Consejos para usar el wifi público de forma segura

Los actores maliciosos pueden aprovecharse de usted en línea. Lea a continuación algunos consejos que debe tener en cuenta si necesita usar wifi público.

En respuesta al brote de coronavirus y al cierre de negocios y bibliotecas, muchos de nosotros estamos pasando más tiempo en línea. Como resultado, es posible que necesitemos usar wifi público para conectarnos a internet. Si necesita usar wifi público, tenga en cuenta las siguientes recomendaciones del director de privacidad del estado para contribuir a la protección de sus datos:

1. Confirme que tiene la red correcta.

Asegúrese de que se está conectando a la red correcta. Los actores maliciosos pueden crear redes que, por su nombre, parecen inofensivas, pero que en realidad lo llevan a conectarse a una red para ver su navegación en internet. Esto significa que, si introduce credenciales de acceso o contraseñas en los sitios web, el hacker podrá robar su información. Para protegerse contra esto, lea el nombre de la red con mucho cuidado y, si es posible, pregunte a un empleado o verifique la señalización del negocio para asegurarse de que la red es legítima.

Las redes conocidas, como las de las cadenas de cafeterías famosas, suelen ser menos sospechosas porque la empresa está operando la red como servicio con su negocio. Por lo general, las redes conocidas son más seguras que cualquier red wifi gratuita que pueda aparecer en su teléfono en un lugar público.

2. Apague la conexión automática.

Muchos dispositivos (teléfonos inteligentes, computadoras portátiles y tabletas) tienen configuraciones de conexión automática. Esta configuración permite que sus dispositivos se conecten convenientemente a redes cercanas. Esto sirve para las redes confiables, pero también puede conectar sus dispositivos a redes que podrían ser inseguras. Puede desactivar esta función a través de la función de configuración de su dispositivo. Mantenga esta

configuración desactivada, en especial cuando viaje a lugares desconocidos. Como precaución adicional, puede seleccionar “Olvidar la red” después de usar un wifi público.

También debe controlar el Bluetooth cuando esté en lugares públicos. La conexión Bluetooth permite que varios dispositivos se comuniquen entre sí, y un hacker puede buscar señales abiertas de Bluetooth para acceder a sus dispositivos. Mantenga desactivada esta función en su teléfono y otros dispositivos cuando se encuentre en un área desconocida.

3. Desactive el uso compartido de archivos.

Asegúrese de desactivar la opción de uso compartido de archivos cuando use un wifi público. Puede desactivar el uso compartido de archivos desde las preferencias del sistema o el panel de control, según su sistema operativo. AirDrop es un ejemplo de una función de uso compartido de archivos que debería desactivar. Algunos sistemas operativos, como Windows/PC, desactivarán el uso compartido de archivos para usted seleccionando la opción “público” cuando se conecte a una nueva red pública por primera vez.

Pasos para desactivar el uso compartido de archivos

En Windows PC:

1. Vaya a “Centro de redes y recursos compartidos”.
2. Luego, seleccione “Cambiar la configuración avanzada de uso compartido”.
3. Desactive el uso compartido de archivos e impresoras.

Para las Mac:

1. Vaya a “Preferencias del sistema”.
2. Seleccione “Compartir”.
3. Deseleccione todo.
4. A continuación, en el Finder, haga clic en “AirDrop” y, en “Permitir que me puedan encontrar”, seleccione “Nadie”.

En el caso de iOS, solo busque AirDrop en el Centro de control y desactívelo.

4. Use una VPN.

Considere la posibilidad de instalar una VPN (red privada virtual) en su dispositivo. Una VPN es la opción más segura para garantizar la privacidad digital con un wifi público. Encripta sus datos cuando se transfieren hacia y desde su dispositivo y actúa como un “túnel” protector para que sus datos no sean visibles cuando se transfieren a través de una red.

5. Advertencia del FBI sobre sitios web cifrados: HTTPS.

El FBI ha advertido sobre los sitios web con direcciones que empiezan con “https”. En teoría, la presencia de “https” y el ícono del candado indican que el tráfico de la web está cifrado y que los visitantes pueden compartir datos de forma segura. Sin embargo, los ciberdelincuentes ahora cuentan con la confianza del público al atraer a la gente a sitios web maliciosos que usan https y parecen seguros cuando no lo son.

