CALIFORNIA
OFFICE OF
PRIVACY
PROTECTION

866.785.9663 *toll free*
916.653.3815 *fax*
www.privacy.ca.gov

Cómo protejer su computadora contra virus, piratas informáticos y espías

Hoy en día usamos nuestras computadoras para hacer muchas actividades distintas. Usamos el Internet para encontrar información, hacer compras y transacciones financieras, hacer deberes escolares, jugar juegos y comunicarnos con familiares y amigos. Como consecuencia, nuestras computadoras contienen una gran cantidad de información personal. Puede contener datos bancarios y otros datos financieros, así como información médica, que es información que queremos proteger. Si su computadora no está protegida los ladrones de identidad y otros estafadores podrían acceder y robar su información personal. Los productores de correo electrónico "chatarra", o *spam*, pueden llegar a usar su computadora como *"zombie drone"* para volver a transmitir spam que parezca haber sido enviado por usted. Se pueden llegar a depositar virus maliciosos o software espía *(spyware)* en su computadora, haciendo que funcione más lentamente o destruyendo sus archivos.

Al usar medidas de seguridad y buenas prácticas para proteger la computadora de su casa podrá proteger también su privacidad y la de su familia. Los siguientes consejos se ofrecen para ayudarle a reducir su riesgo mientras está conectado en línea.

◎ Instale un cortafuegos *(firewall).*

Un cortafuegos es un programa de software o un equipo físico que bloquea la entrada a piratas informáticos para que no puedan usar su computadora. Los piratas informáticos merodean el Internet de la misma manera que los vendedores telefónicos marcan números automáticamente al azar. Envían llamadas *(pings)* a miles de computadoras y esperan las respuestas. Los cortafuegos impiden que su computadora responda a estas llamadas al azar. Un cortafuegos bloquea las comunicaciones que se dirigen a, y provienen de, fuentes que usted no desea aceptar. Esto es especialmente importante si tiene una conexión de Internet de alta velocidad, como DSL o cable.

Algunos sistemas operativos tienen cortafuegos incorporados que inicialmente se encuentran apagados. No se olvide de activarlos. Para que un cortafuegos sea efectivo hay que configurarlo apropiadamente y actualizarlo a periodos regulares. Para obtener instrucciones específicas, consulte la función de "Ayuda" en línea.

◎ Use un programa antivirus.

El programa antivirus protege su computadora de virus que pueden destruir sus datos, hacer que su computadora funcione lentamente o deje de funcionar por completo, o permitir que envíe correo electrónico "chatarra" por medio de su cuenta. La protección antivirus analiza su computadora y los correos electrónicos entrantes para ver si hay virus, y los elimina. Tiene que mantener actualizado su programa antivirus para protegerse contra los virus más recientes que estén circulando por el Internet. La mayoría de

los programas antivirus tienen una función para descargar actualizaciones automáticamente cuando se encuentre en línea. Además, confirme que el programa esté siempre funcionando y verificando el sistema contra virus, sobre todo cuando descargue archivos de la Web o lea su correo electrónico. Configure su programa antivirus para que detecte la presencia de un virus al encender la computadora. También debe hacer un análisis detallado de su sistema con el programa antivirus por lo menos dos veces por mes.

◎ Use un programa contra software espía.

El software espía son programas instalados sin su conocimiento ni consentimiento que pueden vigilar sus actividades en línea y obtener información personal mientras que usted navega la Web. Algunos tipos de software espía, llamados *keyloggers*, registran cada tecla que oprime, incluyendo contraseñas e información financiera. Si recibe una ráfaga de avisos en ventanas emergentes, el navegador va a sitios Web a donde usted no quiere ir, o su computadora comienza a funcionar más lentamente, todos estos pueden ser signos de que su computadora está infectada con software espía.

Algunos programas antivirus también tienen protección contra software espía. Para activar las funciones de protección contra software espía lea la documentación de su programa antivirus para obtener instrucciones. También puede comprar programas separados contra software espía. Mantenga el programa actualizado y ejecútelo regularmente.

Para evitar el software espía en general, descargue información sólo de sitios Web conocidos y de confianza. Muchos programas "gratuitos" pueden incorporar software espía. No haga clic en ventanas emergentes ni en correo electrónico "chatarra".

◎ Administre su sistema y su navegador para proteger su privacidad.

Los piratas informáticos tratan constantemente de encontrar defectos o resquicios en los sistemas operativos y navegadores Web. Para proteger su computadora y la información que contiene, ajuste el nivel de seguridad de su sistema y su navegador a "mediano" o más. Para saber cómo hacerlo, use el menú "Herramientas" *(Tools)* u "Opciones" *(Options).* Actualice su sistema y su navegador regularmente, usando, cuando pueda, el sistema de actualización automática. Microsoft ofrece un servicio llamado *Windows Update*. Descargará e instalará actualizaciones al sistema operativo Microsoft Windows, Internet Explorer, Outlook Express y también instalará actualizaciones de seguridad. Los parches *(patching)* también se pueden usar automáticamente para otros sistemas, como para el sistema operativo de la computadora Macintosh.

◎ Use una contraseña robusta; no se la dé a nadie.

