito, dependiendo de cuándo reportó la pérdida. Además, la mayoría de las tarjetas de débito están conectadas a su cuenta de banco, por lo que un ladrón puede vaciarle la cuenta.

- **No permita** que el navegador guarde identificaciones y contraseñas confidenciales, como las de su cuenta de banco, ni permita que los sitios que pretenden convertirse en su "punto único de compras" almacenen la información de sus tarjetas de crédito o débito. Esto es importante en especial cuando se usan computadoras compartidas o públicas. Borre esta información al hacer clic en "Tools" en la mayoría de los navegadores y al seleccionar "Delete Browsing History" ("borrar el historial de navegación") o "Clear Private Data" (borrar datos privados"). (Las palabras que se utilizan pueden ser distintas según el navegador.)

- **Compre únicamente** con comerciantes de confianza.

- **Si sospecha que** un mensaje de correo electrónico puede ser un intento de obtener información por phishing, comuníquese directamente con la compañía. Un comercio legítimo nunca le va a pedir sus datos personales por esa vía. Borre el mensaje y no lo conteste.

- **Tenga cuidado** al abrir expedientes adjuntos al correo electrónico, al visitar sitios que no conoce y al descargar programas "gratuitos". No descargue ni comparta música o películas con personas extrañas; el expediente que recibe puede contener un virus, programas espías o contenido inapropiado. (Y, es ilegal compartir material registrado con derechos de autor.)

- **No envíe** "cartas cadena" ni cualquier otro correo basura a otras personas aunque los considere agradables o informativos; podrían considerarlo a usted un distribuidor de spam o, lo que es peor, podría estar enviando un expediente destructivo a otra persona. Revise todos los mensajes en sitios anti-engaños ([www.snopes.com](http://www.snopes.com) o [www.quatloos.com](http://www.quatloos.com)) antes de enviarlos a otros para no distribuir "mitos urbanos".

- **Confíe en sus instintos.** Si le parece que algo suena demasiado bueno, es posible que no sea cierto. Su mejor defensa es su buen criterio.

- **Piénselo dos veces** antes de oprimir avisos banner o ventanas automáticas del navegador. Oprima la X en la esquina superior derecha de la ventana para cerrarla.

- **Tenga presente** que la música, los juegos y otras descargas gratuitas con frecuencia incluyen programación indeseada.

- **No use** el correo electrónico y mensajes instantáneos (IM) para enviar información personal confidencial como números de tarjetas de crédito, contraseñas, su fecha de nacimiento o número de Seguro Social.

- **Tome precauciones** similares si conecta a Internet por teléfono inteligente u otro aparato capacitado para Internet.

## Asistencia e información

Las siguientes organizaciones representan un buen punto de comienzo para obtener más información sobre la seguridad en Internet.

**Family Online Safety Institute • [www.fosi.org](http://www.fosi.org)**

La labor de Family Online Safety Institute es lograr un Internet más seguro para niños y familias.

**OnGuard Online • [www.onguardonline.gov](http://www.onguardonline.gov)**

El gobierno federal de los EE. UU. y la industria de tecnología proporcionan información y consejos para promover la seguridad en línea.

**Privacy Rights Clearinghouse • [www.privacyrights.org](http://www.privacyrights.org)**

La organización Privacy Rights Clearinghouse sin fines de lucro ofrece una biblioteca de información, desde consejos para quienes buscan empleo en línea hasta cómo comprar sin peligro en Internet.

**Consumer Action, organización de educación y defensa, ofrece noticias e información sobre privacidad, incluso sobre sus derechos y cómo evitar fraudes.**

**Consumer Action**  
[www.consumer-action.org](http://www.consumer-action.org)

**221 Main Street, Suite 480**  
**San Francisco, CA 94105**  
**415-777-9635 / TTY: 415-777-9456**  
[hotline@consumer-action.org](mailto:hotline@consumer-action.org)

**523 W. Sixth Street, Suite 1105**  
**Los Angeles, CA 90014**  
**213-624-8327**

**Se habla chino, inglés y español.**

Esta publicación fue creada por Consumer Action en colaboración con Microsoft. © Consumer Action 2009

Internet Safety (Spanish version)



# SEGURIDAD POR INTERNET

Guía sobre privacidad y seguridad para el usuario de computadoras

Publicación de Consumer Action