

10 consellos para usar as redes públicas sen riscos



As redes wifi públicas forman parte do noso día a día. Permítenos conectarnos en aeroportos, estacións, bibliotecas, cafeterías ou hoteis, facilitando o acceso a Internet cando máis o necesitamos. Aínda que moitas veces se presentan como un risco que hai que evitar, o certo é que poden empregarse con seguridade se seguimos unhas recomendacións básicas.

A clave é utilizalas con criterio: comprobar que nos conectamos á rede correcta, protexer o noso dispositivo e adaptar o tipo de actividade á confianza que nos ofrece a conexión.

Este decálogo recolle dez consellos sinxelos para que poidas aproveitar as vantaxes das redes wifi públicas reducindo os riscos e navegando con maior tranquilidade.

Coa colaboración de



Antes de navegar



Desactiva a conexión automática ás redes wifi.

Evitarás que o teu dispositivo se conecte sen que te decates a puntos de acceso fraudulentos.



Comproba que te conectas á rede correcta.

Verifica o nome da wifi cos carteis do establecemento ou preguntando ao persoal. Desconfía de redes con nomes moi parecidos á oficial.

Mentres navegas



Usa unha VPN de confianza.

Unha rede privada virtual cifra todo o tráfico entre o teu dispositivo e Internet, engadindo unha capa extra de protección.



Reserva as operacións sensíbles para conexións de confianza.

Evita acceder á banca electrónica, facer pagos ou consultar información persoal ou laboral desde unha wifi pública. Se é posible, utiliza os datos móbiles ou un punto de acceso persoal.



Comproba sempre que as páxinas web son lexítimas.

Asegúrate de que o enderezo é o correcto e de que utiliza HTTPS (o cadeado do navegador). Lembra que unha páxina con cadeado tamén pode ser fraudulenta se o enderezo non é o auténtico.



Non descargues programas nin aceptes peticións inesperadas.

Se a páxina de acceso á wifi che pide instalar software, introducir datos innecesarios ou realizar un pago inesperado, detente e verifica que é unha solicitude lexítima.

No teu dispositivo



Mantén o dispositivo actualizado.

Instala as últimas actualizacións do sistema operativo, do navegador e das aplicacións para corrixir vulnerabilidades coñecidas.



Activa a autenticación en dous pasos cando sexa posible.

Se alguén consegue o teu contrasinal, este segundo factor de verificación dificultará o acceso ás túas contas.



Desactiva o intercambio de ficheiros e o Bluetooth cando non os necesites.

Así reducirás as posibilidades de que outros dispositivos da rede poidan detectarte ou acceder ao teu equipo.

Ao rematar



Ao rematar, desconecta e elimina a rede gardada.

Esquece esa wifi no teu dispositivo para evitar conexións automáticas no futuro a unha rede co mesmo nome.

Unha wifi pública non é necesariamente insegura. O importante é verificar a rede á que te conectas, protexer o teu dispositivo e adaptar o tipo de actividade ao nivel de confianza da conexión. Navegar, consultar información ou ler o correo adoita ser seguro; para operacións críticas, é mellor recorrer aos datos móbiles ou a unha rede de confianza.