La sécurité des réseaux sans fil à domicile

par Martin Felsky
Deuxième édition, 17 janvier 2014

Table des matières

Introduction 1
L'installation de votre réseau sans fil à domicile 2
Sommaire des meilleures pratiques 6
Annexe : Guides d'utilisation des réseaux sans fil à domicile 7

Introduction

Avec la croissance exponentielle dans la popularité des appareils mobiles, l'accès sans fil à Internet à domicile est devenu la norme. Les « appareils sans fil » vont bien au-delà des ordinateurs portatifs, des téléphones intelligents et des tablettes numériques. Votre lecteur Blu-ray, caméra, disques durs, consoles de jeu, thermostats, contrôles d'éclairage, téléviseurs, livres électroniques, imprimantes et plusieurs autres appareils incluant votre voiture, montre-bracelet et lunettes sont ou seront sous peu connectés à Internet, toujours sans fil[1].

Les juges s'inquiètent cependant du fait que les réseaux sans fil domestiques puissent ne pas être suffisamment sûrs ou privés pour traiter des renseignements judiciaires sensibles. Il est facile de se procurer un modem ou un routeur sans fil, et les fournisseurs d'accès Internet les configureront pour vous. Cependant, les installateurs ne modifient pas les configurations de sécurité par défaut; cela est laissé à l'utilisateur. La documentation qui accompagne l'équipement de réseautique sans fil à domicile est souvent incomplète, impossible à comprendre, ou même trompeuse. Si vous avez de la difficulté à comprendre les enjeux techniques ou que vous êtes rebuté par le jargon technique et la documentation remise par votre fournisseur de services, il peut être avantageux d'investir dans une visite à domicile par un spécialiste des réseaux à domicile qui peut rendre votre système aussi sûr que possible. D'un autre côté, si vous êtes relativement à l'aise avec ces éléments, il ne faut que quelques minutes pour configurer la sécurité de votre ordinateur.

Au bout du compte, si votre matériel et vos logiciels ne sont pas configurés et utilisés convenablement, tous les renseignements que vous recevez et transmettez au moyen de

[1] La mise en réseau de tous ces appareils est appelée «Internet des objets ». Google met actuellement au point un moniteur de glucose sanguin sans fil inséré dans un verre de contact.

votre ordinateur ou de vos appareils mobiles à un accès non autorisé par des amateurs, même par inadvertance.

Cet article traite de la sécurité des réseaux sans fil à domicile de façon pratique et en langage clair. Les mesures faciles, gratuites et sensées qui y sont décrites assureront à votre réseau sans fil à domicile une protection raisonnable contre les intrusions. Sachez, cependant, que même si vous suivez toutes les meilleures pratiques recommandées, votre réseau sans fil à domicile ne sera jamais parfaitement protégé. Pour cette raison, toutes les données confidentielles devraient être chiffrées lorsqu'elles sont transmises, ce qui exige l'utilisation d'un réseau privé virtuel ou d'un site Web qui emploie le protocole de chiffrement SSL (l'adresse de ces sites Web débute par https://).

L'installation de votre réseau sans fil à domicile

Les services Internet à domicile passent par les mêmes fils et câbles (ou la même antenne parabolique) que votre service de téléphone conventionnel ou de câblodiffusion. Que vous ayez accès à Internet par la voie de votre service de téléphone ou de câblodiffusion, il vous faut un routeur pour connecter votre ordinateur à Internet. Un routeur est un appareil qui relie deux réseaux – en l'occurrence, votre réseau sans fil à domicile et Internet. Selon l'équipement et le système que vous utilisez, votre routeur peut aussi être appelé passerelle résidentielle, un point de connexion ou un modem.

Point de connexion Internet Bell (Sagemcom) (vue latérale)

Votre routeur se branche dans la prise de téléphone ou de câble murale (ou les deux, selon votre fournisseur Internet) pour accéder à Internet. Un appareil ne peut être branché au routeur par une connexion sans fil que s'il dispose d'une capacité wi-fi interne ou externe.

Un routeur sans fil signale sa disponibilité sur les ondes en tout temps. Toute personne à portée peut capter le signal, dans votre domicile ou à proximité de celui-ci. La sécurité des réseaux sans fil à domicile consiste à empêcher des intrus de capter le signal de votre routeur et d'obtenir accès à votre compte Internet. Comment le fait-on? En configurant le routeur à l'aide du logiciel qui y est intégré et en utilisant le logiciel de gestion de réseau qui fait partie du système d'exploitation de chacun de vos ordinateurs ou appareils mobiles de poche. Commençons d'abord par créer un réseau sans fil à domicile.

