



Cada día aumenta considerablemente el contenido en Internet, sea del tipo que sea, y a su vez, aumentan las amenazas informáticas en contra de organizaciones o personas, principalmente mediante campañas de malware de cualquier tipo, como troyanos, rootkits, adware, spyware, entre otros.

Debido a esto, contar con un buen antivirus es algo muy importante antes de navegar por la red, ya que aunque visites sitios confiables, siempre estás expuesto a virus informáticos.

Aquí tienes cinco razones para utilizar un antivirus

1.- Virus Troyano

[Virus Troyano](#). Este es el tipo de malware que más se propaga en Internet, desde hace muchos años. En caso de no contar con protección antivirus, la infección con un troyano podría ocasionar la pérdida de tu información sensible.

Un troyano es un malware que normalmente se presenta como un programa legítimo, pero al ejecutarlo, brinca al pirata informático acceso remoto. Su nombre proviene de la historia del caballo de Troya, mencionado en la Odisea de Homero.

Sin embargo, al contar con un software antivirus actualizado con la última versión de la base de datos, es posible evitar la infección y alertar cuando el equipo esté en peligro.

2.- Limpiar ordenador

[Limpiar ordenador](#). Se trata de otra acción imprescindible para evitar el mal funcionamiento del sistema, con el fin de evitar saturación del disco duro, eliminar archivos que no sirven, analizar en busca de amenazas, entre otras acciones que mantendrán al ordenador en un funcionamiento óptimo.

Algunos antivirus ya incluyen esta herramienta integrada, para que además de proteger al ordenador contra virus, lo mantendrán libre de archivos no deseados y por ende, funcionando



a la perfección.

3.- Protección contra Ransomware

Un antivirus actualizado podría evitarte muchos dolores de cabeza, especialmente ahora que los ransomware están en auge, pues una licencia de software antivirus puede ser mucho más barata que tener que pagar un rescate para descifrar tus archivos, y que al final podría no funcionar.

Un ransomware es un malware que al activarse, restringe el acceso a determinadas carpetas y archivos del sistema operativo infectado, pidiendo un rescate a cambio del descifrado de los archivos, generalmente solicitado en criptomonedas como Bitcoin.

Este tipo de ataques ha ido en crecimiento en los últimos años, el más grande ocurrió en 2017, con el ransomware WannaCry, que afectó a miles de computadoras en casi todo el mundo.

4.- Protección contra phishing

Loguearte en distintos sitios web es una tarea de todos los días, pero introducir tus contraseñas puede resultar algo peligroso, especialmente cuando se trata de banca en línea o cualquier otro servicio financiero. Un hacker podría imitar un sitio web legítimo de un banco y hacer que ingreses tus datos de ingreso para robarlos.

Un buen antivirus te ayudará al advertir que estás ingresando datos en un sitio web inseguro, lo que hará que verifiques en qué sitio web te encuentras realmente.

5.- Protección de información personal

Algunos antivirus incluyen la opción de poder encriptar tu información confidencial, como nombres de usuario y contraseñas, con el fin de que no puedan ser vistas por algún intruso en el ordenador.



Esto es de mucha ayuda cuando utilizas muchas contraseñas (debería ser una contraseña única por cada servicio) y temes olvidarlas. Anotarlas en papel o guardarlas en el ordenador es algo inseguro, por lo que el uso de software especializado podría ser tu mejor opción.

La próxima vez que pienses que no necesitas un antivirus, recuerda que a diario se registran nuevos malware, que actúan de muchas formas diferentes, si eres usuario de Windows, un antivirus es una prioridad.