WiFi pública: lo que pasa realmente cuando te conectas en un café

Man-in-the-middle sin jerga: riesgos reales, mitos habituales y cuándo una VPN marca la diferencia (y cuándo no)

Hay una escena que se repite cada día millones de veces: llegas a un café, pides el café, preguntas la contraseña del WiFi y te conectas. Sin pensar. Sin preguntar. Sin saber, realmente, a qué red te acabas de conectar ni quién más está en ella.

No es alarmismo decir que esa red puede ser peligrosa. Tampoco es exacto decir que siempre lo es. La realidad, como casi todo en ciberseguridad, vive en un terreno medio que la mayoría de los artículos ignoran: el espacio entre el miedo exagerado y la confianza ciega.

Este artículo existe para darte ese mapa intermedio. Para que la próxima vez que te sientes en una terraza con el portátil sepas exactamente qué puede pasar, qué probabilidad real tiene de ocurrir y qué puedes hacer al respecto sin convertirte en experto en tecnología.

El escenario que nadie visualiza: ¿quién más está en esa red?

Cuando te conectas a una WiFi pública, no estás entrando a un canal privado entre tú y el router. Estás uniéndote a una red compartida donde puede haber decenas de dispositivos desconocidos. El del estudiante que lleva tres horas con el portátil. El del señor que acaba de llegar. El del repartidor que esperaba un pedido. Y, en ocasiones, alguien que no ha venido a tomar café.

La naturaleza técnica de estas redes permite que, bajo ciertas condiciones, un dispositivo en la misma red pueda posicionarse entre tú y el router. Capturar el tráfico. Leerlo.

Modificarlo. Eso es, en esencia, lo que se llama un ataque man-in-the-middle: literalmente, alguien en el medio de tu conversación digital.

No hace falta que sea un hacker de película con capucha negra. Las herramientas para hacerlo son públicas, gratuitas y accesibles. El nivel técnico requerido ha bajado enormemente en los últimos años. No lo menciono para asustar, sino porque cambia el perfil de quién puede llevarlo a cabo: ya no es solo una amenaza teórica de película, es algo al alcance de cualquier persona con motivación y una búsqueda en Internet.

Qué puede ver alguien que intercepta tu tráfico WiFi

Aquí es donde muchos artículos mezclan lo que *podría* pasar con lo que *pasa habitualmente*, y esa diferencia importa.

La buena noticia estructural de 2026 es que la gran mayoría del tráfico web ya viaja cifrado. Cuando ves ese candado en la barra del navegador y la dirección empieza por `https://`, los datos que envías y recibes están codificados de forma que, aunque alguien los intercepte, solo verá ruido ininteligible. Esta tecnología, llamada TLS, ha cambiado el panorama radicalmente respecto a hace una década.

Lo que sí puede ver un atacante en la misma red WiFi, incluso con ese cifrado activo, es bastante revelador: qué dominios visitas, con qué frecuencia, a qué horas y desde qué tipo de dispositivo. No puede leer el contenido de tu correo de Gmail, pero puede saber que lo estás usando. No puede ver qué buscas en Google, pero puede saber que tienes una sesión abierta. Eso se llama metadatos, y los metadatos cuentan una historia.

Donde el riesgo aumenta de forma significativa es en cuatro situaciones concretas:

Aplicaciones sin cifrado actualizado. No todo el software que usas aplica TLS correctamente. Algunas apps antiguas, aplicaciones de empresa mal configuradas o servicios menores todavía transmiten datos en claro o con cifrado deficiente. Si usas una de estas en una red pública, tu información viaja como si fuera en un sobre abierto.

Redes WiFi falsas que imitan las reales. Esta es la variante más peligrosa y la más subestimada. Un atacante puede crear una red llamada "Café_Centro_WiFi" que imita a la red legítima del local. Tu dispositivo, especialmente si tiene el WiFi en modo automático, puede conectarse sin que te des cuenta. Una vez dentro de esa red falsa, el atacante sí controla todo el tráfico, incluyendo la posibilidad de servir páginas web falsas que imitan a

las reales. Esto tiene nombre técnico —evil twin attack— y es más común de lo que parece en aeropuertos, estaciones de tren y grandes centros comerciales.

Ataques de degradación de protocolo. En algunos escenarios, un atacante con los conocimientos adecuados puede intentar forzar a tu dispositivo a usar versiones más antiguas y vulnerables de los protocolos de cifrado. Es una técnica avanzada, pero existe.

Sesiones abiertas en servicios sin reautenticación frecuente. Si tienes sesiones activas en plataformas que no verifican regularmente tu identidad, y alguien logra capturar tu cookie de sesión en un momento de vulnerabilidad, puede acceder a esas plataformas haciéndose pasar por ti sin necesitar tu contraseña.

El ataque que sí deberías tomar en serio: la red falsa

De todos los vectores descritos, el que merece atención especial no es el hacker que intercepta tu tráfico HTTPS —técnicamente difícil y con resultados limitados en 2026—, sino el que crea una red paralela diseñada para que te conectes a ella sin saberlo.

Piénsalo desde la perspectiva del atacante: es infinitamente más sencillo crear una red WiFi con el nombre de la cafetería, esperar a que los dispositivos se conecten automáticamente y servir páginas de inicio de sesión falsas que capturar y descifrar tráfico HTTPS en tiempo real. El primero no requiere conocimientos técnicos profundos. El segundo sí.

La señal de alerta más importante es esta: si te conectas a una red WiFi y el sistema te pide hacer login en una página web antes de darte acceso a internet —lo que se llama un portal cautivo—, observa esa página con atención. ¿La URL tiene candado? ¿El nombre de dominio tiene sentido? ¿Te pide datos que no deberían ser necesarios para conectarte a un WiFi público, como tu correo o tu número de teléfono? Si algo no encaja, desconéctate.

