Fiche Pratique N°83 : Protégez-vous sur un Wi-Fi public et en voyage V1.0

14 nov, 2026 · @Gabriel

Objectif : *utiliser sans crainte le Wi-Fi d'une gare, d'un hôtel, d'un camping ou d'un café, savoir quand préférer le partage de connexion de votre téléphone, et préparer vos appareils avant un voyage.*

- ***Public visé :*** *débutant*
- ***Temps estimé :*** *15 minutes de réglages, une fois pour toutes ; 30 minutes de préparation avant un voyage lointain*
- ***Difficulté :*** ★☆☆☆☆ *(Très facile)*
- ***Prérequis :*** *un téléphone et, si besoin, un ordinateur portable à jour ; votre forfait mobile (vérifier les pays inclus)*
- ***Fiches associées :*** *N°4, N°5 et N°45 (VPN), N°44 (les limites du VPN), N°2 (naviguer sans être pisté), N°18 (authentification à deux facteurs), N°52 (régler la confidentialité de son téléphone), N°19a à N°19e (sauvegardes), N°81 (effacer ses données)*

PARTIE 1 : LES BASES (pour débutants)

1. Le problème : un réseau partagé avec des inconnus

Le Wi-Fi gratuit d'un lieu public est pratique, mais vous le partagez avec tous les autres clients, et vous ne savez pas qui l'a installé. La plupart des sites sont aujourd'hui chiffrés (le petit cadenas, `https`), ce qui protège déjà beaucoup. Les vrais dangers sont ailleurs : un **faux réseau** au nom trompeur, une **page de connexion piégée** qui demande vos identifiants, ou un appareil qui se connecte tout seul à n'importe quel réseau.

Situation	Conséquence
Vous vous connectez à « Gare-WiFi-Gratuit » sans vérifier	C'est peut-être un faux réseau créé par un voisin malveillant
La page d'accueil du Wi-Fi demande votre compte Google ou Facebook	Vos identifiants peuvent être volés, et le lieu collecte vos données
Votre téléphone se connecte automatiquement aux réseaux connus	Un faux réseau qui porte le même nom l'attire sans que vous le sachiez
Vous faites un virement depuis le Wi-Fi d'un camping	Vous prenez un risque inutile, alors que la 4G est plus sûre
Vous rechargez votre téléphone sur une borne USB publique	Une borne trafiquée pourrait tenter d'accéder au téléphone

Une image pour comprendre : un Wi-Fi public, c'est une salle d'attente. Ce que vous dites en clair, vos voisins peuvent l'entendre. Le cadenas `https`, c'est une conversation dans une langue que seul votre interlocuteur comprend. Le partage de connexion de votre téléphone, c'est un bureau fermé où vous êtes seul.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°83 : Protégez-vous sur un Wi-Fi public et en voyage V1.0

Le risque : des identifiants volés, un compte piraté, ou des données personnelles collectées par le lieu qui offre le Wi-Fi.

Le bénéfice : quelques réflexes simples pour profiter du Wi-Fi gratuit sans danger, et voyager l'esprit tranquille.

2. Comprendre vos options de connexion

Option	Sécurité	Coût	Quand l'utiliser
Données mobiles (4G, 5G)	Bonne : la connexion vous est propre	Votre forfait	Banque, achats, démarches administratives
Partage de connexion du téléphone	Bonne, si protégé par un mot de passe	Votre forfait	Travailler sur un ordinateur portable en déplacement
Wi-Fi public avec `https`	Correcte pour la navigation courante	Gratuit	Lire les actualités, consulter un horaire, regarder une vidéo
Wi-Fi public + VPN	Bonne : tout passe par un tunnel chiffré	Gratuit (Proton VPN) ou payant	Usage prolongé d'un Wi-Fi public (hôtel, camping)
Wi-Fi public sans précaution	Faible	Gratuit	À éviter pour tout ce qui demande un mot de passe

Le bon réflexe : pour tout ce qui touche à l'argent ou à l'identité, passez sur les **données mobiles**.

Avant de commencer

- ☐ Mon téléphone et mon ordinateur sont **à jour** (système et applications)
- ☐ L'écran de mon téléphone est **verrouillé** par un code
- ☐ L'**authentification à deux facteurs** est activée sur mes comptes importants (fiche N°18)
- ☐ Je connais les **pays inclus** dans mon forfait mobile (la Suisse n'est pas toujours incluse)
- ☐ J'ai installé un **VPN** de confiance si je compte utiliser souvent des Wi-Fi publics (fiches N°4, N°5 ou N°45)

