# La sécurité des réseaux sans fil à domicile

*par Martin Felsky*
*Novembre 2009*

## Table des matières



## Introduction

Dans le *Plan d'action en matière de sécurité des renseignements judiciaires*[1], les « renseignements judiciaires » sont définis comme « des renseignements qui sont recueillis, produits ou utilisés à des fins judiciaires » (sauf quelques exceptions). Les juges qui rédigent des projets de jugement ou qui communiquent avec leurs collègues à propos d'affaires judiciaires produisent et transmettent des « renseignements judiciaires ». Dans tous les cas, les mêmes mesures que les administrations judiciaires appliquent pour protéger ces renseignements devraient également être appliquées à domicile.

De nombreux juges doutent de la sécurité des réseaux sans fil à domicile, mais ils n'ont pas les connaissances techniques voulues pour configurer convenablement les paramètres de sécurité de ces réseaux. La documentation qui accompagne l'équipement de réseautique sans fil à domicile est souvent incomplète, impossible à comprendre, ou même trompeuse.

Au bout du compte, si vous n'avez pas le matériel et le logiciel nécessaires, et si ceux-ci ne sont pas configurés et utilisés convenablement, tous les renseignements que vous recevez et transmettez au moyen de votre ordinateur et toutes les données qui y sont stockées sont vulnérables.

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

[1] Voir le *Plan d'action du Conseil canadien de la magistrature en matière de sécurité des renseignements judiciaires*, Troisième édition, 2009.

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://).

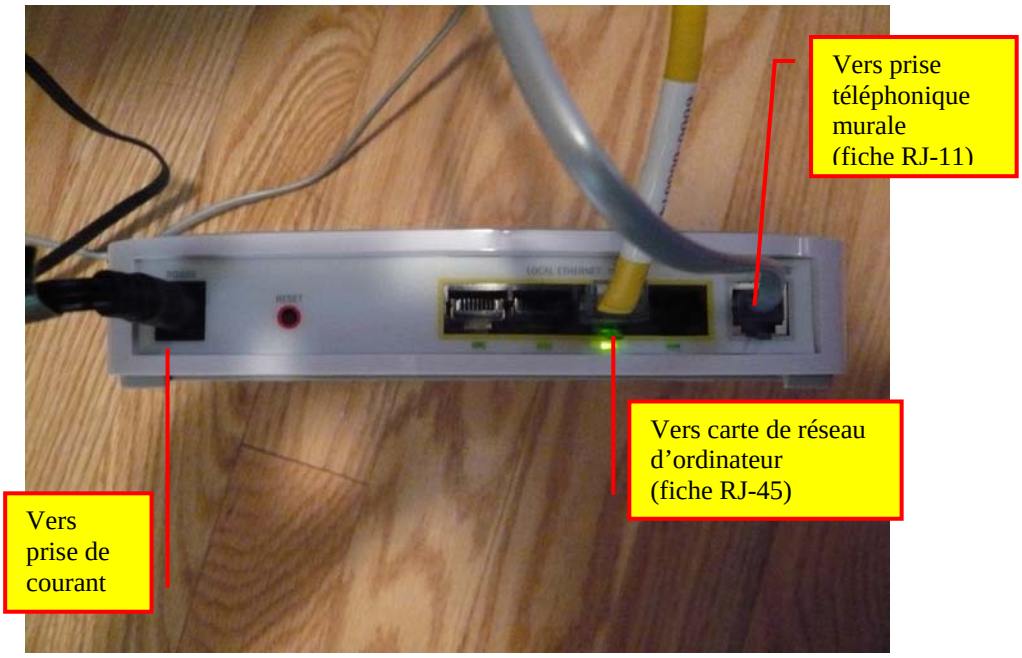
## L'installation de votre réseau sans fil à domicile

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. À titre d'exemple, je vais décrire mon propre réseau sans fil à domicile, qui est relié à ma ligne téléphonique Bell, et je vais vous montrer les paramètres par défaut du fabricant, dont la plupart offrent très peu de protection.

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, modem câble ou modem DSL.

