Cómo navegar sin marejada por Internet

- ***Los virus, los bulos o la utilización ilícita de datos personales ajenos para usos malintencionados son algunas de las principales amenazas en la red.***

- ***Para navegar sin marejada por Internet, lo mejor es tener en cuenta varias recomendaciones.***

27 de septiembre de 2024

Un navegador es una aplicación o programa informático que permite visualizar y explorar páginas web. Aunque hay muchos en el mercado, algunos de los más habituales y valorados son Chrome, Microsoft Edge, Safari o Firefox. Y precisamente el primero de los consejos para una navegación online segura pasa por **utilizar versiones actualizadas de los navegadores**. Si la versión es reciente, mejorará el rendimiento, nos proporcionará nuevas funcionalidades y resolverá posibles fallos o vulnerabilidades. También conviene actualizar el sistema operativo (ya sea Windows, Apple, Linux…) y todas las aplicaciones que tengamos instaladas.

Un gran aliado para evitar sustos son **los antivirus, que se encargan de detectar y eliminar los virus en el equipo informático**. Aunque la protección que otorgan no es del 100%, los riesgos se minimizan si el antivirus está actualizado, ya que cada día aparecen nuevos virus.

Otro consejo pasa por navegar por sitios web conocidos. De hecho, hay **algunos navegadores que alertan del potencial riesgo de hallarse ante una página peligrosa**, por lo que, si te encuentras con una advertencia de este tipo, lo mejor es hacerle caso.

Por otro lado, si vas a dejar desatendido tu equipo mientras está conectado, es **importante bloquearlo con contraseña de usuario hasta que vayas a recuperar el control visual sobre él**. Esta recomendación es todavía más encarecida si se accede a equipos en lugares públicos o en el entorno laboral. Al hilo de las contraseñas, lejos de optar por las recurrentes 1234, 0000 o demás fórmulas sencillas fáciles de descifrar, es muy importante contar con una **clave robusta con más de 8 caracteres en la que tengan cabida tanto mayúsculas como minúsculas, además de dígitos y caracteres especiales** (como interrogantes, exclamaciones, símbolos matemáticos, signos de puntuación…).

También es mejor usar una contraseña distinta en función del uso que le vayamos a dar y no repetir clave para el correo electrónico, las redes sociales, la banca electrónica… **Un gestor de contraseñas puede sernos de gran utilidad, ya que guarda las claves de manera segura** y no hay que fiarlo todo a nuestra memoria.

La ejecución de un programa puede llevar pareja la instalación de código malicioso en el equipo, de manera que, **si tú no lo has solicitado, debes cancelar cualquier ejecución de programas**. De hecho, si no estás convencido del origen de lo que estás descargando, es mejor no hacerlo o verificarlo previamente.

También hay que tener presente que navegando nos podemos topar con Hoax lo que, traducido a un idioma inteligible, quiere decir que **pueden aparecer mensajes electrónicos que contienen *fake news* o bulos** que pretenden sensibilizar al usuario para que realice una aportación económica.

No olvides tampoco ir con **sumo cuidado con tus datos personales**. A veces no somos conscientes de que los exponemos y pueden ser accesibles para otras personas, lo que permite que sean empleados de manera malintencionada e ilícita por otros usuarios.