

## 7 Prácticas para la Seguridad de su Computadora

- 1 Proteja su información personal. Es valiosa.
- 2 Sepa con quién está tratando.
- 3 Use un *software* de seguridad que se actualice automáticamente.
- 4 Mantenga actualizado su sistema operativo y su navegador de Internet y entérese de las funciones de seguridad disponibles.
- 5 Cree contraseñas difíciles de descifrar y protéjalas guardándolas en un lugar seguro.
- 6 Haga copias de seguridad de todos los archivos importantes.
- 7 Aprenda qué hacer en caso de e-mergencia.

El nivel de acceso a la información y al entretenimiento, a los servicios crediticios y financieros, a los productos provenientes de cada rincón del mundo — y hasta a su trabajo — es mayor que nunca. Gracias a Internet usted puede jugar una partida amistosa con un oponente localizado del otro lado del océano, ver y examinar videos, canciones o vestimenta; conseguir al instante el consejo de un experto o colaborar con compañeros de trabajo ubicados en una oficina "virtual" lejana.

Sin embargo, Internet — y el anonimato que ofrece — también permite que los estafadores, *hackers* y ladrones de identidad que operan en línea puedan acceder a su computadora, a su información personal, a su actividad financiera y demás datos.

Pero si usted es conciente de estos riesgos puede crear una red de seguridad para minimizar las probabilidades de enfrentar contratiempos en Internet. Mantenerse alerta en línea lo ayudará a proteger su información, su computadora y su dinero. Para estar más seguro y protegido en línea, adopte rutinariamente las siete prácticas que se listan a continuación.

### 1. Proteja su información personal. Es valiosa.

Su información personal puede darle a un ladrón de identidad acceso instantáneo a sus cuentas financieras, registro de crédito y demás bienes o activos. Si cree que no hay nadie que esté interesado en SU información personal, piénselo dos veces. CUALQUIER persona puede convertirse en una víctima del robo de identidad. En verdad, de acuerdo a los datos que posee la Comisión Federal de Comercio (*Federal Trade Commission*, FTC), este delito perjudica a millones de víctimas por año. Para saber qué hacer si le roban su identidad o si se compromete su información personal o financiera tanto en Internet como en el mundo "real", visite [ftc.gov/robodeidentidad](http://ftc.gov/robodeidentidad).

¿Cómo consiguen su información personal los delincuentes? Una de las maneras utilizadas es mentir sobre su verdadera identidad para convencerlo a usted de que les revele los números de sus cuentas, sus contraseñas y demás información para poder quitarle su dinero o hacer compras en su nombre. Esta estafa llamada "*phishing*" se produce cuando los delincuentes envían mensajes electrónicos, mensajes de texto o de tipo *pop-up* que aparentemente provienen de su banco, una agencia del gobierno, un vendedor que opera en línea o alguna otra organización con la cual usted mantiene un trato comercial. En el mensaje se le indica que haga clic sobre un enlace para redirigirlo a un sitio Web o que llame a un número de teléfono para actualizar los datos de su cuenta o para reclamar un premio o beneficio. El texto de este tipo de mensajes puede insinuar que si usted no responde rápidamente para actualizar su información, le sucederá algo malo. En realidad, los comercios que operan legítimamente nunca deberían utilizar mensajes electrónicos, de texto o *pop-ups* para solicitarle su información personal.

### **Para evitar las estafas de *phishing* tenga en cuenta lo siguiente:**

- Si recibe un *email*, mensaje de texto o si le aparece en pantalla un mensaje de tipo *pop-up* por medio del cual le solicitan información personal o financiera, no responda ni haga clic sobre el enlace incluido en el mensaje. Si quiere acceder al sitio Web de un banco o negocio, escriba usted mismo el domicilio en la barra de su navegador.
- Si recibe un mensaje - *email*, mensaje de texto, *pop-up* o mensaje telefónico - en el cual le indican que llame a un número de teléfono para actualizar los datos de su cuenta o para proporcionar su información personal para recibir un reintegro, no responda ni haga clic. Si necesita comunicarse con una organización con la cual mantiene una relación comercial llame al número que figura en su resumen de cuenta o búsquelo en la guía telefónica.