Lorsque votre routeur est installé, vous pouvez généralement y accéder avec votre navigateur et une adresse IP locale comme 192.168.xxx.xxx. Vous devez ensuite entrer votre nom d'utilisateur et votre mot de passe. Le point de connexion Bell est livré avec « admin » comme nom d'utilisateur et comme mot de passe. Il va sans dire que vous devez immédiatement modifier ces réglages pour utiliser votre propre nom d'utilisateur et un mot de passe approprié.

Lorsque vous êtes entré dans les écrans de configuration, il y a plusieurs réglages importants qui doivent être configurés.

Réglage sans fil	Quelle est sa fonction?	Comment le configurer
SSID	Nom du réseau ou SSID, qui correspond à « service set identifier »	Remplacez-le par quelque chose que vous reconnaîtrez mais qui ne permet pas de vous identifier. Par exemple, « Felsky » et «1 500 avenue Maple » ne sont pas des noms de réseau sûrs, car il s'agit de mon nom de famille et de l'adresse de mon domicile.
Diffusion du SSID	Lorsque le SSID est diffusé, n'importe qui disposant d'un appareil sans fil peut voir votre SSID parmi les réseaux disponibles. Ceci fait en sorte qu'il est facile pour un invité de se brancher sur le réseau, si vous lui donnez le mot de passe.	Désactiver la diffusion du SSID n'interrompt pas la diffusion du signal sans fil lui-même, de sorte que toute personne disposant d'un renifleur le moindrement sophistiqué détectera votre réseau quand même. La désactivation de la diffusion SSID permet quand même de tenir à l'écart les voisins moins bien équipés.
Obtenir un DNS automatiquement ou manuellement	Votre routeur peut être configuré pour attribuer automatiquement des adresses IP uniques à chaque appareil sur votre réseau sans fil, selon les besoins (dynamique); vous pouvez aussi attribuer manuellement une adresse IP à chaque appareil (statique).	En théorie, l'attribution manuelle rend l'accès à votre réseau sans fil plus difficile pour un inconnu, parce que celui-ci n'attribuera pas automatiquement une adresse IP à son appareil. Une personne informée peut cependant contourner facilement cette restriction, et l'attribution manuelle des adresses IP peut être une corvée.
Mode de sécurité WEP WPA2	WPA signifie *Wi-Fi Protected Access* et constitue un mode de chiffrement.	Choisissez WPA2 avec chiffrement AES (n'utilisez jamais l'ancien protocole WEP, facilement brisé). Choisissez un mot de passe