La VPN: cuándo es útil de verdad y cuándo es marketing

Pocas herramientas de seguridad están tan rodeadas de mitos como la VPN. Hay quien la presenta como la solución definitiva a todos los problemas de las redes públicas. Hay quien dice que es completamente inútil. La realidad, como siempre, es más matizada.

Una VPN —Red Privada Virtual— establece un túnel cifrado entre tu dispositivo y un servidor remoto. Todo tu tráfico pasa por ese túnel antes de salir a internet. Lo que consigue en una red WiFi pública es concreto: oculta tu tráfico al operador de esa red. Si alguien en el café intenta ver qué páginas visitas, solo verá que te has conectado al servidor VPN. Punto.

Cuándo una VPN sí marca la diferencia en WiFi pública:

Cuando usas aplicaciones o servicios que no implementan HTTPS de forma consistente. Cuando quieres asegurarte de que ni el propio operador del café —ni nadie que haya comprometido el router— puede ver tus metadatos de navegación. Cuando trabajas con información sensible de empresa y tienes la VPN corporativa configurada. Cuando te conectas a una red que no reconoces del todo y quieres una capa adicional de protección.

Cuándo una VPN no te protege o te da una falsa sensación de seguridad:

Si te has conectado ya a una red falsa tipo evil twin antes de activar la VPN, el atacante puede haber capturado información antes de que el túnel se estableciera. Si usas una VPN gratuita de origen desconocido, estás desplazando la confianza del operador del café al operador de la VPN —que puede ser igual o más problemático—. Si navegas en sitios HTTPS con certificado válido, la VPN añade una capa de protección marginal en la mayoría de los casos. Y en ningún caso una VPN te protege de que hayas metido tu contraseña en una página falsa.

La conclusión práctica es esta: una VPN de confianza, activada antes de conectarte a la red, en una red pública que no controlas, es una herramienta razonable especialmente para usuarios que manejan información profesional sensible. No es obligatoria en todas las situaciones, pero tampoco es exagerado usarla por defecto cuando te conectas fuera de casa.

Lo que cambia el riesgo real: el contexto importa más que la herramienta

El error más común al pensar en seguridad en WiFi pública es tratar todas las situaciones como equivalentes. No lo son. El nivel de riesgo real depende de varios factores que vale la pena considerar:

Qué haces mientras estás conectado. Leer las noticias en una web de un periódico importante tiene un perfil de riesgo radicalmente distinto a acceder al panel de administración de tu empresa, revisar contratos en PDF enviados por correo o hacer una transferencia bancaria. La intensidad de las precauciones debería ser proporcional a la sensibilidad de lo que manejas.

Dónde estás conectado. Una red pública en un pequeño café de tu barrio de confianza no tiene el mismo perfil que la WiFi gratuita de un aeropuerto internacional donde hay miles de viajeros, competidores de negocio, y —en aeropuertos de ciertas regiones— actores con recursos e interés en el espionaje corporativo. El contexto geográfico y social del lugar importa.

Si el establecimiento gestiona su propia red o usa un agregador. Las redes de grandes cadenas con sistemas de seguridad gestionados son generalmente más fiables que la red configurada hace tres años por el propietario del café de barrio con un router doméstico al que nunca le han cambiado la contraseña de administración.

Qué tan actualizado está tu dispositivo. Un sistema operativo actualizado con los parches de seguridad al día reduce significativamente la superficie de ataque. No completamente, pero sí de forma notable.

Reflexión estratégica: el WiFi público como metáfora del ecosistema digital

Hay algo que el análisis técnico del man-in-the-middle no termina de capturar: la razón por la que estas redes son un vector de ataque eficaz no es solo técnica. Es psicológica y cultural.

Nos hemos acostumbrado a que la conectividad sea gratuita y ubicua. Pedimos el WiFi del café con la misma naturalidad con que pedimos la sal. Esa normalización ha erosionado la percepción de riesgo hasta hacerla prácticamente inexistente. Y los atacantes lo saben. Por eso proliferan las redes falsas en aeropuertos: porque la gente llega cansada, distraída y necesitada de conexión, y se conecta a lo primero que aparece con el nombre que suena razonable.

La ciberseguridad aplicada no consiste en vivir con paranoia digital ni en llevar siempre encima una VPN como si fuera un chaleco antibalas. Consiste en desarrollar un criterio:

entender qué acción estás haciendo, qué información está en juego y qué precauciones son razonables en ese contexto. Eso no requiere ser técnico. Requiere ser consciente.

Tu próximo paso (son solo tres hábitos)

Primero, desactiva la opción "conectarse automáticamente a redes conocidas" en tu teléfono y portátil. Que sea siempre una decisión consciente, no un automatismo.

Segundo, cuando uses WiFi pública para algo que importe —trabajo, banca, cuentas con información sensible—, activa una VPN de confianza antes de conectarte. Si no tienes una, el servicio de tu empresa o una de pago con política clara de no registros son opciones razonables.

Tercero, ante cualquier portal cautivo que te pida más datos de los necesarios, desconfía. Tu nombre y correo no son necesarios para darte acceso a internet en un café. Si te los piden, alguien está recopilando algo.

Si este artículo te ha sido útil, compártelo con alguien que se conecte a redes públicas sin pensarlo dos veces. Una persona que entiende el riesgo toma mejores decisiones, y eso importa. Visita el blog para acceder a más recursos gratuitos sobre seguridad digital aplicada.

Isaac Ruiz Romero.