Algunos ladrones de identidad han robado información personal de muchas personas de una sola vez accediendo indebidamente a grandes bases de datos de negocios o agencias gubernamentales. Si bien es cierto que no podrá disfrutar de los beneficios de Internet sin compartir algunos datos de información personal, usted puede protegerse compartiéndola únicamente con las organizaciones conocidas y confiables. No revele su información personal sin antes averiguar cómo será utilizada y protegida.

Si hace compras en Internet, no suministre su información personal ni financiera a través del sitio Web de una compañía antes de verificar los indicadores de seguridad del sitio, como por ejemplo, el ícono del candado que aparece en la barra de estado de su navegador o un domicilio Web URL que comience con "https:" (la "s" corresponde a "seguro"). Lamentablemente, no hay indicadores cien por ciento seguros; algunos estafadores han falsificado íconos de seguridad. Y algunos *hackers* se las han ingeniado para acceder indebidamente a sitios Web que tomaron las precauciones de seguridad apropiadas.

Lea las políticas de privacidad de los sitios Web. Éstas deberían describir qué tipo de información personal recolectan, cómo la utilizan y si será provista a terceros. La política de privacidad también debería informarle si tiene derecho a ver cuál es la información que posee el sitio Web sobre usted y cuáles son las medidas de seguridad adoptadas por la compañía para proteger su información. Si no encuentra la política

de privacidad — o no la entiende — considere hacer negocios en otra parte.

## 2. Sepa con quién está tratando.

Y sepa en lo que se está metiendo. Las personas deshonestas pueden operar tanto en las tiendas tradicionales como en Internet. Pero en Internet usted no puede juzgar la fiabilidad del operador mirándolo a los ojos y confiándose en su instinto. Es extremadamente fácil para los estafadores cibernéticos hacerse pasar por negocios que operan legítimamente, por lo tanto usted necesita saber con quién está tratando. Si está pensando en hacer compras en línea en un sitio Web desconocido, verifique por su propia cuenta la legitimidad del vendedor antes de comprar.

- Si es la primera vez que compra en un sitio desconocido, llame al número del vendedor para estar seguro de poder localizarlo telefónicamente en caso de que sea necesario. Si no encuentra un número de teléfono habilitado, compre en otra parte.
- Escriba el nombre del sitio en un motor de búsqueda: Si encuentra comentarios desfavorables de otros compradores, más le vale hacer negocio con otro vendedor.
- Considere instalar en su navegador una barra de herramientas que califique los sitios Web y que lo advierta cuando visite un sitio con informes desfavorables de expertos y de otros usuarios de Internet. Algunas compañías reputadas ofrecen gratuitamente algunas herramientas que pueden alertarlo cuando visita un sitio Web conocido por sus prácticas de *phishing* o utilizado para distribuir programas maliciosos.

## Tecnología P2P: ¿Valen la pena los costos encubiertos?

Diariamente, millones de usuarios de computadora comparten archivos por Internet. La tecnología P2P les permite a los usuarios acceder a una gran cantidad de información como por ejemplo música, juegos y programas *software*. ¿Cómo funciona? Usted descarga un *software* especial que conecta su computadora a una red informal de la que participan otras computadoras que utilizan el mismo *software*. Con este *software*, millones de usuarios pueden conectarse entre sí al mismo tiempo. A menudo, este programa es gratuito y fácil de conseguir.

Pero la tecnología P2P también presenta una cantidad de riesgos. Si usted no instala la configuración apropiada del programa, podría permitir que otros usuarios accedan no solamente a los archivos que usted desea compartir, sino también a otra información almacenada en su disco duro, como por ejemplo sus declaraciones de impuestos, mensajes electrónicos, registros médicos, fotos u otros documentos personales. Además, usted podría descargar involuntariamente *software* malicioso, malintencionado o pornografía etiquetada bajo otros títulos o material protegido por derechos de autor, lo cual podría implicar una violación a la ley.

Si decide usar un programa de uso compartido de archivos, asegúrese de leer el acuerdo de licencia para el usuario o EULA (End-User License Agreement, en inglés) para estar seguro de comprender y aceptar los posibles riesgos de los programas descargados gratuitamente.

