



Riesgos al navegar por Internet

En los tiempos que vivimos las amenazas a una computadora no solamente provienen de los archivos que bajas o de las aplicaciones que ejecutes, sino también estas en riesgo cada vez que abres tu navegador y viajas de una página a otra. Muchas veces los riesgos a la seguridad de tu equipo no se encuentran en el sitio web que estas visitando sino en contenido que proviene por parte de terceros, como por ejemplo la publicidad que pasan los filtros de los proveedores y que en realidad son amenazas disfrazadas.

¿Qué tan seguro son los navegadores más populares?

Al navegar en la red interactuamos con técnicas de rastreo, cookies (pequeña información usada para consultar la actividad previa del usuario), etc.. Para poder aumentar la seguridad a la hora de navegar por Internet muchos de los navegadores como Internet Explorer, Google Chrome, Mozilla Firefox, etc.. traen una serie de opciones las cuales uno tiene que habilitar para poder tener un mejor nivel de seguridad, el problema con esto es que en ocasiones el usuario difícilmente se da a la tarea de investigar cuales son estas opciones, donde ubicarlas y como activarlas o desactivarlas, añadido a esto cada vez que hay alguna actualización, puede que cambien o no estas opciones y pueda que vuelvan a su estado desactivado por default. Si bien todos estos también tienen la opción de navegación privada no es muy confiable ya que el hecho de permanecer 100% incógnito durante la navegación con la web choca con el modelo de negocios de estas compañías antes mencionadas, ya que todas ellas venden información de los hábitos de navegación de sus usuarios.

Alternativas a los navegadores más populares

Existen otros navegadores los cuales dependiendo de tus hábitos de navegación, te podrían ofrecer más protección durante tus sesiones en línea, algunos de estos navegadores son Maxthon, Aviator, Tor, Comodo Dragon, entre otros. La razón por que estos navegadores son más seguros que los convencionales es por que la mayoría de ellos tienen en mente primero al cliente antes que el modelo de negocio, tienen más herramientas enfocadas a la privacidad y algunos de ellos traen las características relacionadas con la seguridad activadas por default. Esto significa que cada vez que accedas a una página web se bloquearán las cookies, el tracking realizado por las empresas de anunciantes y redes sociales, además de eliminar el historial de navegación así como bloquear anuncios emergentes que te llevan a un liga o página no deseada.

Todo estas opciones de seguridad tienen sus consecuencias ya que todos estos bloqueos significan también bastantes incomodidades, especialmente cuando visitas muy seguido los mismos sitios web, también en ocasiones algunos de ellos puedan tener problemas de compatibilidad con contenido que se ejecuta en JAVA. Lo bueno es que entre sus opciones también encontramos las que nos permiten añadir los sitios a una lista blanca de acceso una vez que lo hayamos auditado debidamente.

Puedes hacernos llegar tus comentarios al siguiente correo:

boletin.tecnico@aaareynosa.org.mx