



Wi-Fi à l'hôtel : les bons réflexes à avoir avant de se connecter en voyage

By Floriane

C'est devenu un vrai casse-tête : lors de nos voyages, Internet est aujourd'hui presque indispensable. Comme on [travaille souvent à distance](#) et qu'on passe beaucoup de temps à organiser nos itinéraires en ligne, on se connecte à de nombreux réseaux Wi-Fi : dans les hôtels, les cafés, les gares ou encore les aéroports.

Avec le temps, on a donc pris quelques habitudes. Avant de se connecter à un Wi-Fi public, on vérifie toujours le **nom du réseau**, on évite certaines **actions sensibles** et, surtout, on **active presque systématiquement notre VPN**.

Quelques bons réflexes suffisent pour profiter du Wi-Fi à l'hôtel ou ailleurs sans s'exposer inutilement, et continuer à voyager connecté l'esprit plus léger.

Pourquoi le Wi-Fi de l'hôtel demande un minimum de vigilance

Quand on se connecte au Wi-Fi d'un hôtel, on rejoint généralement un réseau utilisé par beaucoup d'autres personnes et les [réseaux Wi-Fi des hôtels sont parmi les plus faciles à exploiter](#).

Dans la majorité des cas, tout se passe très bien. On **consulte ses mails**, on prépare **la journée du lendemain**, on **envoie quelques messages** et on n'y pense plus.

Mais un **réseau public reste plus exposé qu'une connexion privée**. Il peut être mal configuré, peu sécurisé ou tout simplement utilisé par des personnes qu'on ne connaît pas. C'est justement ce côté "partagé" qui demande un peu de prudence.

Le risque le plus connu, c'est **l'interception des données**. En clair, une personne mal intentionnée peut essayer de se placer entre votre appareil et le réseau pour observer ce qui circule. On parle souvent d'attaque "man-in-the-middle", mais pas besoin de retenir le terme technique. Ce qu'il faut comprendre, c'est qu'un Wi-Fi public n'offre pas toujours le même niveau de confidentialité qu'une connexion personnelle.

Wi-Fi à l'hôtel : les bons réflexes à avoir avant de se connecter en voyage

Aujourd'hui, beaucoup de sites sont heureusement mieux sécurisés qu'avant grâce au HTTPS, le fameux petit cadenas que l'on voit dans le navigateur. C'est une bonne chose. Mais cela ne veut pas dire qu'il faut cliquer partout les yeux fermés, surtout lorsqu'on se connecte depuis un réseau inconnu.

Wi-Fi à l'hôtel : les bons réflexes à avoir avant de se connecter
en voyage

Wi-Fi à l'hôtel : les bons réflexes à avoir avant de se connecter
en voyage

Les faux réseaux Wi-Fi : le piège tout simple

Il y a un autre risque très concret en voyage : les faux points d'accès Wi-Fi, comme [on a pu en trouver dans certains aéroports](#).

Le principe est assez simple. Une personne mal intentionnée crée un réseau Wi-Fi avec un nom qui semble crédible, justement pour inciter les voyageurs à s'y connecter sans trop réfléchir. Une fois connecté au mauvais réseau, votre trafic internet passe par un point d'accès que vous ne maîtrisez pas.

Voici quelques exemples de noms qui peuvent sembler fiables au premier regard :

- Hotel Guest
- Hotel WiFi Free
- NomDeLHotel_Guest
- Lobby Internet
- Free Hotel WiFi

Les bonnes habitudes à adopter avant de se connecter

Vérifier le nom exact du réseau à la réception

Le bon réflexe, tout simple : demander à la réception le nom exact du réseau Wi-Fi de l'hôtel.

Avant de vous connecter, prenez quelques secondes pour demander à la réception le nom officiel du réseau Wi-Fi de l'hôtel. Cette simple vérification élimine le risque de tomber sur un faux hotspot.

Le VPN, notre réflexe sécurité quand on voyage

Avec les années, le VPN est devenu l'un de nos outils de voyage. Pas le plus glamour, on vous l'accorde. Il ne fait pas rêver comme un lever de soleil sur une plage ou une adresse confidentielle dénichée au hasard d'une ruelle. Mais dans la pratique, il nous simplifie vraiment la vie.

Wi-Fi à l'hôtel : les bons réflexes à avoir avant de se connecter en voyage

Quand on part en voyage, on se connecte à internet partout : hôtels, cafés, gares, aéroports, logements, espaces de coworking... Parfois pour consulter un itinéraire, parfois pour gérer des réservations, parfois pour travailler. Et dans ces moments-là, on préfère ne pas dépendre uniquement du niveau de sécurité du réseau sur lequel on tombe.

Un VPN, ou **réseau privé virtuel**, permet de chiffrer la connexion entre votre appareil et internet. Pour faire simple, il crée une sorte de **tunnel sécurisé**. Même si vous utilisez le Wi-Fi d'un hôtel, vos données deviennent beaucoup plus difficiles à lire pour une personne qui tenterait de les intercepter.

Ce qu'on apprécie surtout, c'est le côté automatique. Une fois l'application installée, **il suffit de l'activer avant de se connecter au Wi-Fi public**. On choisit un serveur, on attend quelques secondes, puis on utilise internet normalement.

Pourquoi choisir un VPN sans logs ?