Recomendaciones del FBI:

- No confíe simplemente en el nombre que aparece en un correo electrónico: ponga en duda la intención del contenido del correo electrónico.
- Si recibe un correo electrónico sospechoso con un enlace de parte de un contacto conocido, confirme que el mensaje sea legítimo llamando o enviando un correo electrónico al contacto. No responda directamente a un correo electrónico sospechoso.
- Compruebe si hay errores ortográficos o dominios incorrectos dentro de un enlace (p. ej., si una dirección termina en “.com”, en vez de terminar en “.gov”, como debería).
- No confíe en un sitio web solo porque tenga un ícono de candado o “https” en la barra de direcciones del navegador.

6. No se recomienda el acceso a información sensible.

Aunque tenga una VPN, no es recomendable acceder a cuentas bancarias personales o a datos personales sensibles similares, como los números de seguridad social, en redes públicas no seguras. Hasta las redes públicas seguras pueden ser peligrosas. Utilice su mejor juicio si debe acceder a estas cuentas con un wifi público. Para las transacciones financieras, en cambio, puede ser mejor utilizar la función de hotspot de su teléfono inteligente.

7. Seguro vs. no seguro.

Básicamente existen dos tipos de redes públicas de wifi: seguras y no seguras.

Siempre que sea posible, conéctese a redes públicas seguras. Se puede conectar a una red no segura sin ningún tipo de función de seguridad como contraseñas o nombres de usuario. Una red segura suele requerir que el usuario acepte los términos y condiciones, registre una cuenta o escriba una contraseña antes de conectarse a la red.

8. Mantenga activado el firewall.

Si utiliza una computadora portátil, mantenga activado el firewall cuando use un wifi público. Un firewall actúa como una barrera que protege su dispositivo contra las amenazas de

malware. Es posible que los usuarios desactiven el firewall de Windows debido a las ventanas emergentes y las notificaciones y luego se olviden. Si desea reiniciarlo en Windows PC, vaya a “Sistema y seguridad” en el Panel de control y seleccione “Firewall de Windows”. Si es usuario de Mac, vaya a “Preferencias del sistema”, luego a “Seguridad y privacidad” y finalmente a la pestaña “Firewall” para activar la función.

9. Use un software antivirus.

También asegúrese de instalar la última versión de un programa antivirus en su computadora portátil. Los programas antivirus pueden ayudar a protegerlo cuando usa un wifi público al detectar el malware que podría entrar en su sistema mientras utiliza la red compartida. Una alerta le avisará si ingresan virus conocidos en su dispositivo o si hay alguna actividad sospechosa o un ataque o si se introduce malware en su sistema.

10. Utilice la autenticación de dos factores o multifactor.

Utilice la autenticación multifactor (MFA) cuando acceda a sitios web con su información personal. Esto significa que cuenta con un segundo código de verificación (enviado por mensaje de texto a su teléfono o mediante una aplicación o una clave física) que lo protege aún más. Así que, incluso si un hacker obtiene su nombre de usuario y su contraseña, no puede acceder a sus cuentas sin un código de autenticación.

11. Controle sus dispositivos personales.

No descuide su computadora portátil, tableta o teléfono inteligente en un lugar o transporte público. Aunque esté tomando precauciones con una red wifi, eso no impedirá que alguien se lleve sus pertenencias o eche un vistazo a su información. Sea consciente de su entorno y esté atento a las personas que lo rodean.

12. Otros consejos de seguridad en línea.

Estos son algunos consejos para mantenerse seguro en línea, en especial si usa una conexión wifi pública.

- Use contraseñas seguras.
- Cifre sus dispositivos.
- Cuídese de los correos electrónicos de phishing.
- Tenga cuidado con lo que publica en las redes sociales. Dar demasiados datos personales puede ayudar a los hackers a adivinar las contraseñas.

- Borre la información antigua que ya no necesita.
- Si una red le pide que instale algún software o alguna extensión de navegador adicionales, no se conecte.
- Asegúrese de que los últimos parches y actualizaciones de software estén instalados en sus dispositivos para protegerse de los problemas conocidos.