CCIN
COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES

WIFI PUBLIC
Principaux risques et conseils pour les éviter

Qu'est-ce que le WIFI ?

Le WIFI est une technologie dite « *sans fil* » qui permet la connexion de tout type de matériel (ordinateurs portables, tablettes, imprimantes, téléphones mobiles, consoles de jeux, télévisions, équipements électroménagers, automates industriels, etc.) à des réseaux professionnels privés ainsi qu'au réseau public, Internet.

Quid du WIFI public

Il s'agit d'un WIFI ouvert à tout public. Il est notamment utilisé dans les lieux publics tels que les cafés, les transports en commun, les centres commerciaux, les aéroports ou encore certaines zones publiques des villes et villages (parc, place centrale, arrêt de bus, etc.).

Le WIFI public présente de nombreux avantages puisqu'il permet à toute personne de se connecter aux réseaux, rapidement et gratuitement, de travailler sur son ordinateur en dehors du bureau, ou bien encore d'utiliser une application de géolocalisation pour se repérer dans une nouvelle ville.

WIFI public et risques

Bien que le WIFI public permette une connexion à Internet et l'usage d'applications en tout lieu, le recours à celui-ci suscite néanmoins de nombreux risques :

- Virus et logiciel malveillant ;
- Collecte massive de données personnelles et/ou confidentielles ;
- Conservation des données par des tiers ;
- Vol et perte de données ;
- Rançongiciel, dit « *ransomware* » (un pirate informatique demande de l'argent en contrepartie des données qu'il a récupérées) ;
- Surveillance du trafic internet et des utilisateurs (connaissance des sites visités, combien de fois, pendant combien de temps, etc.).

CCIN
COMMISSION DE CONTRÔLE
DES INFORMATIONS NOMINATIVES

Comment se protéger ?

Les 8 conseils pour se prémunir des dangers de l'utilisation du WIFI public

1

Préférer passer par le réseau 3G/4G/5G de son opérateur internet

2

Éviter de confier trop de données personnelles en échange d'un accès WIFI gratuit

3

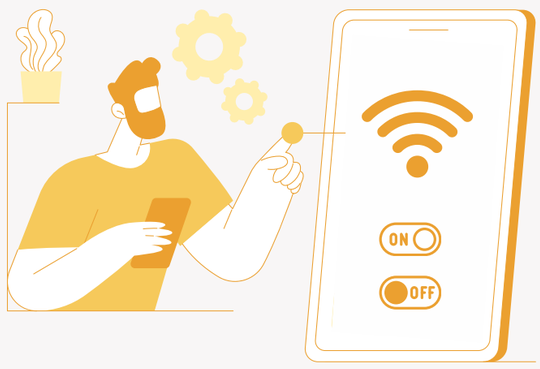
Visiter uniquement des pages « *HTTPS* »

4

Ne pas visiter de pages (sites web) requérant un login et mot de passe

5

Opter pour l'utilisation d'un VPN, permettant une confidentialité des données envoyées et reçues

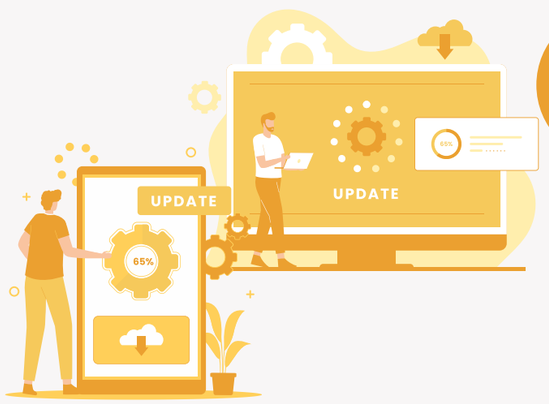


6

Couper « *l'application* » WIFI si elle n'est pas utilisée et ne pas sélectionner la reconnexion automatique

7

Rester vigilant : certains réseaux WIFI sont complètement fictifs et n'existent que pour récupérer des données



8

Garder en permanence le terminal à jour, autrement dit faire régulièrement les mises à jours demandées par l'ordinateur, le téléphone, etc.