Wifi público: navega con seguridad

Viajar no debe comprometer la privacidad de tus datos.

Cuando sales de viaje, la conexión a internet se vuelve una herramienta clave: te permite buscar direcciones, solicitar transporte, confirmar reservaciones, compartir fotos o avisar que llegaste bien. En este contexto, el wifi de aeropuertos, hoteles, plazas o establecimientos comerciales puede ser un gran aliado, siempre que se utilice con precaución.

¿Qué es el wifi público?

El término "público" indica que el servicio está disponible para múltiples usuarios; sin embargo, al conectarte, es importante identificar si la red está protegida o abierta, ya que no todas ofrecen el mismo nivel de seguridad.

Las redes protegidas con contraseña suelen incorporar mecanismos de cifrado que añaden una capa de protección a tu información. En cambio, las redes abiertas requieren mayor precaución, debido a que tu información puede ser interceptada o tu navegación podría ser redirigida a sitios fraudulentos.

A pesar de que no siempre es posible saber con certeza qué tan segura es una red pública, existen señales que pueden ayudarte a tomar decisiones más informadas, como identificar quién ofrece el servicio, si cuenta con contraseña o si su uso implica compartir información sensible.

Por ello, antes de conectarte, te invitamos a revisar el semáforo de conexión:

Puedes conectarte con confianza básica si:
- La red la ofrece algún establecimiento o institución identificable (un hotel, café, aeropuerto o gobierno).
- El acceso requiere una contraseña.
- No te pide datos innecesarios (direcciones de correo, teléfono, información bancaria, datos de acceso a aplicaciones, como contraseñas o códigos PIN).

Úsala para ver mapas, mensajería instantánea o hacer búsquedas.

Conéctate con precaución si:
- La red está abierta (sin contraseña).
- El nombre de la red es genérico o ambiguo, por ejemplo, "wifi gratis 123".
- No sabes quién la administra.

Úsala para consultas rápidas en la web; evita introducir datos sensibles, contraseñas o información financiera.

Evita la conexión o busca otra red si:
- Hay redes duplicadas o sospechosas, por ejemplo: "Café_Oficial" y "Café_Free".
- Te pide información inusual (correo, contraseñas, etc.).
- La navegación te redirige constantemente a otros sitios web.

El wifi como parte del viaje

Un factor importante es que la seguridad no depende exclusivamente de la red. Una vez que te conectas, la seguridad digital también se basa en cómo usas internet, por ejemplo, las páginas que visitas y, sobre todo, las aplicaciones que descargas o utilizas durante el viaje.

Al viajar, las aplicaciones de transporte, mapas o reservas son esenciales; sin embargo, es importante asegurarse de que no se trate de plataformas falsas, ya que podrían intentar obtener datos personales o financieros.

Ten cuidado con aplicaciones que:

- Muestran nombres similares a los originales, pero con ligeras variaciones o faltas de ortografía.
- Tienen un volumen bajo de descargas y reseñas inconsistentes.
- Solicitan permisos que no justifican su función, como acceso a contactos, cámara o micrófono.
- Se descargan fuera de tiendas oficiales.

Si necesitas acceder a un sitio web, revisa en la barra del navegador que la dirección comience con "https://" y muestre el ícono de un candado cerrado, lo que indica que la conexión está protegida. Asegúrate también de que estás en la página correcta.

Si el sitio presenta una interfaz diferente a la habitual, se comporta de forma extraña o te redirecciona o muestra ventanas emergentes, es mejor abandonar el sitio. Por último, más allá de la conexión, la clave está en decidir con cuidado qué tipo de información se comparte en cada momento.

El wifi público es un gran aliado para moverse por el mundo. Aprender a decidir cuándo, dónde y para qué conectarte te permitirá aprovechar la red con mayor tranquilidad. Conectarte es tu derecho, pero hacerlo con seguridad es tu responsabilidad.

Recomendaciones

- Verifica cuál es la red wifi oficial.
- Evita iniciar sesión o ingresar contraseñas en cuentas importantes.
- No guardes contraseñas en el navegador.
- Siempre cierra la sesión de tus cuentas.
- No realices compras ni compartas datos personales.
- Desactiva la conexión automática a redes wifi.
- Si descargas aplicaciones, hazlo desde las tiendas oficiales.

Artículo escrito por la Subprocuraduría de Telecomunicaciones de la Procuraduría Federal del Consumidor.