

BullGuard : Comment sécuriser un réseau sans fil ?

Sécurité

Posté par : JPilo

Publié le : 25/7/2011 14:00:00

BullGuard, spécialiste des solutions de sécurité pour PC et téléphones mobiles donne ses conseils pour sécuriser un réseau sans fil.

De nombreux ménages optent pour un réseau sans fil afin que tous les appareils de la maison soient connectés sans être physiquement branchés à un routeur. Le routeur sans fil se connectant de manière digitale aux différents appareils de la maison, cela peut potentiellement entraîner certains risques.

Par exemple :



⚠ **Le fait que d'autres personnes se connectent** à votre réseau sans fil sans permission à votre voisin de palier est peut-être dans son propre

appartement mais il est physiquement assez proche pour accéder à votre connexion Internet si vous ne la protégez pas.

⚠ **La possibilité que quelqu'un pirate votre accès à Internet.**

⚠ **L'absence de confidentialité que des e-criminels piratent votre système** et interceptent les données que vous envoyez ou recevez, incluant vos mots de passe, vos coordonnées personnelles et bancaires, mettant potentiellement vos

finances en danger et risquant jusqu'au vol d'identité.

Ce que vous pouvez faire

Utiliser des mesures pour sécuriser Internet peut limiter ce type de risques.

La plupart de ces mesures sont assez simples à mettre en place :

⚡ **Changer le mot de passe de l'administrateur** ⚡ le mot de passe donné par le fabricant est facile à pirater. Changez-le donc immédiatement et choisissez votre propre mot de passe. N'utilisez pas votre nom, votre date de naissance, le nom de votre animal ou de votre enfant, ou encore leurs dates de naissance, et essayez d'inclure des nombres aléatoires ainsi que des symboles non-alphanumériques. Tout cela rendra votre mot de passe plus difficile à deviner pour un hacker.

⚡ **Paramétrez votre réseau en mode « caché »** : Éteignez la diffusion SSID (Service Set Identifier) sur le routeur qui indique aux appareils que votre réseau existe ainsi votre réseau cessera de manifester sa présence. Il est évidemment bien plus dur de pirater quelque chose d'invisible !

⚡ **Favorisez l'encodage dans vos paramètres de connexion** . Si votre appareil le supporte, alors l'encodage WPA est le meilleur. Autrement, utilisez l'encodage WEP.

⚡ **Changez le nom SSID par défaut de votre appareil** et choisissez un nom qui ne soit pas facilement identifiable avec vos propres données personnelles. Par exemple, évitez d'appeler votre réseau 27 rue Petit ou

réseau de Jean D. Trouvez un nom dont vous puissiez facilement vous souvenir mais impersonnel.

En prenant ces mesures il sera plus difficile de pirater, d'utiliser votre accès Internet gratuitement, de voler des informations bancaires ou d'effectuer un vol d'identité.

[Pour en savoir plus](#)