

Wi-Fi public : travailler dehors sans s'exposer

Hôtel, gare, café, salon professionnel : les vrais risques des réseaux publics et les réflexes qui les neutralisent.

7 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/wifi-public

Le Wi-Fi gratuit est partout — et travailler dessus est devenu banal. Les risques réels ont évolué : le chiffrement généralisé (HTTPS) a tué une partie des attaques d'hier, mais les faux points d'accès, les portails piégés et les réseaux mal isolés restent des pièges efficaces. Les bons réflexes tiennent en peu de choses — et le meilleur d'entre eux tient dans votre poche.

1. Ce qui peut vraiment arriver

- Le faux point d'accès : un réseau nommé « WiFi_Hotel_Gratuit » monté par un attaquant dans le hall — tout votre trafic passe par lui, et son portail « de connexion » collecte ce que vous y tapez
- Le réseau partagé mal isolé : sur certains réseaux publics, les appareils se voient entre eux — un poste mal configuré expose ses partages
- Le portail captif piégé : la page de connexion qui demande email et mot de passe « pour accéder » — et récolte des identifiants souvent réutilisés ailleurs
- Ce qui n'arrive plus guère : lire vos emails « en clair » — le HTTPS généralisé chiffre l'essentiel ; le danger s'est déplacé vers la tromperie

2. Le réflexe n° 1 : votre propre connexion

Le partage de connexion 4G/5G du téléphone est presque toujours la meilleure réponse : votre réseau, chiffré, sans inconnu au milieu. Les forfaits actuels le permettent largement, et le débit dépasse souvent le Wi-Fi public saturé. Réservez donc le Wi-Fi public aux cas où la 4G fait défaut (sous-sols, étranger sans forfait data, gros téléchargements) — et appliquez alors les règles qui suivent.

3. Si le Wi-Fi public s'impose

- Vérifier le nom exact du réseau auprès du lieu (le comptoir, l'affichette) — les clones jouent sur les variantes
- VPN d'entreprise activé pour tout accès aux ressources professionnelles (voir notre guide)
- Jamais d'identifiants saisis sur un portail captif au-delà du strict nécessaire — et jamais un mot de passe que vous utilisez ailleurs
- Vérifier le cadenas HTTPS avant toute saisie sensible ; un avertissement de certificat sur un réseau public = on arrête tout
- Désactiver le partage de fichiers et déclarer le réseau « public » quand le système le demande (Windows le propose)
- Oublier le réseau après usage : votre appareil ne doit pas s'y reconnecter tout seul le mois prochain

CAS CONCRET

Salon professionnel : un « WiFi_Salon_Exposants » gratuit apparaît, sans mot de passe. Des dizaines de commerciaux s'y connectent et consultent leur messagerie. Le réseau était monté depuis un sac à dos, à des fins de démonstration par des chercheurs en sécurité — mais il aurait pu l'être par n'importe qui. Le vrai réseau du salon exigeait un code remis à l'accueil.

4. Cadrer pour l'équipe

- La règle simple dans la charte : partage 4G d'abord ; Wi-Fi public seulement avec VPN
- Des forfaits mobiles dimensionnés pour le partage — l'économie sur la data se paie en risques
- Les portables configurés d'avance : VPN installé, partages désactivés, pare-feu actif
- Un mot d'ordre pour les portails captifs : jamais le mot de passe de l'entreprise, nulle part

L'essentiel à retenir

- 01 Privilégier systématiquement le partage de connexion 4G/5G
- 02 Activer le VPN avant tout usage professionnel d'un Wi-Fi public
- 03 Vérifier le nom du réseau auprès du lieu
- 04 Ne jamais réutiliser un mot de passe sur un portail captif
- 05 Déclarer le réseau « public » et couper les partages
- 06 Faire oublier le réseau après usage

Questions fréquentes

Un VPN grand public (NordVPN, etc.) suffit-il sur le Wi-Fi public ?

Pour chiffrer votre trafic vers Internet, oui — c'est leur vrai cas d'usage pertinent. Il ne remplace pas le VPN d'entreprise pour accéder aux ressources internes, et ne protège ni d'un faux portail où vous tapez vos identifiants, ni d'un site de phishing. Utile en déplacement, mais ce n'est pas une immunité.

Consulter simplement ses emails sur le Wi-Fi de l'hôtel, est-ce risqué ?

Avec une messagerie moderne (HTTPS, MFA activée), le risque de simple consultation est faible. Le vrai danger est le contexte : la fausse page de connexion qui ressemble à votre webmail, le certificat douteux qu'on accepte par lassitude. Si la MFA est active et que vous ne validez rien d'anormal, vous êtes raisonnablement protégé — la 4G reste mieux.

Et les bornes USB de recharge dans les gares et aéroports ?

Le risque (« juice jacking ») est plus théorique que massif, mais la parade coûte zéro : votre propre chargeur sur une prise secteur, ou une batterie externe. Si le téléphone demande « Autoriser le transfert de données ? » en se branchant quelque part : refuser, toujours.

Pour aller plus loin

Cybermalveillance.gouv.fr — les usages en mobilité — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso

ANSSI — recommandations sur le nomadisme numérique — cyber.gouv.fr/publications/recommandations-sur-le-nomadisme-numerique

Besoin d'aide pour le mettre en place ?

Audit, durcissement, accompagnement : Cyberionis sécurise les TPE, PME et collectivités, à Nancy, Lure et à distance.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr