Alerta para Consumidores

Federal Trade Commission ■ Bureau of Consumer Protection ■ Office of Consumer and Business Education

Cómo Conectarse al Internet de Manera Segura

Dialing Up to the Internet: How to Stay Safe Online

La mayoría de los estadounidenses que utilizan Internet desde sus hogares lo hacen a través de una "conexión de discado" la cual usa un módem para llamar a un servidor por medio de una línea telefónica corriente. Una conexión de discado *(dial-up)* a Internet puede ser de más baja tecnología — y también más lenta — que una conexión de banda ancha, pero hay un elemento que ambas conexiones comparten: las dos dependen del usuario para que sea operada de manera segura y confiable.

Si su computadora es atacada por un virus o un *hacker*, no es realmente importante cual sea el tipo de conexión que usted utiliza: el daño ya fue ocasionado. Usted puede perder información personal importante o programas *software* almacenados en su disco rígido, y además puede perder tiempo valioso tratando de hacer las reparaciones. Asimismo, su computadora puede ser utilizada sin su conocimiento para atacar a otras computadoras, incluyendo a aquellas que protegen nuestra seguridad nacional.

Si usted usa una conexión de discado, algunos pocos consejos para aplicar "ahora" pueden ayudarlo a minimizar y quizás a evitar completamente — el daño que un virus o un *hacker* pueden causar a su computadora.

1. Use un programa *software* antivirus. Un virus es un *software* implantado en su computadora para dañar sus archivos y desestabilizar su sistema. La mayoría de los virus ingresan a su computadora ocultos en un programa aparentemente inofensivo, generalmente como archivo adjunto *(attachment)* de un mensaje de correo electrónico. Una vez ingresado a su computadora, el código del programa del virus produce copias de sí mismo e inserta el código copiado dentro de otros programas. Un virus puede producir la pérdida de datos o requerir costosas reparaciones de su sistema. Usted puede evitar la exposición a estos riesgos instalando y utilizando un programa *software* que revisa los virus del sistema de su computadora y de todos los mensajes de correo electrónico que recibe y que los elimina.

Usted puede descargar programas antivirus de los sitios web de las compañías de *software* o comprarlos en los comercios especializados. Busque un programa antivirus que reconozca los virus actuales y también los más antiguos, que pueda reparar los daños y que se actualice automáticamente.

2. Actualice regularmente el programa antivirus. Para que el programa antivirus sea efectivo, tiene que ser actualizado rutinariamente para que se incorporen los antídotos contra los *"bugs"* de más reciente circulación en Internet. La mayoría de los programas antivirus que se comercializan, incluyen una característica que posibilita que se descarguen automáticamente las actualizaciones de detección y eliminación cuando usted está en Internet.

3. No se deje atrapar por mensajes de correo electrónico mentirosos. La mayoría de los virus no dañarán su computadora si usted no abre los documentos adjuntos de su correo electrónico conteniendo los virus. Por lo tanto, los *hackers*, personas que usan el Internet para acceder a las computadoras sin autorización — mienten con frecuencia para lograr que usted abra los documentos adjuntos. El mensaje electrónico puede aparentar ser enviado por un amigo o colega, o el mensaje puede tener un nombre atractivo, como por ejemplo "Re/Fwd: TEXTO DIVERTIDO" o "En respuesta a su Solicitud". El mensaje también puede tener un vínculo con un sitio Web o prometer la limpieza de los virus de su computadora con sólo abrirlo. No abra ningún archivo adjunto a su correo electrónico — aún cuando parezca provenir de un amigo o colega — a menos que usted lo esté esperando o sepa cuál es su contenido. Si usted envía un mensaje de correo electrónico con un archivo adjunto, incluya un texto en el mensaje explicando de qué se trata.

Además, no reenvíe ningún mensaje electrónico advirtiendo la aparición de un nuevo virus. Puede ser un engaño y podría estar siendo utilizado para diseminar el virus. Si usted recibe un mensaje en cadena o un alerta de virus engañoso, hágaselo saber a quien se lo envió para poder detener la diseminación del mismo.

4. Use contraseñas sólidas. Los *hackers* pueden intentar robar sus contraseñas para acceder a la información personal almacenada en su computadora. Para dificultarles la tarea, utilice contraseñas con por lo menos ocho caracteres y que incluyan números o símbolos. Evite las palabras comunes; algunos *hackers* utilizan programas que pueden hacer intentos con cada una de las palabras que figuran en un diccionario. No utilice como contraseña su información personal, el nombre que utiliza para conectarse al sistema *(log in)* o teclas adyacentes en la configuración del teclado, como por ejemplo "asdfghjk".

No comparta su contraseña en línea o telefónicamente. Su Proveedor de Servicio de Internet *(Internet Service Provider, ISP)* nunca le debe pedir su contraseña.

