# Panoptinet

Gardez un oeil sur votre réseau

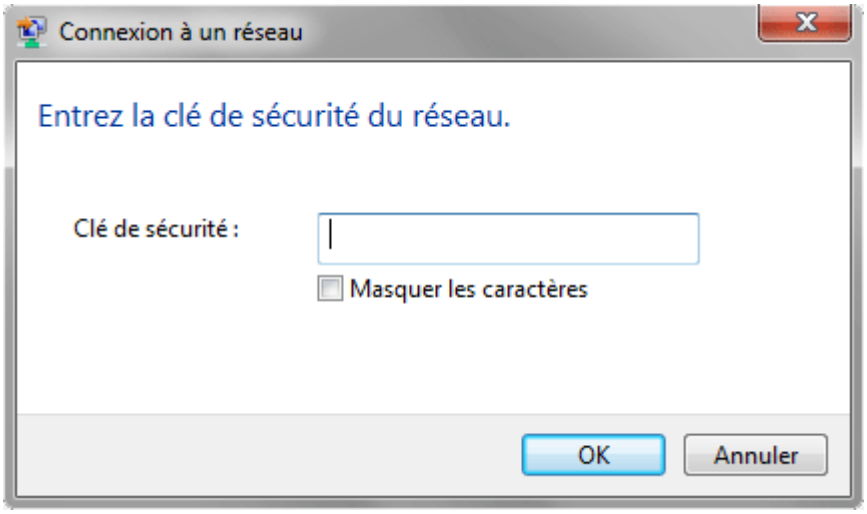
## Pourquoi crypter son réseau Wi-Fi ?

admin · Monday, September 26th, 2011

**Si vous achetez un routeur dans un magasin informatique ou que vous recevez la box de votre FAI, vous vous rendrez compte que c'est assez facile à installer : vous êtes rapidement connecté à Internet ! Que cache cette facilité ?**

A l'installation, la plupart des box et des routeurs propose un **assistant** pour que l'utilisateur puisse utiliser son nouveau jouet dans les meilleurs délais. Mais pas nécessairement dans les bonnes conditions ! La plupart de ces routeurs sont configurés par défaut comme des serveurs DHCP, si bien qu'à partir du moment où l'ordinateur est relié au réseau, il est également connecté à Internet (une adresse IP lui est automatiquement assignée). Ces matériels sont aujourd'hui perçus comme étant **faciles à installer**. Et ils le sont.

Le problème avec les assistants d'installation, c'est qu'**ils oublient souvent de mentionner le chiffrement du Wi-Fi**. Et oui, cela nécessiterait un peu de pédagogie et environ 30 secondes supplémentaires dans l'installation de la box ou du routeur. Gravissime ! Il faut quand même reconnaître que quelques modèles le font, mais la plupart **proposent par défaut un réseau Wi-Fi non-sécurisé**, ou alors avec une sécurisation minimale, pour ne pas rendre le client confus… Le problème, c'est qu'un réseau Wi-Fi peu ou pas crypté, c'est la porte ouverte à toutes sortes d'**attaques**.




### Quels sont les risques d'un réseau Wi-Fi sans chiffrement ?

Prenons l'exemple de Monsieur Sépagrave*, qui revient chez lui avec sa **nouvelle box** ou son **nouveau routeur**. Hop il le branche et commence à surfer sur le web en Wi-Fi, sans régler de cryptage particulier. Si Monsieur Sépagrave habite dans un immeuble, en ville, la couverture Wi-Fi de son routeur peut "arroser" l'ensemble de ses voisins, des commerces du rez-de-chaussée, des parkings environnants, du parc public, etc. **Potentiellement des dizaines d'inconnus pouvant se connecter sur sa box**. Le signal émis peut être à portée de l'autre côté de la rue.

Peut-être Monsieur Sépgrave n'est-il pas conscient de cette réalité, ou peut-être s'en moque-t-il éperdument. A tort : c'est en effet une **pratique dangereuse**. Certains pirates adorent le Wi-Fi, non seulement parce que **ses protections peuvent être faciles à contourner**, mais aussi parce qu'un réseau Wi-Fi peut donner **accès à des informations** particulièrement intéressantes. Dans le cas de Monsieur Sépgrave par exemple, un pirate en herbe peut facilement accéder via le Wi-Fi aux **informations stockées sur son ordinateur** :

- **Mots de passe** et **informations bancaires** pouvant servir à voler de l'argent ou commettre des fraudes
- **Documents personnels**, photos de famille, identifiants web, **mails**, etc. pouvant servir à l'usurpation d'identité ou la revente sur des marchés spécialisés

Bien évidemment, tous ces vols d'information se font au nez et à la barbe de Monsieur Sépagrave, qui n'a aucun moyen de savoir ce qu'il se trame sur son réseau : **le Wi-Fi est invisible** !

Le pirate peut aussi s'intéresser à la connexion de notre triste héros pour en bénéficier à des fins non-avouables, en toute discrétion :

- **Fraudes** en tout genre
- Visite de sites au **contenu illégal** ou suspect (pédo-pornographie, extrêmismes, etc.)
- **Téléchargement illégal** de contenus protégés par le droit d'auteur : films, musique, spectacles, etc. (cf. Hadopi et le délit de négligence caractérisée)

Même si Monsieur Sépagrave n'est pas personnellement l'auteur de ces pratiques, c'est lui le **responsable de sa connexion**, d'un point de vue pénal. De quoi risquer de sérieux démêlés avec les autorités !

Laisseriez-vous des étrangers déambuler librement dans toutes les pièces de votre domicile, à faire l'inventaire de toutes vos affaires personnelles ? Probablement pas. Alors **pourquoi le faire sur votre réseau informatique ?**

Ne soyez pas aussi imprudent que Monsieur Sépagrave, et **cryptez votre réseau Wi-Fi** dès aujourd'hui !

### De la théorie à la pratique, en savoir plus sur le cryptage

- Fiche théorique : Comment fonctionne le Wi-Fi ?
- Fiche pratique : Qu'est ce qu'une clé de cryptage ? WEP, WPA, WPA2
- Tutoriels : Configurer et sécuriser son Wi-Fi, en fonction de sa box
- Logiciel : Au-delà de la protection, surveiller son réseau Wi-Fi

* *Toute ressemblance avec un personnage existant ou ayant existé ne serait que pure coïncidence. Ou pas.*

Source : ghacks.net

Image : Wikimedia

This entry was posted on Monday, September 26th, 2011 at 3:52 pm and is filed under Autres actualités
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.