### 3. Use un **software de seguridad que se actualice automáticamente.**

Active su *software* de seguridad y manténgalo actualizado: como mínimo tiene que instalar en su computadora un *software antivirus*, un *antiespía* y un *firewall*. Usted puede conseguir programas de seguridad para tratar cada elemento individualmente o uno que le ofrezca múltiple protección. Puede comprar estos programas en tiendas especializadas o puede obtenerlos por medio de su Proveedor de Servicio de Internet. En general, los *software* de seguridad que vienen preinstalados en las computadoras solamente funcionan por un corto tiempo excepto que usted pague una suscripción para mantenerlo activo. En cualquier caso, sepa que el *software* de seguridad protegerá su computadora contra las más recientes amenazas solamente si lo mantiene actualizado. Por esta razón, resulta sumamente importante que configure su *software* de seguridad para que se actualice automáticamente.

Algunos estafadores oportunistas distribuyen *malware* disfrazándolo como un programa antiespía. Resista la tentación de comprar programas ofrecidos por medio de mensajes pop-up o mensajes electrónicos inesperados, especialmente si se trata de anuncios que dicen que han escaneado su computadora y detectado *malware*. Se trata de una táctica utilizada por los estafadores para distribuir *malware*. AlertaenLínea.gov puede conectarlo con una lista de herramientas de seguridad para computadoras ofrecidas a la venta por proveedores legítimos seleccionados por el proyecto de *Internet Education Foundation* llamado *GetNetWise*.

Después de confirmar que su *software* de seguridad esté actualizado, actívelo para escanear su computadora a la búsqueda de virus y programas espías. Elimine todo lo que el programa identifique como problemático.

#### **Programa *antivirus***

El programa o *software antivirus* protege su computadora de los virus que pueden destruir sus datos, lentificar o congelar su funcionamiento, o hasta permitir que los *spammers* envíen mensajes electrónicos por intermedio de su cuenta. El *software antivirus* funciona como un escáner, en otras palabras revisando y escudriñando su computadora y los mensajes electrónicos que entran a la búsqueda de virus y cuando los encuentra, los elimina.

#### **Software antiespía**

Los programas espías son programas instalados en su computadora sin su consentimiento que monitorean o controlan el uso de su computadora. Estos programas pueden utilizarse para enviar anuncios de tipo *pop-up*, redirigir su computadora a sitios Web, monitorear su navegación de Internet o para registrar lo que escribe en el teclado, lo cual, a su vez, puede facilitar el robo de su información personal.

Si su computadora tiene algunos de los siguientes problemas, es posible que esté infectada con *malware*:

- Funciona lentamente, funciona mal o muestra mensajes de error repetidamente.

- No puede apagarla o encenderla.
- Recibe un montón de anuncios *pop-up*, o le aparecen este tipo de ventanas cuando no está navegando en Internet.
- Aparecen en pantalla páginas Web o programas que usted no tenía intención de visitar o utilizar, o envía mensajes de correo electrónico que usted no escribió.

## **Firewall**

El *firewall* ayuda a impedir que los *hackers* o piratas informáticos usen su computadora para enviar su información personal sin su autorización. Mientras que el *software antivirus* revisa los archivos y los mensajes de correo electrónico entrantes, un *firewall* es como un guardián que se mantiene vigilante a los ataques exteriores que intenten acceder a su sistema y bloquea las comunicaciones con y desde fuentes no autorizadas por usted.

## **No permita que su computadora se incorpore a un ejército de "Robots de la Red".**

Algunos *spammers* hacen búsquedas en Internet a la caza de computadoras que no están protegidas para poder controlarlas y utilizarlas anónimamente para enviar mensajes masivos no deseados o *spam* convirtiéndolas en *robots* de la red, también llamados "*botnets*". Estos *botnets*, también conocidos como "ejércitos de zombis", están compuestos de varios miles de computadoras hogareñas que envían mensajes electrónicos por millones. La mayor parte de los mensajes de tipo *spam* se envían de este modo; los *botnets* están integrados por millones de computadoras de uso hogareño.