**Passerelle Internet Bell (vue de face)**

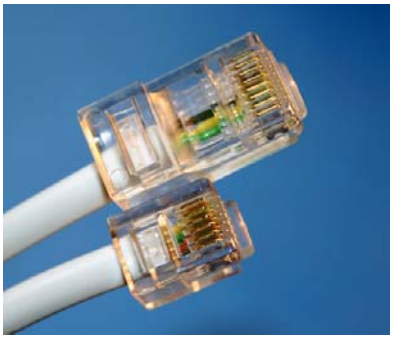
Votre routeur se branche dans la prise de téléphone ou de câble murale (à cet égard, il ne fonctionne pas « sans fil »). Après avoir branché le routeur à la prise murale, vous devez brancher votre ordinateur au routeur. Il y a deux façons de le faire : au moyen d'un câble de réseau (branché) ou d'une connexion sans fil. Pour pouvoir communiquer sans fil avec le routeur, votre ordinateur doit être muni d'une carte de réseau sans fil interne ou externe. Voir les illustrations suivantes :




**Routeur sans fil muni de quatre ports réseau (vue arrière)**

**Carte de réseau sans fil interne (s'insère dans l'ordinateur)**

La sortie à l'extrême droite sert à brancher le routeur à une prise téléphonique murale au moyen d'un câble téléphonique ordinaire (sans filtre). Le câble jaune est un câble de réseau local qui relie le routeur à la carte de réseau de l'ordinateur. La fiche RJ-45 à l'extrémité du câble de réseau local ressemble à celle d'un câble de téléphone, mais elle est un plus grande :



**La fiche RJ-45 (de réseau) est plus grande que la fiche RJ-11 (de téléphone)**

Étant donné que mon ordinateur de bureau est branché à mon routeur, je n'utilise pas vraiment une connexion sans fil, même si mon routeur fonctionne « sans fil ». Cependant, le routeur émet un signal que je peux capter n'importe où à l'intérieur ou à proximité de mon domicile, au moyen de mes appareils de réseau sans fil, comme mon ordinateur portatif, qui est muni d'une carte de réseau sans fil, ainsi que mon appareil mobile de poche Blackberry, qui me permet également de me connecter à Internet sans fil (en plus de me donner accès au réseau de téléphone cellulaire).

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.

**Note :** Les écrans illustrés ci-après montrent comment créer un réseau sans fil en se servant d'un ordinateur fonctionnant en Windows XP et en ayant recours à Bell comme fournisseur de services Internet. Vous trouverez à l'annexe de ce document des renseignements sur d'autres options.


**La création d'un réseau sans fil**

Comme le montre l'écran illustré ci-dessus, l'Assistant de configuration de réseau de Windows XP vous aidera à créer un réseau sans fil à domicile. Si vous utilisez un différent système d'exploitation, consultez le guide d'emploi de ce système ou demandez l'aide d'un spécialiste en informatique qualifié.

La première étape pour protéger votre réseau sans fil à domicile consiste à changer le nom de réseau par défaut, c'est-à-dire le SSID (***S**ervice **S**et **Id**entifier*). Remplacez-le par quelque chose 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.


**Le nom de réseau**

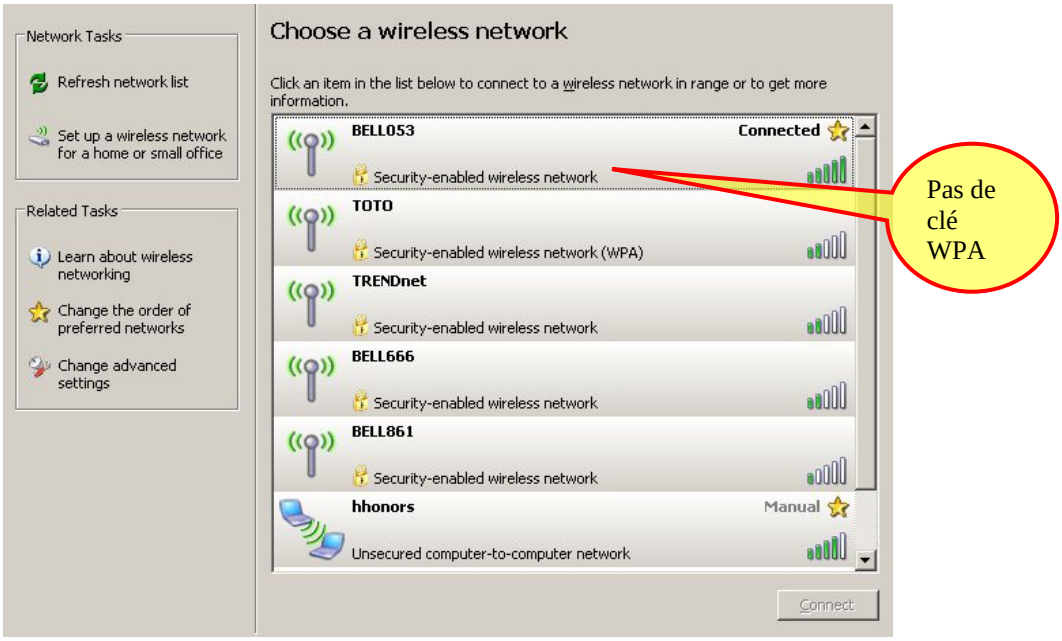
À l'écran illustré ci-haut, vous pouvez également choisir « Utiliser la clé de sécurité WPA … » (***W**i-Fi **P**rotected **A**ccess*). Même si une mise à niveau est nécessaire (par exemple, si vous avez un vieil ordinateur muni d'une carte de réseau sans fil interne qui n'accepte pas la clé de sécurité WPA), vous devez choisir WPA[2] et ne pas utiliser la clé de sécurité WEP[3] (ou, pire encore, n'utiliser aucune une clé de sécurité). À titre d'exemple, à l'écran illustré ci-haut, j'ai gardé le nom de réseau par défaut (« Bell053 ») et je *n'ai pas* choisi la clé de sécurité WPA.

