Utiliser un Wifi public ? Voici 5 précautions à prendre

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Utiliser un Wifi public ? Voici 5 précautions à prendre				

Le plus souvent proposés gratuitement ou en échange de la collecte de données de navigation, certaines de ces connexions « gratuites » n'offrent pas les garanties suffisantes pour une navigation sécurisée.

Ces conseils valent aussi bien pour votre ordinateur (personnel ou professionnel) que pour votre smartphone ou votre tablette.

1.

Évitez de vous connecter à des réseaux sans fil inconnus ou qui ne sont pas de confiance

Plutôt que de vous fier uniquement au nom du réseau qui s'affiche, demandez systématiquement le nom du réseau au commerçant.En effet, il est très facile pour un pirate de créer un point d'accès WiFi au nom d'un restaurant puis de détourner l'ensemble du trafic qui y transitera. Cela peut par exemple permettre au pirate de récupérer les données que vous échangez avec un site de e-commerce ou encore d'obtenir vos données bancaires, les identifiants d'accès à votre compte, …

2.

Ne confiez pas trop d'informations à un portail d'accès Wi-Fi

Difficile de savoir si un portail d'accès Wi-Fi offre un niveau de sécurité satisfaisant ! Si celui-ci vous demande des informations personnelles en échange d'un accès à internet, évitez d'utiliser votre adresse mail principale, remplissez le moins d'informations possibles, et ne cochez pas la case « communiquer mes données à des tiers » à moins que vous ne souhaitiez que vos données soient transmises à des tiers afin qu'ils vous adressent des mails de prospection commerciale.

3.

Evitez de passer par un Wi-Fi public pour transmettre des données personnelles

Préférez passer par le réseau 3G/4G de votre opérateur internet. Si vous n'avez pas le choix, privilégiez toujours la visite de sites HTTPS et utilisez un VPN, de préférence payant ou que vous avez installé vous-même chez vous sur votre connexion personnelle.

4.

Désactivez la fonction Wi-Fi de votre appareil lorsqu'il n'est pas utilisé

N'activez pas la connexion automatique pour les réseaux WiFi autres que ceux de votre bureau ou votre domicile. Ainsi si vous repassez dans la zone de couverture du réseau, votre téléphone ne s'y connectera pas sans votre permission. Attention, même avec la fonction wifi désactivée, certains types de téléphones continuent d'émettre un signal Wi-Fi et sont susceptibles de permettre à des tiers de suivre vos déplacements, dans des centres commerciaux par exemple. Pour éviter cela, désactivez l'option « recherche toujours disponible » si votre téléphone vous le permet.

5.

et soyez à jour !

L'utilisation sécurisée d'un smartphone ou d'un ordinateur nécessite de maintenir le système d'exploitation et les pilotes Wi-Fi du terminal en permanence à jour des correctifs de sécurité. Appliquez régulièrement les mises à jour de sécurité proposées par le fabricant de votre smartphone, ou par l'éditeur de votre système d'exploitation.

LE SAVIEZ-VOUS ?

Les organismes (restaurant, aéroports…) qui proposent un accès au réseau internet au public, à titre payant ou gratuit, sont tenus de conserver les données de trafic de leurs clients. Ils doivent conserver les données techniques (ex. adresse IP, date, heure, durée de chaque connexion, informations permettant d'identifier le destinataire d'une communication). Les informations relatives au contenu des communications, comme l'objet ou le corps d'un courrier électronique ou bien les URL consultées sur un site web, ne doivent pas être conservées. Pour aller plus loin, consultez cette fiche.

LE NET EXPERT

:

• **SENSIBILISATION / FORMATIONS** :

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• **MISE EN CONFORMITÉ RGPD / CNIL**

- **ÉTAT DES LIEUX RGPD** de vos traitements)
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements

• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• **EXPERTISES** & **AUDITS** (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Réagissez à cet article

Source : *Utiliser un Wifi public ? Voici 5 précautions à prendre … | CNIL*