Proteja su computadora contra intrusos al usar una contraseña difícil de adivinar. Use contraseñas robustas con por lo menos ocho caracteres, una combinación de letras, números y caracteres especiales. No use una palabra que se pueda encontrar fácilmente en el diccionario. Algunos piratas informáticos usan programas que pueden probar todas las palabras del diccionario. Trate de usar una frase que le ayude a recordar su contraseña, usando la primera letra de cada palabra en la frase. Por ejemplo, @pN9YlV@c – "Al preso número 9 ya lo van a confesar". Proteja su contraseña de la misma manera que protegería la llave de su

casa. Es, al fin de cuentas, la "llave" de su información personal.

◎ Use las opciones de seguridad de su red inalámbrica.

Si usa una red inalámbrica en su casa, asegúrese de tomar las precauciones necesarias para protegerla contra piratas electrónicos. El primer paso es encriptar las comunicaciones inalámbricas. Use un enrutador inalámbrico con capacidad de encriptación y actívela. La encriptación llamada WPA se considera más robusta que la WEP.[1] Su computadora, enrutador y otros equipos tienen que usar la misma encriptación. Si su enrutador tiene habilitada la función *broadcasting*, desactívela. Anote el nombre de SSID del enrutador para poder conectar sus computadoras a la red manualmente.[2] Los piratas informáticos conocen las contraseñas por defecto de este tipo de equipos. No se olvide de cambiar el identificador por defecto de su enrutador y la contraseña administrativa que viene de fábrica. Cuando no esté usando su red inalámbrica, apáguela.

Recuerde que los lugares públicos con acceso a redes inalámbricas *(hot spots)* no son seguros. Lo mejor es no acceder ni enviar información personal delicada usando una red inalámbrica pública.

◎ Si comparte sus archivos, tenga cuidado.

A muchos consumidores les gusta compartir archivos digitales, como música, películas, fotos y programas. Los programas para compartir archivos, que conectan a su computadora con una red de computadoras, con frecuencia se pueden conseguir gratis. Pero, estos programas presentan una serie de riesgos. Cuando se conecta a una red de computadoras que comparten archivos es posible que permita la copia de archivos que no tenía intención de compartir. Podría descargar un virus o software espía que haga que su computadora sea vulnerable a piratas informáticos. También podría violar la ley al descargar material protegido por derechos de autor.

◎ Haga sus compras en línea en forma segura.

Cuando haga compras en línea, verifique el sitio Web antes de ingresar su número de tarjeta de crédito u otra información personal. Lea las normas de privacidad y fíjese si hay una opción para no tener que compartir información. (Si no hay normas de privacidad publicadas, ¡tenga cuidado! Haga sus compras en otro lado). Aprenda a darse cuenta cuando un sitio Web es seguro. Verifique que aparezca "https" en la barra de direcciones o un símbolo de candado cerrado en la parte inferior de la ventana del navegador. Éstos son signos que indican que su información será encriptada o cifrada, protegiéndola de los piratas informáticos a medida que se mueve por el Internet.

---

[1] WEP son las siglas en inglés de *Wired Equivalent Privacy*, un protocolo de seguridad que encripta los datos enviados y recibidos por los dispositivos inalámbricos de una red. WPA son las siglas en inglés de *Wi-Fi Protected Access:* un protocolo de seguridad desarrollado para corregir los defectos del WEP.

[2] SSID son las siglas en inglés de *Service Set Identifier*, el nombre que el fabricante asigna a un enrutador de red inalámbrica. Es posible que el mismo SSID sea asignado a todos los equipos del mismo tipo.

◎ Padres, tomen el control.

No dejen que sus hijos pongan en riesgo la privacidad de su familia. Enséñenles a navegar el Internet en forma segura. Instale programas de control paterno para sus hijos menores. Estos programas limitan los sitios Web que sus hijos pueden visitar. Pero recuerde… ningún programa puede sustituir la supervisión de los padres.

◎ Información adicional

Hoja 6 de información al consumidor: Cómo leer normas de privacidad
Hoja 9 de información al consumidor: Cómo proteger la privacidad de su hijo en línea

Información para el consumidor de la Oficina de Protección de Privacidad de California, que puede encontrar en www.privacy.ca.gov.

OnGuard en línea

Consejos prácticos del gobierno federal y las empresas de tecnología para ayudarle a estar en guardia contra el fraude de Internet, mantener la seguridad de su computadora y proteger su información personal. Visite www.onguardonline.gov.

Guía en línea a herramientas prácticas de privacidad

Recursos de seguridad para computadoras del Centro de Información sobre Privacidad Electrónica (EPIC, por sus siglas en inglés), una organización sin fines de lucro, que se pueden obtener en: www.epic.org/privacy/tools.html.

Evaluaciones de productos

Consumers Union, una organización sin fines de lucro, le ofrece estrategias sobre cómo mantener la seguridad de su computadora. Para sugerencias en línea sin costo, visite www.consumerreports.org. También están disponibles para los suscriptores de *Consumer Reports* y en las bibliotecas públicas clasificaciones de productos de software de seguridad así como una guía de compra.

La revista *PC Magazine*, febrero de 2010, tiene evaluaciones de productos en su artículo, "The Best Security Suites for 2010", disponible en línea de forma gratuita en: www.pcmag.com/article2/0,2817,2333448,00.asp.

La revista *PC Magazine*, junio de 2009, tiene evaluaciones de software gratuito, "12 Free Security Software Tools", disponible en línea de forma gratuita en: www.pcmag.com/article2/0,1759,2304349,00.asp.