Los *spammers* escanean la red para encontrar computadoras que no tienen instalado un programa de seguridad e instalarles un *software* malicioso - conocido como "malware" - atravesando esas "puertas abiertas". Por esta razón, resulta sumamente importante que actualice su *software* de seguridad.

Los programas maliciosos o *malware* pueden estar ocultos en las aplicaciones de los programas gratuitos. Puede resultar tentador descargar gratuitamente juegos, programas de archivos compartidos, barras de herramientas personalizadas o algunos otros programas de este tipo. Pero algunas veces, el solo hecho de visitar un sitio Web o descargar archivos puede causar lo que se llama una descarga encubierta de archivos o "drive-by download" que le instala en su computadora un programa malicioso que podría convertirla en un "bot".

Otra forma utilizada por los *spammers* para acceder a su computadora y controlarla es enviarle un *email* con enlaces o con imágenes o archivos adjuntos y si usted los abre o hace clic le instalan el *software* oculto. Tenga cuidado al abrir archivos electrónicos adjuntados o al descargar archivos de mensajes electrónicos recibidos. No abra ningún archivo adjuntado a un *email* — aunque aparente provenir de un amigo o colega de trabajo — a menos que lo esté esperando o conozca su contenido. Si usted envía un *email* con un archivo adjunto, incluya un mensaje de texto explicando de qué se trata.

#### **4. Mantenga actualizado su sistema operativo y su navegador de Internet y entérese de las funciones de seguridad disponibles.**

Los *hackers* también se aprovechan de los navegadores de Internet (como por ejemplo Firefox o Internet Explorer) y de los programas de los sistemas operativos (como Windows o MAC's OS) que no poseen las más recientes actualizaciones de seguridad. Las compañías de sistemas de seguridad para computadoras ofrecen parches para reparar las fallas detectadas en sus sistemas, por lo tanto, es importante que usted configure su sistema operativo y navegador de Internet para que descargue e instale automáticamente los parches de seguridad.

Además, usted puede aumentar el nivel de seguridad en línea cambiando las características de las funciones de seguridad y privacidad de su sistema operativo o navegador de Internet que vienen instaladas de fábrica. Abra el menú de "Herramientas" (*Tools*) u "Opciones" (*Options*) para saber cómo aumentar el nivel predeterminado de seguridad. Para consultar información sobre sus opciones, use el botón de la función "Ayuda" (*Help*).

Si no va a usar su computadora por un período de tiempo prolongado, desconéctela de Internet. Cuando la computadora está desconectada, no envía ni recibe información de Internet y es invulnerable a los ataques de los *hackers*.

#### **5. Proteja sus contraseñas.**

Mantenga sus contraseñas en un lugar seguro y fuera del alcance de los demás. No comparta sus contraseñas en Internet, por correo electrónico ni por teléfono. Su proveedor de servicio de Internet (*ISP*) no debería solicitarlas nunca.

Además, para poder acceder a su computadora, los *hackers* pueden intentar descifrar sus contraseñas. Usted puede complicarles la tarea haciendo lo siguiente:

- Usar contraseñas compuestas de por lo menos ocho caracteres incluyendo números y símbolos. Cuanto más extensa sea su contraseña más difícil será descifrarla. Una contraseña compuesta de 12 caracteres es más sólida que una de ocho.
- Evitar palabras de uso común: algunos *hackers* utilizan programas que pueden probar cada una de las palabras que figuran en el diccionario.
- No use como contraseñas su información personal, su nombre de inicio de sesión, o una serie de letras dispuestas adyacentemente en el teclado (por ejemplo qwertyui).
- Cambie sus contraseñas con regularidad (como mínimo cada 90 días).
- No use la misma contraseña para todas las cuentas a las cuales acceda en línea.

#### **6. Haga copias de seguridad de todos los archivos importantes.**

Si usted sigue estas recomendaciones, tendrá más probabilidades de librarse de las interferencias de los *hackers*, virus y *spammers*. Pero

ningún sistema es completamente seguro. Si almacena en su computadora archivos importantes, cópielos a un disco removible o disco duro externo y guárdelo en un lugar seguro.

