¿Por qué deberíamos dejar de ‘temerle’ al Wi-Fi?

Por Chester Wisniewski, jefe de Investigación Científica de Sophos

¿Alguna vez has estado con alguien que se conecta, sin miedo, a las redes públicas de centros comerciales, cafeterías, hoteles y aeropuertos? Si has sentido celos de la capacidad que tienen de no preocuparse y temer a los riesgos de hacerlo, debes seguir leyendo esto.

Luego de casi dos años de pandemia, parece que las personas están saliendo de sus hogares de forma gradual. Esto inevitablemente conduce a la necesidad de acceso a Internet mientras viajamos, compramos y socializamos nuevamente.

Casi 10 años después de que Edward Snowden nos dijera que nos estaban espiando en línea, ¿podemos pensar que es seguro simplemente "conectarnos"?

Sin duda hemos logrado un gran progreso en la mejora de la línea de base de seguridad al realizar cambios en la forma en que se implementa el cifrado para garantizar que nuestras comunicaciones sigan siendo privadas.

Pero primero, evaluemos los riesgos que aún existen en el uso de Wi-Fi público considerando las mejoras en los protocolos de seguridad fundamentales que se utilizan para los sitios web y las aplicaciones telefónicas modernas:

- **La lista de ataques vía Wi-Fi**

La mayoría de las redes Wi-Fi públicas no están encriptadas, es decir, cualquier persona que se encuentre dentro del alcance determinado puede ver la información que se envía a través de la conexión. Esto era problemático en el pasado, ya que ofrecía muchas oportunidades para espiar o secuestrar sus comunicaciones.

El primer requisito para un atacante es estar dentro del alcance de la red y realizar una de las siguientes acciones:

- Operar un punto Wi-Fi "gemelo malicioso” con el mismo nombre que tenga una señal más fuerte al que se conecte en lugar de la real
- Engañar mediante búsquedas para que los usuarios comiencen a redirigir sus solicitudes a páginas falsas o mediante proxies.
- Observar las comunicaciones para interceptar cualquier dato no protegido

Esto no es demasiado difícil, pero el aspecto físico de esto lo hace poco práctico. Los atacantes deben acercarse físicamente a sus víctimas, limitando a las víctimas potenciales a las personas en su área inmediata.

A continuación, los atacantes deben predecir qué sitios podrían querer visitar sus víctimas y si estos sitios están protegidos por protocolos HSTS. Además, no podrán interceptar el tráfico sin convencer a una autoridad de certificación de que les emita uno válido para el dominio protegido.

Por supuesto, los atacantes podrían simplemente espiar el tráfico no cifrado y esperar lo mejor. Pero menos de aproximadamente el 5% de las conexiones no están encriptadas y la gran mayoría de ellas son rastreadores de publicidad y marketing, según datos de Sophos. Ninguno de los destinos más populares que carecían de cifrado aceptaba nombres de usuario y contraseñas, por lo que esta posibilidad es de uso limitado para los delincuentes.

- **Desafíos de los atacantes**

Los ataques basados en Wi-Fi son un delito de muy bajo rendimiento con una probabilidad muy alta de arresto. Si algo hemos aprendido a lo largo de los años es que los delincuentes suelen ser vagos y buscan la fruta más fácil de conseguir. Sin embargo, el riesgo de ataques como este variará según su perfil de riesgo.

Sin embargo, los sitios web encriptados no son inmunes al secuestro. Un sitio web que no utiliza HSTS puede ser "degradado" por un adversario para utilizar una conexión no cifrada que les permita manipular o interceptar su información.

Datos de Sophos indican que esto sucede con la mayoría de los sitios vulnerados vía WiFi (61.03%). Eso suena aterrador, pero recuerda que deben estar cerca y apuntar a destinos específicos con anticipación o degradar los sitios sin HSTS al protocolo HTTP, una hazaña difícil, si no imposible. Ninguno de los sitios sin protección HSTS estaba en categorías donde se transmite el tipo de información que los delincuentes a menudo valoran. Esto incluye redes sociales, proveedores de correo electrónico basados en la web, aplicaciones de oficina, instituciones financieras o sitios de citas.

Si bien algunos de estos sitios eran de alto perfil, por lo general no ofrecen páginas de inicio de sesión y no es fácil para un delincuente monetizar los datos robados.