Mon réseau figure en tête d'une liste de réseaux (voir l'écran illustré ci-dessous) accessibles dans mon quartier.[4] On voit que le signal émis par le réseau « Toto » est assez fort. Mon voisin a un chien qui s'appelle Toto, donc je suis pas mal certain que ce réseau est le sien. Comme on peut le voir, son réseau est protégé par la clé de sécurité WPA. On voit également que d'autres voisins qui utilisent Bell Internet – Bell666 et Bell861 – n'ont pas changé leur nom de réseau par défaut et qu'ils n'utilisent pas la clé de sécurité WPA, ce qui font d'eux une cible facile pour les intrus.

Ainsi, toute personne qui utilise un appareil sans fil ou un programme renifleur peut voir cette liste de réseaux sans fil accessibles (il y a des gens qui parcourent les quartiers à la

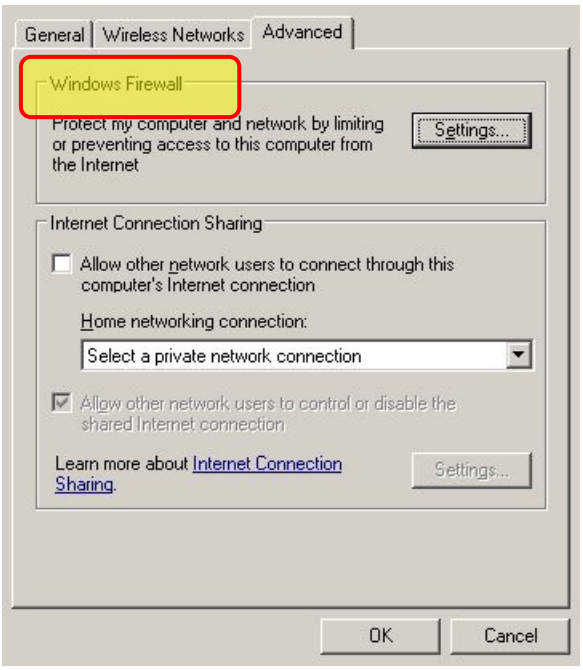
[2] Un article paru en août 2009 a révélé que la clé de sécurité WPA peut être déchiffrée en une minute – mais seulement à l'aide d'outils très perfectionnés. Voir http://tech.yahoo.com/blogs/null/147906.
[3] La clé de sécurité WEP (***W**ired **E**quivalent **P**rivacy*) a été conçue à l'origine pour offrir un niveau de protection comparable à celui d'un réseau câblé. Elle est facile à déchiffrer.
[4] 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.

recherche de réseaux sans fil non protégés) et, à l'aide de technologies faciles à obtenir, elle peut a) utiliser mon réseau sans fil pour naviguer dans Internet, 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.