## 7. Aprenda qué hacer en caso de e-mergencia.

Si sospecha que su computadora está bajo la amenaza de un malware, pare inmediatamente de hacer compras, trámites bancarios o detenga cualquier otra actividad en línea que involucre nombres de usuario, contraseñas o cualquier otra información delicada. Un programa malicioso instalado en su computadora podría enviar su información personal a los ladrones de identidad.

Confirme que su *software* de seguridad esté activado y actualizado y úselo para escanear su computadora. Elimine todo aquello que el programa identifique como problemático. Es posible que tenga que reiniciar su computadora para activar los cambios.

Si el problema persiste después de agotar su propia capacidad técnica para diagnosticarlo y tratarlo, posiblemente desee recurrir a alguien que le brinde asistencia profesional. Si su computadora está bajo una garantía que ofrece servicio técnico, comuníquese con el fabricante. Antes de llamar, anote el modelo y número de serie de su computadora, el nombre de los programas instalados y una breve descripción del problema. Estas anotaciones lo ayudarán a describir el problema correctamente cuando hable con el técnico.

Si necesita ayuda profesional, si su computadora no está cubierta por una garantía o si su *software* de seguridad no funciona correctamente, es posible que tenga que recurrir a un servicio técnico y que deba pagarlo. Varias compañías — incluso algunas que están afiliadas con tiendas minoristas — ofrecen apoyo técnico por teléfono, en línea, en las mismas tiendas o a domicilio. En general, la manera más económica de recibir apoyo técnico es por medio de los servicios que se prestan telefónicamente o en línea — especialmente si le dan la posibilidad de comunicarse por medio de una línea telefónica de acceso gratuito — pero usted deberá hacer parte de la tarea por su cuenta. Habitualmente, llevar la computadora a la tienda es menos costoso que llamar a un técnico o servicio de reparación para que vaya hasta su casa.

Cuando su computadora esté reparada y en funcionamiento, piense de qué manera pudo haber descargado un malware a su máquina y qué es lo que puede hacer para evitar que vuelva a sucederle en el futuro.

Además, hable sobre la manera de utilizar la computadora de manera segura con todos aquellos que la usan. Dígales que algunas de las actividades realizadas en línea pueden poner en riesgo la computadora y comparta con ellos las siete prácticas de seguridad para computadoras.

## Dónde reportar los problemas

### Ataques de virus o *hackers*

Alerte a las autoridades correspondientes, comunicándose con:

- Su proveedor de servicio de Internet (*ISP*) y el del *hacker* (si puede determinarlo). Generalmente, puede encontrar la dirección de correo electrónico del *ISP* en su sitio Web. En su mensaje incluya la información del incidente que aparezca en el archivo de registro del *firewall*. Al alertar del problema a su *ISP*, puede ayudar a prevenir la aparición de problemas similares en el futuro.
- El FBI en [www.ic3.gov](http://www.ic3.gov). Para luchar contra los delincuentes cibernéticos los funcionarios de esta agencia necesitan recibir toda la información que usted pueda suministrarles.

## Fraude en Internet

Si un estafador se aprovecha de usted cuando está haciendo compras en Internet, a través de una subasta electrónica o de cualquier otra manera, denúncielo a la Comisión Federal de Comercio en [ftc.gov/espano](http://ftc.gov/espano)!. La FTC ingresa todas las quejas relacionadas a fraudes de Internet, robo de identidad y otras quejas sobre prácticas fraudulentas a una base de datos segura llamada Centinela del Consumidor (*Consumer Sentinel*) que se encuentra a disposición de cientos de agencias de cumplimiento de las leyes civiles y penales en los Estados Unidos y en el extranjero.

## Spam engañoso

Si recibe mensajes electrónicos de tipo *spam* con contenidos engañosos, incluyendo mensajes que están a la "pesca" de su información, reenvíelos a [spam@uce.gov](mailto:spam@uce.gov). Asegúrese de incluir el encabezado (header) completo del mensaje de correo electrónico con toda la información del remitente. También puede reportar un *email* de *phishing* a [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org). La organización llamada *Anti-Phishing Working Group*, es un consorcio de Proveedores de Servicio de Internet, vendedores de sistemas de seguridad, instituciones financieras y agencias encargadas de velar por el cumplimiento de la ley que usan las denuncias para combatir el *phishing*.