5. Aproveche los dispositivos de seguridad de su programa *software*. Es muy probable que su navegador o explorador de Internet y su sistema operativo le brinden algunas opciones para incrementar su seguridad en línea. Consulte los menús "Herramientas" *(Tools)* y "Opciones" *(Options)* para saber cuales son las características de seguridad incorporadas. Probablemente usted cuente con numerosas opciones con respecto al tipo de archivos que usted desea aceptar de parte de otras computadoras. Si no comprende las opciones, consúltelas con la asistencia de la función "Ayuda" *(Help)*.

De igual manera, el programa *software* de su correo electrónico puede darle la opción de filtrar determinados tipos de mensajes, como por ejemplo mensajes de correo electrónico masivos no solicitados o correo electrónico basura. Pero es **usted** quien debe activar la función de filtro.

6. Haga copias de seguridad de los archivos importantes. Si usted sigue estas recomendaciones reducirá las probabilidades de ser víctima de un ataque de un *hacker* o de un virus. Pero ningún sistema es completamente seguro. Si usted tiene archivos importantes almacenados en su computadora, haga copias en un disco extraíble y consérvelos en un lugar seguro.

7. Si su computadora se infecta, actúe inmediatamente. Si su computadora es atacada por un *hacker* o infectada con un virus, desconéctese de Internet inmediatamente. Luego, active el escáner sobre la totalidad del sistema con una versión completamente actualizada de su programa antivirus.

Antes de reconectarse a Internet, piense de qué manera se pudo haber accedido a su computadora y que podría haber hecho usted para evitarlo. ¿Abrió un archivo adjuntado a un mensaje de correo electrónico y dejó escapar el virus? ¿Está desactualizado su programa *software* antivirus? Tome medidas para reducir las posibilidades de que le vuelva a suceder.

8. Reporte los incidentes graves. Si usted piensa que ha sido atacado por un *hacker* o que su computadora ha sido infectada con un virus, reporte el incidente a través de un mensaje electrónico enviado a su proveedor de servicio de Internet y al proveedor del *hacker* (en caso de que pueda saberlo). Con frecuencia el domicilio de correo electrónico de los proveedores de servicio de Internet se compone de la palabra *abuse* seguida del carácter @ y a continuación el nombre de su proveedor de servicio de Internet ISP ejemplo: abuse@nombredesuisp.com o la misma fórmula pero comenzando con la palabra postmaster ejemplo: *postamster*@nombredesuisp.com. De esta manera usted le informa a su ISP del problema en el sistema y lo ayuda a tomar recaudos para el futuro.

Si usted tiene almacenada en su computadora información de vital importancia o tiene planes de pasarse a un programa mejorado de alta velocidad para acceder a Internet, no olvide:

- **Instalar un *firewall***. Un *firewall* o pared de contención, es un programa *software* o *hardware* diseñado con un procedimiento de seguridad para bloquear el acceso de los *hackers* a su computadora. Un programa *firewall* correctamente configurado, hace que les sea más difícil a los *hackers* localizar su computadora e ingresar a sus programas y archivos. Un *firewall* es un programa que ofrece una protección diferente a la que ofrecen los programas *software* antivirus: un programa antivirus es un escáner que revisa las comunicaciones y archivos entrantes para detectar los archivos problemáticos; un programa *firewall* lo ayuda a permanecer invisible en Internet y bloquea todas las comunicaciones provenientes de fuentes no autorizadas.

- **Apague o desactive los dispositivos del programa *software* que no utiliza**. Es posible que desee desactivar ciertas características del programa *software* — mensajes instantáneos, impresora compartida, archivos compartidos — que generalmente están activadas cuando recibe su computadora. Debido a que estos programas facilitan el traspaso de información entre computadoras, esta característica se convierte en un punto de entrada excelente para los *hackers*.

La FTC trabaja en favor del consumidor para la prevención de prácticas comerciales fraudulentas, engañosas y desleales dentro del mercado y para proveer información de utilidad al consumidor con el objeto de identificar, detener y evitar dichas prácticas. Para presentar una queja o para obtener información gratuita sobre temas de interés del consumidor visite *www.ftc.gov* o llame sin cargo al 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. La FTC ingresa todas las quejas relacionadas a fraudes de Internet y sistema de telemercadeo, robo de identidad y otras quejas sobre prácticas fraudulentas a una segura base de datos en línea llamada Centinela del Consumidor *(Consumer Sentinel)* que se encuentra a disposición de cientos de agencias de aplicación de la ley civil y penal en los Estados Unidos y en el exterior del país.

septiembre 2002

Federal Trade Commission
Bureau of Consumer Protection
Office of Consumer and Business Education