



Cómo proteger tus datos durante los viajes

Cinco consejos para asegurar tus datos durante viajes de negocios o placer

Todo el tiempo, innumerables individuos viajan por trabajo o por ocio. Si bien sus espíritus pueden ser elevados, el estado de ánimo es aún más brillante para los piratas informáticos malintencionados que están a punto de ganar en grande. El acceso a Wi-Fi en los aviones, en las habitaciones de los hoteles y en las redes públicas hace que los usuarios sean vulnerables a los malos actores que buscan información confidencial.

Cuando viaje, es fácil aprovechar el acceso público a Wi-Fi para acceder a su cuenta bancaria, utilizar un servicio de transporte o iniciar sesión en cuentas de correo electrónico o redes sociales. Sin embargo, es posible que muchas personas no se den cuenta de que las redes Wi-Fi públicas no requieren ninguna autenticación antes de que los usuarios puedan conectarse a ellas, lo que brinda a los piratas informáticos un acceso fácil a los dispositivos no seguros en estas redes.

¿Por qué el wifi público es la mina de oro de un cibercriminal?

Según un análisis realizado por Kaspersky Labs, el 24,7% de los puntos de acceso Wi-Fi no utilizan el cifrado, lo que deja a los usuarios vulnerables a los piratas informáticos. Hay muchas maneras en que los piratas informáticos atacan a los usuarios en Wi-Fi público, como:

Configuración de puntos de acceso Wi-Fi no autorizados

Los ciberdelincuentes con frecuencia establecen puntos de acceso falsos y les dan nombres que se parecen a puntos de acceso abiertos legítimos. Cuando las personas se conectan a un punto de acceso no autorizado, los ciberdelincuentes pueden inyectar malware en sus dispositivos o interceptar sus datos.

Lanzar ataques de hombre en el medio (MITM – Man In The Middle)

En un ataque MITM, los hackers se insertan entre el usuario y el punto de conexión. Esto significa que los piratas informáticos pueden interceptar cualquier información personal que envíe a través de Internet, incluidos sus correos electrónicos, información de tarjetas de crédito y credenciales de inicio de sesión. También pueden ver sus actividades de navegación, la información de su cuenta y cualquier compra que realice en línea.

Distribuir malware

Incluso si utiliza una VPN, los ciberdelincuentes también pueden distribuir malware a través de redes Wi-Fi no seguras. Esto es especialmente cierto si permite compartir archivos a través de la red, lo que brinda a los piratas informáticos un medio para plantar fácilmente malware en su dispositivo. En algunos casos, los ciberdelincuentes piratean el punto de conexión para que cuando los usuarios se conecten, aparezca una ventana emergente que ofrece una actualización de software. Cuando el usuario hace clic en la ventana, el malware se instala en su dispositivo. Solo debes conectarte a redes en las que confíes.

Para evitar la interceptación de datos y aumentar la privacidad, use siempre una red privada virtual (VPN) cuando se conecte a redes públicas de Wi-Fi para cifrar el tráfico de Internet.

¿Qué es una VPN y cómo te protege?

Una VPN es un método de conexión que proporciona a los usuarios capas adicionales de seguridad cuando se conectan a una red. Encripta los datos de los usuarios y transmite su tráfico de Internet a través de una conexión segura. Esto permite a los usuarios iniciar sesiones de navegación anónimas en cualquier red, lo que dificulta mucho más que los piratas informáticos puedan interceptar sus datos.

Además, la conexión a una VPN oculta las verdaderas direcciones IP de los usuarios para que no se pueda rastrear su ubicación exacta. Por ejemplo, puede vivir en California, pero cuando se conecta a su VPN, su ubicación puede cambiar dependiendo de la ubicación de su servidor VPN. Esto protege su privacidad y dificulta el seguimiento de terceros.

Dados los riesgos de la conexión Wi-Fi pública gratuita, es esencial utilizar las prácticas de seguridad necesarias antes de viajar. Estas son algunas de las mejores maneras de mantenerse a salvo al usar Wi-Fi público:

1. Use una VPN para asegurar su conexión

El uso de una VPN es la forma más efectiva de protegerse en Wi-Fi público. Instalar la VPN y activarla antes de conectarse a un punto de acceso Wi-Fi público le permite a su dispositivo la capacidad de mantener sus datos a salvo de los piratas informáticos.

2. Evite iniciar sesión en sitios web protegidos por contraseña sin una VPN

Si necesita acceder a sus cuentas de correo electrónico, bancarias o sociales a través de Wi-Fi público, asegúrese de activar su VPN antes de hacerlo, especialmente para los sitios web que no utilizan su propio cifrado (consulte la viñeta de HTTPS a continuación).

3. Evite conectarse automáticamente a puntos de acceso Wi-Fi

Muchos dispositivos se conectarán automáticamente a las redes Wi-Fi utilizadas en el pasado. Por motivos de seguridad, es recomendable eliminar estas redes mediante la opción "Olvidar esta red" en su dispositivo después de usarlas.

4. Solo visite sitios web con HTTPS en la URL

Los sitios web que utilizan el protocolo HTTPS encriptan la comunicación entre el servidor web y su navegador, lo que resulta en un nivel de seguridad mucho más alto.

5. Habilite la autenticación de dos factores en sus cuentas

La autenticación de dos factores (2FA) requiere que los usuarios proporcionen un código único bajo demanda al iniciar sesión en sus cuentas, además de su nombre de usuario y contraseña. El código en sí se entrega generalmente por mensaje de texto o correo electrónico, lo que hace que sea mucho más difícil para un pirata informático hacerse pasar por usted y acceder a su cuenta.

Al implementar estas prácticas de seguridad puede reducir en gran medida su riesgo de compromiso al usar Wi-Fi público en su próximo viaje.