## Divulgación de información personal

Si cree que por error le dio su información personal a un defraudador, presente una queja en <http://www.ftc.gov> y posteriormente visite el sitio Web de la FTC para casos de robo de identidad en [ftc.gov/robodeidentidad](http://ftc.gov/robodeidentidad) para informarse sobre cómo minimizar los riesgos de los perjuicios causados por un potencial robo de su identidad.

## Padres

En ocasiones, los padres pueden sentirse sobrepasados por la habilidad tecnológica de sus hijos. Dejando la tecnología de lado, hay varias lecciones que los padres pueden enseñar a sus hijos para ayudarlos a mantenerse seguros mientras que se socializan en línea. La mayoría de los servidores de servicio de Internet ofrecen controles para padres, o puede comprarlos por separado. Pero ningún *software* puede

reemplazar la supervisión paterna. Hable con sus hijos acerca de las prácticas seguras para usar la computadora y también sobre lo que pueden ver y hacer cuando están en línea.

## Sitios de redes sociales

Muchos adultos, adolescentes y niños usan los sitios de redes sociales para intercambiar información sobre sí mismos, para compartir fotografías y videos, y utilizan *blogs* y el sistema de mensajes privados para comunicarse con amigos, con otras personas que comparten los mismos intereses, y en ocasiones con el mundo entero. Estas son algunas recomendaciones para aquellos padres que deseen que sus hijos usen estos sitios sin exponerse a riesgos:

- Utilice las funciones de privacidad para limitar el acceso al sitio Web de su hijo y para restringir la colocación de información. Algunos sitios Web de redes sociales poseen funciones de privacidad muy efectivas. Enséñeles a sus hijos a utilizar estas funciones para limitar el acceso solamente a aquellas personas que desee que vean sus perfiles en línea y explíqueles la importancia de este punto.
- Aliente a sus hijos a reflexionar acerca del lenguaje que usan en un blog y a pensar en las posibles consecuencias antes de colocar fotos o videos en línea. Los empleadores, los encargados de admisiones de las universidades, los entrenadores de equipos deportivos y los maestros pueden ver lo que sus hijos colocan en línea. Y también puede ser importante el tipo de nombre de pantalla o *screen name* seleccionado. Aliente a sus hijos a pensar sobre la impresión que pueden causar los nombres de pantalla que elijan.
- Recuérdeles a sus hijos que una vez que colocan la información en línea, no la pueden quitar. Aunque eliminen la información de un sitio Web, las antiguas versiones quedan registradas en las computadoras ajenas y pueden ser circuladas en línea.
- Hable con sus hijos sobre las prácticas de intimidación o *bullying*. La intimidación o acoso en línea puede presentarse de varias formas, desde dispersar rumores sobre alguna persona, colocar mensajes en línea o reenviarlos sin el consentimiento del autor, hasta mandar mensajes amenazantes. Dícales a sus hijos que las palabras que escriben y las imágenes que colocan en línea pueden tener consecuencias reales. Sus actividades en línea pueden provocar el malestar de la víctima de una intimidación, pueden desprestigiar al autor de un mensaje privado - y en algunas ocasiones pueden causar el castigo de las autoridades. Aliente a sus hijos a conversar con usted cuando se sientan amenazados por un "matón" o por algún tipo de intimidación.
- Hable con sus hijos sobre la importancia de evitar conversaciones de naturaleza sexual en línea. Los resultados de una investigación realizada recientemente demuestran que los adolescentes que no hablan de sexo con extraños tienen menos probabilidades de entrar en contacto con un acosador.
- Dícales a sus hijos que si tienen alguna sospecha confíen en sus instintos. Si cuando están en línea se sienten amenazados por alguna persona o si se sienten incómodos con algo que ven en la red es necesario que se lo digan a usted. Puede ayudarlos a reportar sus inquietudes a la policía y al sitio de redes sociales. La mayoría de estos sitios incluyen enlaces para que los usuarios puedan reportar inmediatamente los comportamientos abusivos, sospechosos o inapropiados en línea.

Para solicitar folletos con esta información, [haga clic aquí](#).