3. Pas à pas : régler votre téléphone une fois pour toutes

1. **Désactivez la connexion automatique** aux réseaux Wi-Fi ouverts. Sur Android : **Paramètres** › **Réseau et Internet** › **Internet** › **Préférences réseau** › désactivez **Se connecter aux réseaux publics** ou **Activer le Wi-Fi automatiquement** (selon la marque). Sur iPhone : **Réglages** › **Wi-Fi** › **Demander à rejoindre** › **Demander**.
    - Vous devez voir : le téléphone vous demande avant de rejoindre un nouveau réseau.
2. **Faites le ménage dans les réseaux enregistrés** : supprimez ceux des hôtels, gares et cafés (**Réseaux enregistrés** sur Android ; sur iPhone, touchez le réseau › **Oublier ce réseau**).

gabriel.ananda@mailo.com
CC BY SA

   - Vous devez voir : seuls vos réseaux de confiance (maison, travail, famille) restent dans la liste.
3. **Protégez votre partage de connexion** : **Paramètres** › **Partage de connexion** (ou **Point d'accès**) : mot de passe long, sécurité **WPA2** ou **WPA3**.
   - Vous devez voir : un nom de réseau et un mot de passe que vous avez choisis.
4. **Désactivez le Bluetooth et le Wi-Fi** quand vous ne vous en servez pas, en voyage.
   - Vous devez voir : les icônes Wi-Fi et Bluetooth grisées dans le volet des réglages rapides.

4. Pas à pas : se connecter à un Wi-Fi public

1. **Demandez le nom exact du réseau** au personnel ou lisez-le sur l'affiche officielle.
   - Vous devez voir : un nom identique, lettre pour lettre, dans la liste des réseaux.
2. **Connectez-vous**, puis remplissez la **page d'accueil** (portail) si elle apparaît : acceptez les conditions, sans donner vos comptes Google ou Facebook. Préférez une adresse de courriel jetable ou un alias (fiche N°56) si un courriel est exigé.
   - Vous devez voir : un message « Vous êtes connecté ».
3. **Activez votre VPN** si vous restez longtemps sur ce réseau.
   - Vous devez voir : l'icône de clé ou « VPN » dans la barre d'état.
4. **Vérifiez le cadenas** dans la barre d'adresse avant de saisir un mot de passe.
   - Vous devez voir : un cadenas fermé et une adresse en `https://` exacte (pas de faute dans le nom du site).
5. **En partant, oubliez le réseau** (voir section 3, étape 2).
   - Vous devez voir : le réseau absent de la liste des réseaux enregistrés.

5. Dépannage

Symptôme	Cause possible	Action
Connecté au Wi-Fi, mais aucune page ne s'ouvre	La page d'accueil du réseau n'est pas apparue	Ouvrez le navigateur et tapez `http://neverssl.com` pour la faire apparaître
Le VPN empêche la page d'accueil de s'afficher	Le VPN bloque tout avant la connexion	Désactivez le VPN, validez la page d'accueil, puis réactivez-le
Deux réseaux portent presque le même nom	L'un d'eux est peut-être un faux	Demandez au personnel lequel est le bon ; dans le doute, utilisez les données mobiles
Le navigateur affiche « Connexion non sécurisée »	Site sans `https`, ou réseau qui intercepte les connexions	Ne saisissez rien ; quittez ce réseau
Le téléphone se reconnecte tout seul à un vieux réseau	Réseau resté enregistré	Oubliez-le (section 3, étape 2)

gabriel.ananda@mailo.com
CC BY SA

Symptôme	Cause possible	Action
Le forfait ne marche pas à l'étranger	Itinérance désactivée, ou pays non inclus	Activez l'**itinérance des données** ; vérifiez les pays inclus auprès de votre opérateur

PARTIE 2 : ALLER PLUS LOIN (pour intermédiaires et avancés)

6. Ordinateur portable : trois réglages utiles

- **Mode HTTPS uniquement** dans Firefox : menu ☰ › **Paramètres** › **Vie privée et sécurité** › **Mode HTTPS uniquement** › **Activer le mode HTTPS uniquement dans toutes les fenêtres**.
- **Pare-feu activé** : sous Linux Mint, Menu › **Administration** › **Configuration du pare-feu** › **État** activé ; sous Windows, le pare-feu est actif par défaut (choisissez **Réseau public** quand Windows le demande).
- **Partage de fichiers désactivé** sur les réseaux publics : sous Windows, un réseau déclaré **public** désactive le partage.

7. Préparer un voyage

Avant le départ	Pendant le voyage	Au retour
Faire les mises à jour et une sauvegarde (fiches N°19a à N°19e)	Garder ses appareils sur soi, ne pas les prêter	Supprimer les applications installées pour le voyage
Vérifier les pays inclus dans son forfait, et le coût hors forfait	Utiliser son propre chargeur sur une prise électrique plutôt qu'une borne USB	Oublier les réseaux Wi-Fi des hôtels et des gares
Noter les numéros utiles (opposition bancaire, consulat) sur papier	Limiter les connexions aux comptes sensibles au strict nécessaire	Changer un mot de passe saisi sur un ordinateur public
Hors de l'Union européenne : ne partir qu'avec les données nécessaires, voire un téléphone réinitialisé	Ne pas publier sa position ni ses dates d'absence en direct	Restaurer sa sauvegarde si l'on est parti avec un téléphone vide

Dans l'Union européenne, votre forfait français s'utilise en général aux mêmes conditions qu'en France (itinérance « comme à la maison »), dans les limites fixées par votre opérateur. **Hors Union européenne**, y compris en **Suisse**, tout dépend du forfait : vérifiez avant de franchir la frontière.

