Alerta aeropuertos: el WiFi gratuito puede jugar malas pasadas

?El nivel de peligro frente a los ciberataques es, al menos, cuatro veces mayor ahora que hace dos o tres años?, cuenta Brian Schippers, Sales Engineer de Sophos

La forma de viajar ha cambiado por completo. El mundo parece más pequeño conforme las fórmulas de transporte son más rápidas y accesibles. **Tierra, mar y aire.** Y de esto último se desprenden los mayores cambios.

Lejos quedan aquellos tiempos en los que adquirir un billete de avión era solo para privilegiados. Pero ojo, los viajeros se enfrentan a una nueva amenaza: **los ciberdelincuentes.**

La inmensa mayoría de personas que se encuentran en un aeropuerto cuentan con un dispositivo inteligente, y aquí es donde llega el peligro: los riesgos en estos espacios aumentan mediante “el aumento de dispositivos IoT, como **el uso de dispositivos tecnológicos para acreditaciones y geolocalización personalizada para los pasajeros**, los sistemas de información conectados del propio aeropuerto, así como la digitalización de los servicios ofrecidos por las aerolíneas”, tal y como cuentan desde la compañía de software y hardware de seguridad Sophos.

Un claro ejemplo de ello es el wifi spoofing. Al estar tantas horas en un lugar cerrado, muchos de los cargos importantes de empresas recurren a los puntos de conexión de wifi abiertos para hacer sus gestiones. El término spoofing se refiere generalmente al uso de técnicas de suplantación de identidad. En relación al wifi, las herramientas de spoofing están fácilmente disponibles, lo que permite a los cibercriminales hacer que sus portátiles imiten un punto de acceso wifi para que los usuarios se conecten y expongan sus datos.

“El nivel de peligro frente a los ciberataques es, al menos, cuatro veces mayor ahora que hace dos o tres años”,cuenta Brian Schippers, Sales Engineer de Sophos. Y esto no solo se refiere a esta práctica.

Simplemente los puntos de conexión públicos pueden recabar toda nuestra información, como puede ser la del aeropuerto o la de alguno de los restaurantes que se encuentran en ellos. Aun así, **en el caso de que ya estemos dentro, todavía hay esperanzas para paliar lo máximo posible un desenlace perjudicial.** La Oficina de Seguridad del Intertrnauta (OSI) da las siguientes claves:

- Deshabilitar cualquier proceso de sincronización de nuestro equipo
- Mantener siempre el equipo actualizado, con el antivirus instalado correctamente y, si es posible, hacer uso de un cortafuegos
- Tener preocupación a la hora de navegar por páginas cuyos datos no viajan cifrados (la URL no empieza por HTTPS)
- No iniciar sesión en ningún servicio
- Tras la conexión, eliminar los datos de la red memorizados por el equipo en cuestión

La palabra gratuito, por muy atractiva que nos parezca, puede esconder peligros no esperados. Cuando un usuario se conecta a este tipo de redes wifi pierde el control de todo lo que hay en nuestro dispositivos. **Y los ciberdelincuentes son conscientes de ello.**

Fuente: Dirigentes Digital