- **Nivel de riesgo para la mayoría de las personas**

Entonces, ¿dónde nos deja eso? Todo lo que la mayoría de nosotros usamos desde nuestros teléfonos móviles y computadoras portátiles en lugares públicos está protegido a un nivel increíblemente difícil de comprometer.

¿Significa eso que es imposible? Claramente no. Siempre existen riesgos e inquietudes, así que investiguemos las razones para no confiar en las redes Wi-Fi públicas y qué alternativas podría utilizar para reducir los riesgos.

- **Nivel de riesgo para objetivos sensibles**

¿Eres un objetivo de alto perfil? ¿Eres periodista, político, famoso o incluso espía? En ese caso e Wi-Fi público podría ser una táctica demasiado arriesgada para ti. Y para ello, es importante

decir que en muchos países los planes de datos de los teléfonos móviles son lo suficientemente asequibles como para funcionar sin molestarse en conectarse a Wi-Fi.

Es por eso que en Sophos recomendamos, para aquellos que necesitan más seguridad para sus comunicaciones, ya sea usando Wi-Fi o teléfonos móviles les recomiendo el uso de Tor. Se trata de un navegador de privacidad y seguridad mejorada para bloquear a cualquiera que pueda estar fisgoneando en la red. Puede ser un poco lento de vez en cuando, pero si tienes motivos para creer que puedes tener adversarios avanzados jugando contigo, Tor es lo mejor que existe para defenderte de ellos.

- **Seguridad adicional**

Sin embargo, hay algunas cosas que las personas conscientes de la privacidad pueden hacer para que sea un poco más seguro, y esto se aplica a cualquier red que pueda usar:

Un ejemplo es utilizar un administrador de contraseñas. Las contraseñas largas, seguras y únicas son esenciales, además de quea protegen contra ataques de interceptación de phishing y *machine-in-the-middle* (MiTM) Es importante destacar la utilización de sistemas de nombres de dominio (DNS) sobre HTTPS del siguiente modo:

- En Firefox: Vaya a Configuración -> Configuración de red -> Configuración -> Habilitar DNS sobre HTTPS
- En Chrome: vaya a Configuración -> Privacidad y seguridad -> Seguridad -> Usar DNS seguro ->
- En Edge: vaya a Configuración -> Privacidad, búsqueda y servicios -> Configuración -> Usar DNS seguro -> Elija un proveedor
- Los usuarios de MacOS e iOS pueden utilizar la aplicación DNSecure

Y finalmente para la utilización de la banca móvil, lo más recomendable es utilizar su plan de datos de teléfono móvil.

En conclusión, para la mayoría de las personas la mayor parte del tiempo la conexión Wi-Fi funciona perfectamente. Los delincuentes oportunistas tienen formas mucho mejores de comprometer a las víctimas sin los riesgos físicos de tener que estar a poca distancia de sus crímenes.

Con calma, puedes navega por Facebook, Twitter y revisa tu Gmail, así como aprovechar todas esas ofertas online Black Friday y Cyber Monday mientras viajas. ¿Y si eres un poco más paranoico? Siga los consejos anteriores para ir un paso por delante.

###

de la actualidad. Con tecnología de inteligencia de amenazas, inteligencia artificial y aprendizaje automático de SophosLabs y SophosAI, Sophos ofrece una amplia cartera de productos y servicios avanzados para proteger a los usuarios, las redes y los puntos finales contra ransomware, malware, exploits, phishing y una amplia gama de otros ciberataques. Sophos proporciona una única consola de gestión integrada basada en la nube, Sophos Central, la pieza central de un ecosistema de ciberseguridad adaptable que cuenta con un lago de datos centralizado que aprovecha un amplio conjunto de API abiertas disponibles para clientes, socios, desarrolladores y otros proveedores de ciberseguridad. Sophos vende sus productos y servicios a través de socios revendedores y proveedores de servicios administrados (MSP) en todo el mundo. Sophos tiene su sede en Oxford, Reino Unido. Hay más información disponible en www.sophos.com

Síguenos en:
Facebook: https://www.facebook.com/SophosLatam/
Twitter: https://twitter.com/SophosLatAm
LinkedIn: https://www.linkedin.com/company/sophos/