

# Connexion Wi-Fi : 5 conseils pour sécuriser votre smartphone

## 1- Verrouillez vos appareils

Lorsque vous voyagez, verrouillez vos appareils mobiles (smartphones, ordinateurs portables et tablettes) grâce à vos empreintes digitales, reconnaissance faciale ou un code PIN. Tout cela représente votre première ligne de défense contre une brèche de sécurité dans le cas où n'importe lequel de vos appareils ait été oublié ou perdu momentanément

## 2 – Limitez le partage de localisation

On le sait ! Vous voulez partager vos souvenirs de vacances avec vos amis et votre famille sur les réseaux sociaux. Cependant, le partage excessif, en particulier le partage de données de localisation, crée une menace pour la sécurité à la maison.

Si vous partagez une photo sur un bateau ou à la Tour Eiffel, il est facile pour les criminels de réaliser que vous n'êtes pas chez vous ou à votre hôtel, ce qui rend vos effets personnels vulnérables au vol ou piratage.

Si vous devez partager vos données de localisation, attendez d'être de retour à la maison pour géolocaliser les selfies de votre voyage.

## 3 – Apportez vos propres chargeurs et adaptateurs

Les cybercriminels ont la capacité d'installer des malwares dans des endroits publics tels que les kiosques d'aéroports et les stations de chargement USB. Si vous ne pouvez pas trouver un espace sécurisé pour charger vos appareils ou si vous n'êtes pas certains de la sécurité de la zone de chargement, éteignez votre appareil avant de le brancher.

## 4 – Désactivez la connexion automatique

La plupart [des téléphones](#) possèdent un paramètre qui permet à l'appareil de se connecter automatiquement aux réseaux Wi-Fi ouverts ou enregistrés. Cette fonctionnalité est utile pour une utilisation à la maison, mais peut laisser votre appareil vulnérable aux cybercriminels qui accèdent à ces fonctionnalités pour des attaques « man-in-the-middle ».

Désactivez la connexion automatique sur vos appareils et effacez les réseaux SSID enregistrés

avant votre voyage pour éviter l'exploitation.

## **5 - Faites attention aux réseaux Wi-Fi publics**

On peut souvent trouver des accès Wi-Fi gratuits dans des cafés ou des hôtels pour les voyageurs, mais les réseaux Wi-Fi non cryptés devraient être évités. Avant de vous connecter à une nouvelle source Wi-Fi, demandez des informations sur le protocole de l'emplacement et si vous devez utiliser une connexion Wi-Fi publique, soyez très prudent.

Utilisez un VPN pour vous connecter à vos réseaux professionnels et évitez d'accéder à vos comptes personnels et données sensibles lorsque vous êtes connecté à un réseau Wi-Fi public.