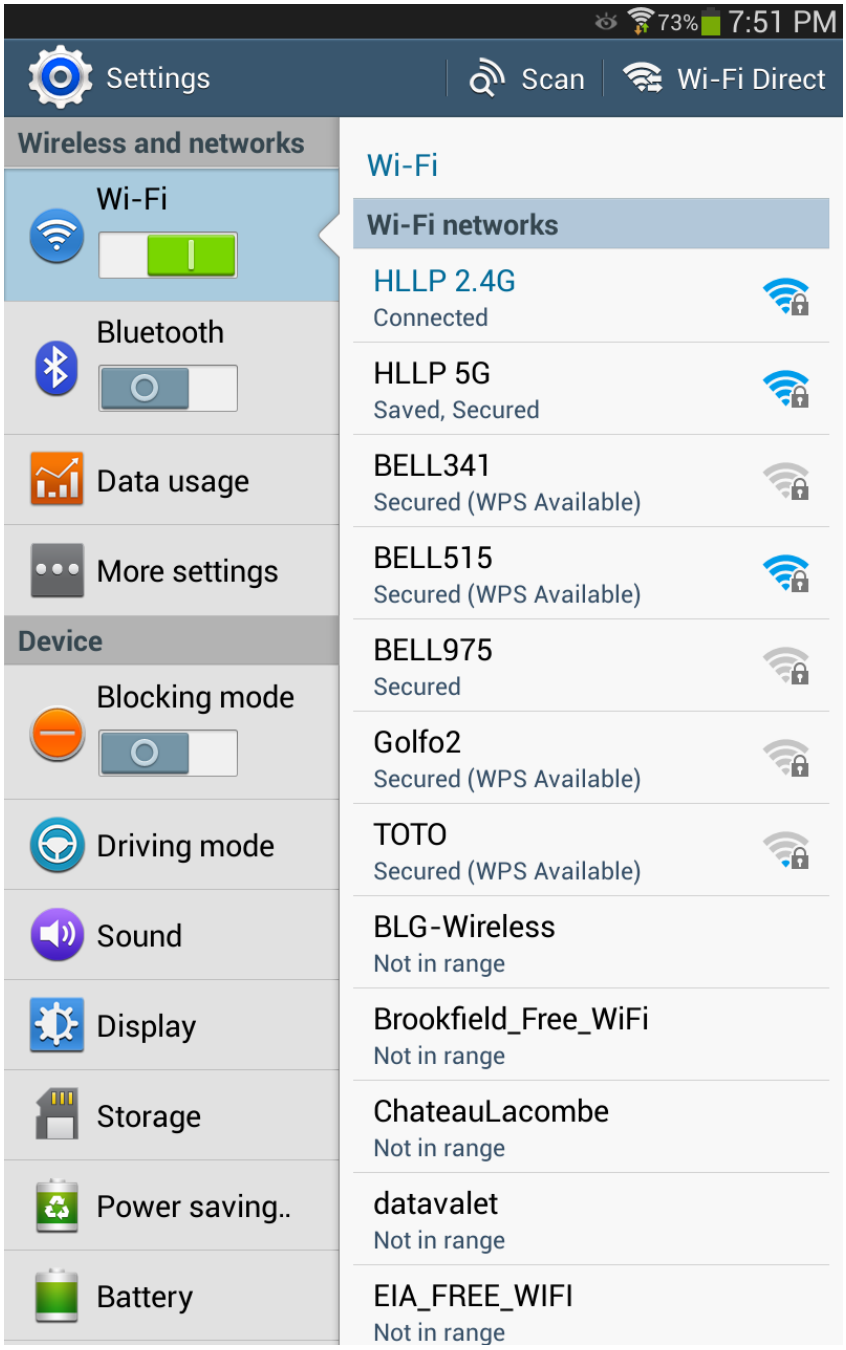
		long, complexe et aléatoire pour protéger le réseau.
Bouton de mode d'enregistrement (WPS)	WPS signifie *Wi-Fi protected Access*. Ce protocole permet aux appareils mobiles d'accéder au réseau en appuyant sur un bouton sur votre routeur plutôt qu'en procédant à des réglages de configuration au moyen de votre navigateur.	Il s'agit d'un outil commode, mais certains experts suggèrent de le désactiver, parce qu'il est vulnérable à certains types d'attaques.
Réglage visiteur	Certains routeurs vous permettent d'établir plus d'un réseau sans fil, par exemple un réseau pour les personnes qui travaillent de la maison et un réseau pour les visiteurs.	C'est une bonne idée de créer un réseau pour les visiteurs, avec accès Internet seulement, tandis que votre propre réseau peut comprendre les imprimantes partagées et le téléchargement progressif (*streaming*) en plus de l'accès Internet.
Chronomètre pour accès visiteur (Temps limité ou illimité)	Il est souvent possible de fixer une limite de temps à l'accès Internet pour les visiteurs, mais surtout si vous avez établi un réseau distinct pour les visiteurs, il n'y a rien à gagner.	0 = illimité
Filtrage MAC Activer ou désactiver	Chaque appareil pouvant être mis en réseau possède un identificateur unique (Media Access Control) intégré dans le matériel. C'est différent de l'adresse IP, qui est attribuée et qui peut facilement être changée par l'administrateur du réseau. Activer le filtrage MAC permet de restreindre l'accès à votre réseau aux appareils que vous avez vous-même approuvés.	En théorie, cela semble être une mesure intéressante, et cela peut éloigner les amateurs. Mais il est fastidieux de saisir et de tenir à jour la liste des adresses MAC pour vous et les visiteurs, et toute personne raisonnablement versée dans l'utilisation d'un réseau sans fil peut contrefaire une adresse MAC et obtenir quand même l'accès au réseau.

