Consejos Para Mantenerse Seguro En Una Red Wi-Fi Pública

Sabemos que el encontrar una **red Wi-Fi pública** o abierta es una tentación bastante grande. Ademas, puede llegar a ser bastante conveniente, pero la seguridad de la misma puede convertirse en un problema. No importa el dispositivo que uses, ya sea un portátil, SmartPhone, Tablet u otro, siempre estarás expuesto a un ataque para vulnerar tus datos.

A continuación te compartimos algunos consejos sobre lo que debes tener en cuenta al utilizar puntos de acceso Wi-Fi sin protección, en cualquier dispositivo. Con esto, podras navegar tranquilamente sin correr el riesgo que roben tus datos mas sensibles.

Seleccione Una Red Con Inteligencia

Evita la tentación de conectarte a una red Wi-Fi de llamativo nombre. Asegurate de no seleccionar cualquier red que esté abierta o que no sea conocida. Por ejemplo, si estás en una cafetería o en un lugar público, asegúrate de verificar el nombre de la red con los empleados o en los avisos, antes de

conectarte.

Es bastante fácil para alguien que quiere interceptar los datos con un ataque de hombre en el medio, para configurar una red que parezca ser real y sin fraude. Si te conectas usando Windows, asegúrate de desactivar el uso compartido de archivos y marcar la conexión **Wi-Fi como red pública**. Puedes encontrar esta opción en el **panel de control > Red y Centro de Intercambio> Cambiar configuración avanzada de uso compartido**. Bajo el título público, des habilite la opción de intercambio de archivos. También es posible que desee **activar el Firewall de Windows** al conectarse a una red pública. Estos ajustes también se encuentran en Panel de control> Firewall de Windows.

En **Mac**, abre **Preferencias del sistema** y navega hasta el icono **Compartir**. Luego, quite la marca de la casilla junto a **Uso compartido de archivos**. He aquí un resumen completo sobre cómo deshabilitar el uso compartido y la eliminación de opciones de uso compartido de la carpeta pública en el **home de OS X**.

Use Una VPN

La creación de una red privada virtual (VPN) es una de las mejores maneras de mantener su sesión de navegación en secreto. Un cliente VPN, cifra el tráfico entre el dispositivo y el servidor VPN, lo que significa que es mucho más difícil para un intruso rastrear tus datos.

Si aún no dispone de una VPN, existen otras opciones disponibles. Una aplicación gratuita es **SecurityKISS** que ofrece **acceso VPN** sin publicidad con datos limitados a 300 MB / día.

Existe un cliente dedicado de Windows disponible, pero para **dispositivos iOS y Android**, puedes registrarte para obtener una cuenta gratuita que generará un nombre de usuario y una contraseña. A continuación se le enviará una lista de servidores que se pueden introducir manualmente en el dispositivo para configurar el VPN correctamente.

Existen varios **servicios VPN** disponibles, incluidas las opciones de pago y gratuitos. Vale la pena investigar para averiguar cuál es el mejor según tus necesidades, especialmente si eres un usuario que maneja una gran cantidad de datos.

Disconnect.me ayuda a proteger contra el robo de sesión a través de las extensiones del navegador de Chrome, Opera y Safari, pero en el frente VPN también ofrece una aplicación para Android independiente llamada Secure Wireless que detecta automáticamente las **redes Wi-Fi inseguras** y activa una VPN cuando es necesario.

Habilitar HTTPS

Puedes forzar el uso del protocolo HTTP en tu navegador a través de una extensión, tal como HTTPS Everywhere. Esta extension está disponible para Chrome, Firefox, Firefox para Android, y Opera.

Es importante señalar que **HTTPS Everywhere** funciona mediante la activación de cifrado en todas las piezas compatibles de la página web. Como se indica en su FAQ:

> *«HTTPS Everywhere depende por completo de los elementos de*

seguridad de los sitios web individuales que se utilizan;. Activa los elementos de seguridad, pero no puede crearlos si no existen ya Si utiliza un sitio no soportado por HTTPS Everywhere o un sitio que ofrece información de una manera insegura, HTTPS Everywhere no pueden proporcionar una protección adicional para su uso de ese sitio «.

Actualiza Tus Aplicaciones

Mantén tu navegador y dispositivos actualizado con las ultimas versiones, pero asegúrese de hacerlo en una red de confianza, como la de tu casa o la del trabajo, no en una red publica. Existe el caso de que los viajeros actualizan sus aplicaciones en una red publica, dando el momento perfecto para que un atacante pueda **inyectar malware** en su dispositivo.

Habilite La Autenticación

De Dos Factores

Sin duda, es una buena práctica **habilitar la autenticación de dos pasos** en los servicios, como Gmail, Twitter y Facebook. De esta manera, incluso si alguien se las arregla para obtener tu contraseña cuando estar una una red Wi-Fi pública, tendrás esa capa de protección adicional.

Olvide La Red Wi-Fi Pública

Una vez que hayas usado la red abierta sin problemas, asegúrarte de cerrar la sesión en cualquier servicio web que has usado. Luego podrás borrar la conexión establecida con aquella red. Esto significa que el teléfono o el PC no se conecta de nuevo automáticamente a la red, si estás en su rango.

En Windows, puede desmarcar la opción «**Conectar automáticamente**» al lado del nombre de la red antes de conectar, o dirigirse al Panel de control> Conexiones de red y recursos compartidos y haga clic en el nombre de la red. Haga clic en «Propiedades inalámbricas» y luego desmarque «Conectar automáticamente si esta red está en rango».

En Mac, ve a Preferencias del sistema, red y, en la sección

Wi-Fi, haga clic en Opciones avanzadas. Luego desmarque «Recuerde redes este equipo». También puedes eliminar de forma individual redes seleccionando el nombre y pulsando el botón menos de abajo.

En **Android**, puedes hacerlo entrando en la lista de redes Wi-Fi, mantenga pulsado el nombre de red y seleccione «Olvidar red». En **iOS**, dirígete a Configuración, seleccione las redes Wi-Fi a continuación, seleccione el nombre de red y seleccione «Omitir esta red». Como precaución adicional, también debe activar el «Preguntar al conectar», que también se encuentra en el menú de redes Wi-Fi.