8 pasos para prevenir un ciberataque

No hay fórmulas infalibles para proteger tu ordenador, pero siguiendo unos consejos básicos puedes ponerle el camino difícil a los atacantes.

Alejandro García

¿Qué pasos mínimos hay que seguir para prevenir un ataque?

1. Proteger los equipos

Cualquier dispositivo electrónico que se tenga en casa o la oficina debe estar completamente actualizado. Las clásicas actualizaciones del sistema pueden ser molestas pero son fundamentales pues muchas corrigen agujeros de seguridad. Además debe contarse con antivirus y antimalware que sean avalados por la comunidad a la hora de detectar archivos maliciosos.

2. Contraseñas fuertes

Ni el nombre de nuestros hijos, ni el de nuestra mascota, ni el equipo de fútbol favorito. Por supuesto no poner sólo números y que encima estén relacionados con la contraseña de otro tipo de cuenta como puede ser la bancaria. Siempre hay que combinar números, letras mayúsculas, minúsculas y símbolos. De esta forma es más difícil conseguirlas y que no aparezcan en librerías estándar.

3. Utilizar protocolos de seguridad

Es un paso imprescindible pues de lo contrario las transferencias de archivos a un servidor pueden volverse completamente vulnerables. Si además se accede o se mandan datos a través de fuentes desconocidas o sitios de poca confianza se está facilitando el ciberataque.

4. Comprobar la autenticidad de enlaces y perfiles

Es muy común sufrir ataques a través de *phishing* mediante el cual se intenta adquirir información confidencial de forma fraudulenta, normalmente a través del email. Hoy en día **en las redes sociales se crean perfiles falsos** para captar estos datos, sobre todo por medio de cuentas no oficiales de empresas con el fin de engañar.

5. Evitar dar datos personales

Principalmente en las propias redes sociales y en cualquier tipo de página web que no sea de fiar. Lo recomendable es sólo utilizarlos cuando sea indispensable, pero aún así grandes compañías han sufrido el robo de información de sus clientes por lo que **no hay una seguridad máxima para esta cuestión**. También hay que tener constancia de con quién compartimos nuestra información en la red, sea a través de imágenes o texto.

6. No descargar contenido pirata

En la red son numerosas las opciones para bajar software o archivos multimedia con la mejor música o películas. Son una fuente propicia para intentar colocar programas maliciosos en el sistema y así poder realizar un ataque. Incluso aunque la descarga sea legal es necesario comprobar previamente que el sitio web no es sospechoso.

7. Realizar una copia de seguridad

Es algo fundamental pues si sufrimos algún tipo de ataque o tenemos algún problema siempre podremos **recuperar la información perdida.** En un primer momento puede que provoque pereza hacerla pero a la larga se agradece tener ese respaldo.

8. Denunciar a las autoridades

Siempre que nos encontremos con un contenido que no sea adecuado o con una página que pueda suponer un riesgo para el usuario lo mejor es **denunciarlo a la policía** o cuerpos encargados de este tipo de procesos. De lo contrario se está permitiendo que sigan operando contra el sistema cibernético.

Alejandro García escribe en Geekpunto.com