Mon réseau à domicile (HLLP2.4G) et mon réseau visiteurs (HLLP5G) figurent en premier dans la liste des réseaux ci-dessous accessibles dans mon voisinage et visible sur ma tablette numérique Samsung[2]. Vous pouvez voir que le réseau « Bell515 » émet un

[2] L'endroit où vous placez votre routeur importe sur le plan de la sécurité. Si vous le placez près d'un mur extérieur, il est plus facile pour les voisins de capter un signal fort. Si vous placez votre routeur à un endroit plus central dans votre domicile, le signal sera plus faible et moins facile à capter de l'extérieur.

signal relativement fort et qu'il y a d'autres réseaux Bell numérotés dans le voisinage (marqués « sécurisés »).

Toute personne qui utilise un appareil sans fil ou un programme renifleur peut voir cette liste de réseaux sans fil accessibles et, à l'aide de technologies faciles à obtenir, elle peut a) utiliser mon compte Internet pour naviguer sur le Web, peut-être pour envoyer du pourriel, et b) voir tout document non chiffré que je reçois ou que je transmets au moyen de mon ordinateur.



Recherche de réseaux accessibles – bande SSID

Sommaire des meilleures pratiques

1. Placez votre routeur à un endroit central pour éviter les fuites de signal.
2. Modifiez le nom de réseau par défaut (SSID) et évitez les noms qui permettent de vous reconnaître.
3. Désactivez la fonction « Diffusion SSID » pour que d'autres personnes ne puissent pas voir le nom de votre réseau (sachez qu'il est quand même possible de détecter un réseau même si son nom n'est pas diffusé).
4. Utilisez seulement un réseau privé virtuel judiciaire pour accéder aux fichiers d'un réseau judiciaire.
5. Si vous n'utilisez pas un réseau privé virtuel, utilisez seulement des sites Web protégés (par exemple, ceux dont l'adresse débute par https://...).
6. Si vous n'utilisez pas un réseau privé virtuel (RPV), assurez-vous que les services que vous utilisez sont protégés (par exemple, JUDICOM est protégé, tandis que Yahoo Mail ne l'est pas).
7. Utilisez les clés de sécurité les plus récentes, comme WPA2 (n'utilisez pas la clé de sécurité WEP).
8. Entrez un mot de passe d'administrateur sûr pour la gestion de votre routeur.
9. Désactivez la fonction DHCP et attribuez une adresse IP statique à chaque ordinateur relié à votre réseau sans fil à domicile.
10. Activez le pare-feu de chaque ordinateur relié à votre réseau et celui du routeur lui-même.
11. Débranchez votre routeur si vous vous absentez de votre domicile pendant une longue période.
12. Configurez un réseau sans fil distinct pour les visiteurs, avec accès limité.
13. Gardez votre système d'exploitation à jour et installez tous les correctifs de sécurité recommandés.

Pour voir une vidéo instructive, allez à http://www.youtube.com/watch?v=A88XB7_Jz7s

Annexe : Guides d'utilisation des réseaux sans fil à domicile
Bien que les concepts généraux soient les mêmes pour la plupart des connexions Internet sans fil, la présentation peut varier selon l'endroit où vous êtes et le fournisseur de services Internet que vous utilisez. Pour vérifier la sécurité de votre connexion, communiquez avec le service à la clientèle de votre fournisseur de services Internet.

Voici une liste de guides d'utilisation qui peuvent être utiles pour créer un réseau sans fil à domicile.

Cogeco	http://www.cogeco.ca/web/resources/pdf/support/user_guides/Internet/self_install_fr.pdf http://www.cogeco.ca/web/resources/pdf/support/user_guides/Internet/Cisco%20DPC%203825.pdf
Rogers	http://downloads.rogershelp.com/UG/RogersHomeNetworkingUG.pdf http://www.rogers.com/web/support/Internet/wireless-network/128?setLanguage=fr
Bell	http://Internet.bell.ca/img_gallery/2701_UserGuide_2wire_fr.pdf http://soutien.bell.ca/Services-Internet/Aide-connexion/Point-de-connexion.comment_modifier_les_reglages_wifi_sur_mon_modem
Telus	http://www.telus.com/content/help/Internet-support/wireless-home-networking.jsp
Bell Aliant	http://www.bellaliant.net/ naviguer à *Soutien* et naviguer à *Internet* et ensuite naviguer à *Internet sans fil*.
Shaw	https://community.shaw.ca/docs/DOC-1564