

Consumer Reports WebWatch

Proyecto para prevenir delitos en línea (Web)

Hoja informativa #1: Diez consejos generales para su protección

Este es el primer artículo de una serie de hojas informativas editado por *Consumer Reports WebWatch*, con una subvención de la Oficina de la Procuraduría General del Estado de Nueva York.

Si tiene una computadora en su casa, ya sea portátil o de escritorio, debe de seguir los siguientes consejos. Recuerde: una conexión de banda ancha o *broadband* (de alta velocidad y sin marcar números de teléfono) al Internet es como tener una puerta adicional en su casa. Tome las mismas precauciones de seguridad con las computadoras de su casa que usted toma al salir de la misma.

1. Active una protección. Si su sistema operativo (como Microsoft Windows, XP o Vista) tiene una barrera de control de acceso o *firewall*, bloqueador de spam u otro tipo de aplicación incluida para proteger su computadora, asegúrese de que esté encendida. El *firewall* incluido con Windows Vista es adecuado. El de las computadoras Macintosh no es tan bueno, pero sus sistemas operativos son más difíciles de penetrar. ZoneAlarm 7.0 es gratuito para Windows XP si no ha bajado aún el paquete de servicio 2 para el XP.

2. Actualice y renueve. Ajuste su sistema operativo y software de seguridad para que se actualice automáticamente. Los programas contra el spam, spyware y detección contra virus incorporan archivos de “reglas” y “definiciones” que deben de permanecer actuales para detener los últimos peligros. Cuando su software le advierta que debe renovar su servicio, asegúrese de hacerlo, para que su protección no cese. Si está teniendo dificultad en bajar las actualizaciones en línea, pídale al fabricante de su sistema operativo que se las envíe en un CD-ROM.

3. Actualice su sistema operativo y su navegador o browser. Si tiene Windows XP o una versión anterior de Windows, considere Windows Vista que es más seguro. A pesar de que el software tiene algunos problemas, Vista le permite navegar en un ambiente protegido que impide que las amenazas en línea dañen su sistema operativo y contiene una barrera de protección de dos vías que bloquea peligros que vienen o van. Considere usar el browser de Firefox, que le notificará si está en un sitio riesgoso.

4. Aproveche las características de seguridad ofrecidas por los proveedores de servicios por Internet (ISP) y otros. La barra de herramientas de EarthLink (www.earthlink.net/software/free/toolbar), por ejemplo, incorpora un bloqueador contra el spam y los anuncios repentinos o “pop-ups”, un escáner contra los programas pirata o spyware y protección para su página principal del Internet. La barra de herramientas contra la pesca fraudulenta de datos (phishing) de Netcraft (www.toolbar.netcraft.com) advierte sobre los sitios conocidos de pesca fraudulenta de datos. El sitio de McAfee Site Advisor (www.siteadvisor.com), le advierte si McAfee ha examinado el sitio, y de ser así, lo que encontró, tal como virus, spyware, spam, anuncios repentinos, pesca de datos fraudulenta y estafas contra los consumidores. McAfee sobrepone los informes de un sitio con los resultados de la búsqueda en la Web y automáticamente bloquea el acceso a sitios que se aprovechan de las debilidades de un navegador de Internet.

5. Apague su computadora. Esto puede reducir la posibilidad de que una computadora maliciosa remota penetre la seguridad de su sistema operativo y obtenga acceso a éste. Además, así ahorrará energía.

6. Guarde su información personal. Nunca responda a un e-mail que solicite su contraseña, nombre de usuario, número de Seguro Social u otra información personal, no importa lo oficial que parezca. Si se le pide que llame a un número de teléfono, verifíquelo independientemente.

7. Considere comprar una computadora Macintosh. A pesar de que los dueños de estas computadoras enfrentan los mismos problemas con spam y phishing que los usuarios de Windows, tienen mucho menos que temer en cuanto a virus y spyware. Ya que las computadoras Apple son menos comunes que las máquinas basadas en Windows, los criminales cibernéticos obtienen menos dividendos por su inversión cuando concentran sus esfuerzos ilegales en las Macintosh.

8. Tenga cuidado con lo que baje del Internet. Un sinfín de juegos y aplicaciones gratuitas pueden ser útiles, pero muchos de éstos vienen repletos de virus y spyware. Trate de bajarlos solamente cuando se trata de fabricantes bien conocidos o sitios dignos de su confianza tal como www.download.com, www.snapfiles.com y www.tucows.com. Si no está seguro, vaya a StopBadware.org, un proyecto conjunto de *Consumer Reports WebWatch* y el Berkman Center for the Internet & Society. Hay más de 11,000 direcciones registradas de sitios con problemas.

9. Baje el software contra virus Avast! de manera gratuita. Si tiene dificultad al bajar el software contra virus que vino con su computadora, pruebe el Alwil's Avast!, gratis para uso casero y no comercial en www.avast.com. Si no usa Avast, asegúrese de usar el software antivirus y hacer exploraciones regularmente.

10. Utilice dos programas contra el spyware. El spyware es tan insidioso y, a veces, tan difícil de detectar que se necesita una protección doble. Utilice el mejor de los dos programas para bloquear el spyware en tiempo real. Use el otro como escáner cuando sospeche que algo se le haya escapado al primer programa. Una recomendación es el Spybot Search & Destroy (<http://www.safer-networking.org/index2.html>), que ofrecen gratis, pero considere hacer una donación.

Para más información y para mantenerse al día sobre otras maneras de proteger las computadoras de su casa contra invasores indeseados, marque como favorito el sitio de *Consumer Reports WebWatch*: <http://www.consumerwebwatch.org>.