Hors de l'Union européenne, la CNIL conseille de se renseigner sur les règles du pays, d'installer au dernier moment une application imposée et de limiter ses autorisations, et si possible de voyager avec un téléphone vierge (sauvegarde, puis réinitialisation, fiche N°81).

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°83 : Protégez-vous sur un Wi-Fi public et en voyage V1.0

8. Les ordinateurs publics (hôtel, médiathèque, cybercafé)

- Utilisez une **fenêtre de navigation privée**, et déconnectez-vous de chaque site avant de partir.
- Ne cochez jamais **Se souvenir de moi** ni **Enregistrer le mot de passe**.
- Évitez d'y saisir vos mots de passe les plus importants (messagerie principale, banque) ; si vous l'avez fait, changez-les au retour.
- N'y branchez pas votre clé USB personnelle si vous pouvez l'éviter.

À savoir avant de se lancer

Crainte fréquente	La réalité
« Sur un Wi-Fi public, tout le monde voit ce que je fais. »	Grâce au `https`, le contenu des pages et vos mots de passe sont chiffrés. Le danger principal, ce sont les faux réseaux et les fausses pages de connexion.
« Avec un VPN, je ne risque plus rien. »	Le VPN protège la connexion, pas contre une fausse page qui vous demande votre mot de passe (fiche N°44).
« Le partage de connexion va vider mon forfait. »	La navigation courante consomme peu ; seules les vidéos et les mises à jour pèsent lourd.
« Je suis en Europe, donc la Suisse est incluse. »	Pas forcément : la Suisse n'est pas dans l'Union européenne. Vérifiez votre forfait.
« Les bornes USB des gares sont faites pour recharger. »	Oui, mais votre propre chargeur sur une prise électrique ne présente aucun risque.

Challenge 7 jours

- **Jour 1 :** désactivez la connexion automatique aux réseaux Wi-Fi ouverts.
- **Jour 2 :** supprimez les réseaux enregistrés d'hôtels, de gares et de cafés.
- **Jour 3 :** protégez votre partage de connexion par un mot de passe long, et testez-le avec votre ordinateur.
- **Jour 4 :** activez le mode HTTPS uniquement dans Firefox.
- **Jour 5 :** installez un VPN de confiance (fiches N°4, N°5 ou N°45).
- **Jour 6 :** vérifiez les pays inclus dans votre forfait, dont la Suisse.
- **Jour 7 :** notez sur papier les numéros d'urgence à emporter en voyage.

Vous allez constater : quelques réglages suffisent pour profiter du Wi-Fi gratuit sans arrière-pensée.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°83 : Protégez-vous sur un Wi-Fi public et en voyage V1.0

En résumé (ce que vous gagnez)

Action	Gagné	Renvoi
Désactiver la connexion automatique	Plus de connexion à un faux réseau à votre insu	Section 3
Vérifier le nom du réseau et le cadenas	Vos identifiants restent à vous	Section 4
Utiliser les données mobiles pour la banque	Les opérations sensibles hors des réseaux partagés	Section 2
Préparer ses appareils avant un voyage	Moins de risques, et un retour sans mauvaise surprise	Section 7

À retenir absolument

- **Banque, achats, démarches** : sur les données mobiles, pas sur un Wi-Fi public.
- **Vérifiez le nom exact du réseau** et le **cadenas** avant de saisir un mot de passe.
- **Désactivez la connexion automatique**, et oubliez les réseaux publics après usage.
- **Votre chargeur sur une prise** plutôt qu'une borne USB inconnue.

Test final :

1. Mon téléphone ne se connecte plus tout seul aux réseaux ouverts.
2. Ma liste de réseaux enregistrés ne contient que des réseaux de confiance.
3. Mon partage de connexion est protégé par un mot de passe.
4. Je sais quand utiliser les données mobiles plutôt que le Wi-Fi.
5. Je sais préparer mes appareils avant un voyage. ✅

Références

- ANSSI – Les essentiels : sécurisation des réseaux Wi-Fi (V1.0, août 2026)
- CNIL – Voyager en dehors de l'UE : la checklist pour protéger votre téléphone, ordinateur ou tablette
- Préfecture de la région Île-de-France – Les risques liés à l'utilisation des réseaux Wi-Fi publics (fiche d'information n°55)
- Selectra – Wi-Fi de camping, d'hôtel ou public : trois réflexes de sécurité (juillet 2026)
- Cybermalveillance.gouv.fr – Guide de sensibilisation pour les familles
- The Connexion – Warnings issued over connecting to public WiFi networks in France

gabriel.ananda@mailo.com
CC BY SA