Tous les VPN ne se valent pas. Quand on parle de voyage et de confidentialité, un point revient souvent : la politique de conservation des données.

Un [VPN no log](#), signifie que le service annonce ne pas conserver l'historique de navigation de ses utilisateurs. En pratique, cela veut dire qu'il ne garde pas de traces détaillées de ce que vous faites en ligne.

C'est un critère important, car utiliser un VPN revient aussi à faire confiance au fournisseur du VPN. Il ne s'agit donc pas seulement **d'en installer un au hasard** parce qu'il apparaît en premier dans une recherche. Mieux vaut prendre le temps de regarder sa réputation, sa politique de confidentialité, les pays dans lesquels il opère, les appareils compatibles et la simplicité d'utilisation.

En voyage, on privilégie surtout un VPN facile à utiliser. Parce que le meilleur outil de sécurité reste celui qu'on utilise vraiment. Si l'application est trop compliquée, trop lente ou trop instable, on finit par la désactiver. Et là, elle ne sert plus à grand-chose.

Les critères qui comptent le plus selon nous :

- une application simple sur téléphone et ordinateur ;
- une connexion stable ;

Wi-Fi à l'hôtel : les bons réflexes à avoir avant de se connecter en voyage

- une politique sans logs claire ;
- des serveurs dans plusieurs pays ;
- une activation rapide ;
- une bonne compatibilité avec les usages en voyage.

Les situations où on active toujours notre VPN

Il y a des moments où on ne se pose même plus la question.

Quand on est sur un Wi-Fi public, on active le VPN automatiquement.

C'est le cas à **l'hôtel**, bien sûr, mais aussi dans les **aéroports** et **gares**. Les longues attentes entre deux vols sont souvent le moment où l'on sort l'ordinateur pour avancer sur deux ou trois choses. Sauf que les réseaux d'aéroport sont très fréquentés, parfois ouverts, parfois avec des noms qui se ressemblent. Dans ce contexte, le VPN devient un vrai réflexe de base.

Même chose dans les **cafés**. On adore s'installer quelque part avec un ordinateur et une boisson. C'est souvent dans ces moments-là qu'on prépare la suite du voyage, qu'on trie des photos ou qu'on répond à quelques messages. Mais là encore, le Wi-Fi est partagé avec tous les clients autour de nous.

On l'active aussi dans **les espaces de coworking** quand on ne connaît pas bien la configuration du réseau.

Ce qu'il vaut mieux éviter de faire sur le Wi-Fi public

Même avec un VPN, on garde quelques réflexes simples. Sur le Wi-Fi d'un hôtel, d'un café, d'une gare ou d'un aéroport, voici notre petite check-list :

- **Ne pas se connecter au premier réseau venu** : on vérifie toujours le nom exact du Wi-Fi, surtout à l'hôtel en demandant à la réception.
- **Éviter d'envoyer des documents sensibles** : passeport, justificatif d'identité, documents bancaires ou informations professionnelles importantes.
- **Ne pas saisir ses informations bancaires sur un site douteux** : avant de payer, on vérifie que le site est bien en **https** et que le petit cadenas apparaît dans le navigateur.
- **Ne pas oublier d'activer son VPN** : dès qu'on utilise un Wi-Fi public, on l'active presque automatiquement, surtout pour consulter ses mails, réserver un transport ou se connecter à un compte personnel.
- **Éviter de rester connecté à ses comptes sensibles** : banque, assurance, espace administratif, messagerie pro... une fois terminé, on se déconnecte.

Wi-Fi à l'hôtel : les bons réflexes à avoir avant de se connecter en voyage

- **Désactiver la connexion automatique au Wi-Fi** : cela évite que le téléphone ou l'ordinateur se connecte tout seul à un réseau non sécurisé.
- **Faire les mises à jour avant le départ** : téléphone, ordinateur, navigateur, applications importantes... c'est toujours plus simple à faire à la maison qu'avec un Wi-Fi d'hôtel capricieux.

Notre routine simple avant de se connecter en voyage

Aujourd'hui, quand on arrive dans un hôtel, notre routine est presque toujours la même.

Wi-Fi à l'hôtel : les bons réflexes à avoir avant de se connecter en voyage

On demande le nom exact du Wi-Fi à la réception. On se connecte uniquement au réseau indiqué. On active le VPN sur le téléphone et l'ordinateur. On vérifie que les sites utilisés sont bien sécurisés. Et si quelque chose nous paraît étrange, on passe plutôt par notre connexion mobile.

Ce n'est pas une routine parfaite, mais elle a le mérite d'être simple. Et en voyage, c'est souvent ce qui fonctionne le mieux.

N'hésitez pas à nous laisser un **petit mot** ci-dessous si vous avez des questions ici ou sur [Instagram](#), nous vous répondrons avec grand plaisir.

Donnez une note à cet article :
1 avis (5/5)

Merci de partager notre article :

- [Partager sur X\(ouvre dans une nouvelle fenêtre\) X](#)
- [Partager sur Facebook\(ouvre dans une nouvelle fenêtre\) Facebook](#)
- [Partager sur Pinterest\(ouvre dans une nouvelle fenêtre\) Pinterest](#)
- [Partager sur WhatsApp\(ouvre dans une nouvelle fenêtre\) WhatsApp](#)
- [Plus](#)