Guía práctica: cómo eliminar malware de tu ordenador

Virus, gusanos, troyanos y demás especímenes maliciosos acechan a ordenadores y redes. La llegada de malware de todo tipo y para todas las plataformas, el robo de datos, el ciberespionaje o la invasión a la privacidad, cotizan al alza en la Internet mundial, obligando a usuarios y empresas a tomar **medidas pro-activas para su control**.
Aunque la prevención es siempre la primera y principal línea de defensa, no siempre es posible mantenerse a salvo de una infección y cualquier usuario habrá tenido que ponerse a la tarea de eliminar malware en alguna ocasión.

Incluso aunque uses alguna solución de seguridad, si notas que tu equipo va más lento de lo normal; el sistema muestra errores aleatorios; el navegador web se congela luchando para deshacerse de anuncios extraños o no puedes acceder a tus documentos, seguramente padezcas una infección digital que además de impedir el uso habitual del equipo pone en riesgo tus datos.
Si es tu caso y no puedes eliminar la infección con tu antivirus o no usas ninguna solución de seguridad, es hora de enfrentarte a un proceso para eliminar malware de un PC con Windows, como el que proponen desde BusinessNow y que te recomendamos:

Intenta salvar archivos

Las copias de seguridad son el mayor “salvavidas” para contrarrestar cualquier tipo de virus informáticos y en ocasiones con algunos de ellos la única solución. Si no la habías realizado previamente, puedes intentar salvar documentos, fotos, vídeos y cualquier otro tipo de información personal o profesional que no puedas perder incluso aunque estén infectados, **para intentar recuperarlos después en un sistema limpio**.
Se incluyen en este grupo los más peliagudos que serán los infectados por los mencionados Ransomware (con archivos cifrados habitualmente), para poder recuperarlos cuando se publiquen herramientas para su descifrado. Por supuesto, **solo copiar los**

archivos a una unidad externa controlada, ya que no debemos ejecutar ninguno de estos archivos hasta su limpieza porque pueden infectarnos otros equipos.
Para realizar estas copias podemos intentar dos métodos. El modo seguro de Windows, también llamado "a prueba de errores" o "arranque avanzado" es una forma del inicio del sistema que solo carga controladores y servicios más básicos y es de; **utilidad para encontrar y resolver problemas del sistema operativo** que no son posibles de resolver en un arranque estándar donde suele cargarse el código malicioso.
Si no es posible realizar las copias de seguridad con la función anterior, debemos utilizar **otro método más avanzado** para acceder a los archivos de un equipo infectado, como es usar discos de rescate (auto arrancables desde unidades ópticas, pendrives o discos externos USB) tanto los nativos de Windows para recuperación del sistema, como soluciones especialmente preparadas especialmente para resolución de problemas como Hiren's BootCD o Ultimate Boot CD.

Desinfecta el equipo

Una vez que hayamos intentado poner a salvo nuestros archivos esenciales es la hora de comenzar la desinfección, si bien conviene indicar que no siempre es posible dependiendo del malware en cuestión y finalmente nos obligará a realizar una instalación limpia del todo el sistema y aplicaciones.

Intentamos la desinfección utilizando un medio de arranque para rescate contra virus. Un medio efectivo teniendo en cuenta que una gran mayoría de malware se **carga/oculta en la memoria** complicando su detección/eliminación una vez que arranca el sistema operativo. Todos los grandes proveedores de seguridad ofrecen la posibilidad de crearlos. La mayoría son Linux en formato "Live CD" (creados y auto arrancables desde unidades ópticas, pendrives o discos externos USB), que podemos utilizar en el PC independientemente del sistema y sin tener que instalar nada en él. **Diez buenas soluciones** que podemos utilizar son las siguientes:

- **Kaspersky Rescue Disk**
- **ESET SysRescue Live**
- **Bitdefender Rescue CD**
- **AVG Rescue CD**
- **Panda SafeDisk**
- **Trend Micro Rescue Disk**
- **Norton Bootable Recovery Tool**
- **Avira Rescue System**
- **F-Secure Rescue CD**
- **Avast**

Su funcionamiento es muy sencillo, no sin antes arrancar el equipo con el medio de rescate creado. Todos actualizan la firma de virus y el programa, comenzando a continuación el escaneo y la desinfección del malware en su caso.

Desde el explorador de archivos del Live CD podremos acceder a la unidad donde está instalado el sistema principal. Útil si queremos borrar algún archivo o directamente para hacer las copias de seguridad de los archivos esenciales que vimos en el apartado anterior.

Recupera el sistema

Si la limpieza del malware fue efectiva, retira el disco de rescate e **intenta arrancar el equipo de la forma habitual**. Si es posible instala la mejor solución de seguridad que tengas disponible y revísalo de nuevo en la búsqueda de virus. Si el sistema funciona normalmente hay que comprobar si todas las aplicaciones que teníamos instaladas funcionan correctamente. También controladores y drivers. Incluso si el sistema operativo está limpio y funcionando, puede ser que existan daños.
Si a pesar de los esfuerzos anteriores **no hemos sido capaces de acabar con la infección, solo nos queda la reinstalación del sistema operativo**. Si tenemos una partición de recuperación o discos del sistema como los que ofrecen los fabricantes, será lo primero a utilizar para revertir el equipo a su estado de fábrica.
Restaurar el sistema operativo utilizando la misma herramienta del sistema operativo, es otra alternativa sencilla al uso de copias de seguridad o a una instalación desde cero. Si no funciona nada de los anterior, toca realizar una instalación limpia de todo el sistema, formateando la partición para asegurarse de la eliminación del virus en el equipo.
Por último, puedes recuperar tus datos y aplicaciones no sin antes **escanear y desinfectar a fondo** los archivos de datos que teníamos guardados en la copia de seguridad. Asegúrate bien de su limpieza antes de volverlos a copiar en el equipo porque podrían ser la causa de la infección y tener que repetir de nuevo todo el proceso.

Impide nuevos daños

La partición del sistema está limpia pero también debemos comprobar el resto de particiones del equipo y también de **toda la red local** si está conectado, porque el virus ha podido llegar por esa vía e infectar de nuevo el equipo. Puedes comprobarlo con los discos de rescate creados anteriormente y también con una solución de seguridad instalada en el equipo, porque hoy por hoy, por mucha precaución que tengamos, es complicado mantener limpio un ordenador personal sin ninguna protección adicional y al menos, es recomendable utilizar el Windows Defender que viene instalado en sistemas Windows.
También es recomendable el cambio de contraseñas. Una buena parte del malware actual infecta los equipos con el objetivo de obtener las contraseñas de acceso. No es improbable que estén en manos de terceros a pesar que tu sistema esté limpio.Por ello y después de una infección, es **altamente recomendable cambiar todas las contraseñas**, desde las locales para autenticación de Windows a las utilizadas en los servicios de Internet, especialmente las destinadas a servicios financieros o de comercio electrónico.

Prevención, siempre por delante

Para finalizar, insistir en que la **prevención es la primera y principal línea de defensa**, observando la precaución debida en los sitios web por los que navegamos; las aplicaciones que instalamos; la recepción de correos electrónicos y adjuntos; las descargas o el uso de redes sociales; la imprescindible actualización de sistema operativo y aplicaciones y el uso de una buena solución de seguridad.