Como Proteger su Computadora en Contra de “Hackers” y Programas Maliciosos

Felix Uribe
Uribe100.com

Gracias a la Internet, millones de personas en todo el mundo pueden comunicarse, trabajar, estudiar, socializarse y mucho más. De la misma manera, millones de computadoras se encuentran continuamente a la merced de individuos cuyo solo propósito es de utilizar programas maliciosos diseñados específicamente para atacar, dañar y obtener información ilegalmente de personas e instituciones que usan la Internet.

Una solución a este problema es la instalación y el uso de programas de seguridad diseñados exclusivamente para proteger la computadora y sus programas. A través de varios años he sido testigo de su gran utilidad. Aunque los riesgos de que una computadora conectada al internet sea atacada o invadida con programas maliciosos son grandes, de la misma manera podemos frenar o minimizar sus impactos con la instalación y el uso de estos programas de seguridad.

Programas de Antivirus

Si usted ha utilizado computadoras por varios años, puede ser que haya sido testigo de las consecuencias de lo que significa tener un "virus" informático en la computadora. Un virus es un programa diseñado especialmente para propagarse de computadora en computadoras "infectándolas" a todas en su paso.

Regularmente los virus vienen adjuntos a archivos que han sido infectados y se propagan causando daños que en la mayoría de los casos son catastróficos (por ejemplo: borrando información en el disco duro, paralizando la ejecución de la computadora y provocando la pérdida de mucho dinero invertido en la restauración de servicios y en la productividad).

Dado que la Internet es una red utilizada por más de un billón de usuarios en todo el mundo, un virus puede infectar a millones de computadoras en cuestión de un par de horas. Un buen ejemplo es el famoso virus llamado "Klez", que apareció en el año 2001 y que desde entonces ha infectado a millones de computadoras en todo el mundo. Cada año el nombre de este virus es modificado, sin embargo las características siguen siendo las mismas. El medio que se utiliza para propagar este virus es el correo electrónico (e-mail). Una vez que el virus se encuentra en una computadora, se apodera del programa de correos y automáticamente empieza a enviar correos electrónicos infectados a todos los que se encuentra en el libro de direcciones del usuario.

Además del correo electrónico los virus usan otros medios para su propagación, tales como mensajes instantáneos (instant messaging), programas de par a par - o de punto a punto (peer-to-peer o P2P) y los navegadores o exploradores web (web browsers).

La mejor defensa contra estos virus es la instalación en la computadora de programas llamados antivirus. Estos programas pueden detectar a un virus incluso antes que ataque y que lleve a cabo sus destructores objetivos como los ya mencionados anteriormente.

Programas Antiespías

Los programas espías (spyware) son aquellos que una vez instalados pueden recopilar y mandar información (archivos, claves, información personal acerca del usuario, etc.) a otras computadoras sin el conocimiento o permiso del usuario o sistema en el cual residen. Muchos de estos programas son famosos por causar que la computadora trabaje de forma lenta y disparatada; así como la aparición de incómodas "ventanas emergentes" (pop-up windows) las cuales suelen ser utilizadas con el objetivo de mostrar avisos de manera intrusiva.

Otros programas espías suelen tomar el control total de la conexión de Internet de la computadora. En los pasados años, sitios de Internet dedicados al intercambio de archivos que utilizan la tecnología punto a punto (Peer-to-Peer) facilitaron la propagación exponencial de estas aplicaciones.

Programas Cortafuegos Personales

La función de los programas cortafuegos personales (personal firewalls o desktop firewalls) es limitar, controlar o parar el tránsito de información entre la computadora en el cual residen y todos aquellas computadoras o equipos que se comunican con ella.

Como habíamos mencionado anteriormente, muchas personas en el mundo tratan de penetrar el sistema operativo de las computadoras con el objetivo de dañarlas o de extraer información sin el conocimiento o autorización del usuario. Los cortafuegos personales evitan que esto suceda, ya que funcionan como si fueran un guardia que tiene la habilidad de saber quiénes tienen autorización para ingresar.

Programas de Encriptación

La encriptación es el proceso para volver ilegible cualquier tipo de archivo (fotos, música, documentos, etc.). La información una vez encriptada sólo puede leerse aplicándole una clave. Cuando los archivos están encriptos solo la persona con la clave puede verlos, de esa manera pueden ser almacenados o transferidos y no pueden ser vistos o accesados por terceros.

Tenemos que reconocerlo, existe muchos tipos de información que no queremos que otros vean (documentos personales, financieros, empresariales, etc). Una vez que la información ha sido encriptada, puede ser almacenada en un medio inseguro, o transmitida por una red insegura (como Internet), y aun así permanecer secreta. Luego, la información puede ser desencriptada a su formato original. Un ejemplo seria si su computadora se pierde, es robada o es accesada por alguien, si los archivos importantes están encriptos, puede estar seguro que nadie podrá verlos.

Medidas de Seguridad en General

Es un constante trabajo mantenerse libre de las amenazas de los programas e individuos maliciosos que constantemente azotan la Internet; nosotros mismos debemos de desarrollar y ejercer buen sentido común para prevenir y detectar el peligro. Dos de los mejores consejos que uno puede seguir para evitar estas amenazas son:

- Nunca habrá un correo electrónico con enlaces a sitios en la Internet o archivo adjunto que provenga de personas que no conozca, lo que tiene que hacer es eliminarlo inmediatamente. Si conoce a la persona pero no esperaba el mensaje o duda de su contenido, verifique la veracidad del mensaje contactando a la persona que se lo envió; más vale prevenir que tener que lamentarse.

- Mantenga al día su computadora con todos los parches (patches) nuevos tanto como para el sistema operativo así como para los otros programas que residen en la computadora.

Para obtener y ver más información acerca de estos programas y muchos otros dedicados a la prevención y eliminación de programas maliciosos, visite www.uribe100.com.