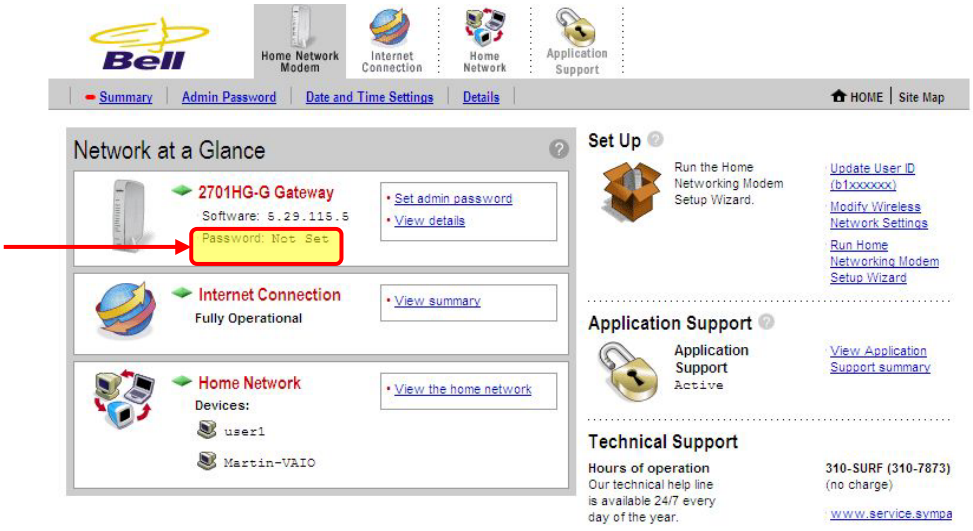

**Liste de réseaux sans fil accessibles**

Vous pouvez configurer votre système d'exploitation pour aider à empêcher des personnes non autorisées d'utiliser votre réseau sans fil pour obtenir accès à votre ordinateur. Par exemple, Windows a un pare-feu intégré qui peut être configuré de manière à désactiver la fonction de partage de la connexion sur chaque ordinateur du réseau domiciliaire (voir l'écran illustré ci-dessous) :




**Les paramètres du pare-feu intégré de Windows**

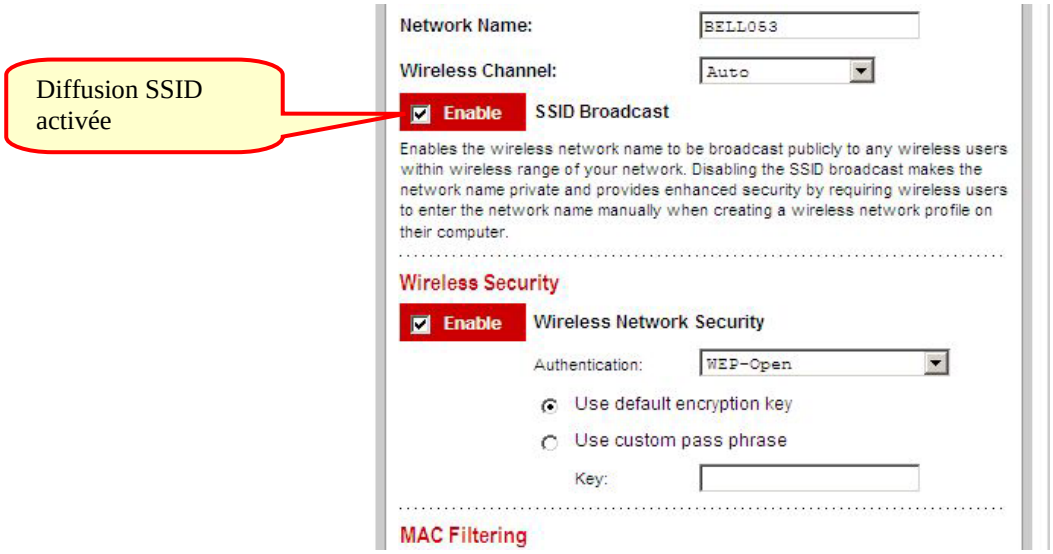
Une fois que votre routeur est installé et que votre connexion Internet est établie, vous pouvez utiliser le logiciel qui accompagne le routeur pour le sécuriser et le protéger à l'aide d'un pare-feu. L'illustration ci-dessous montre l'écran d'accueil de mon routeur sans fil. À titre d'exemple, on peut voir que je n'ai *pas entré un mot de passe d'administrateur*, ce qui veut dire que toute personne qui obtient accès à mon réseau pourrait facilement modifier tous les paramètres du routeur et m'interdire l'accès au réseau. *Il est important d'entrer un mot de passe d'administrateur sûr pour protéger les paramètres de votre réseau.*




**MAUVAISE PRATIQUE : Aucun mot de passe d'administrateur**

À l'écran illustré ci-dessous, on voit que la fonction « Diffusion SSID » est activée, ce qui veut dire que vos voisins peuvent voir votre nom de réseau parmi la liste des réseaux

accessibles. Cela accroît le risque d'intrusion dans votre réseau. Si la fonction « Diffusion SSID » n'est pas activée, votre nom de réseau ne s'affichera pas sur la liste des réseaux accessibles :

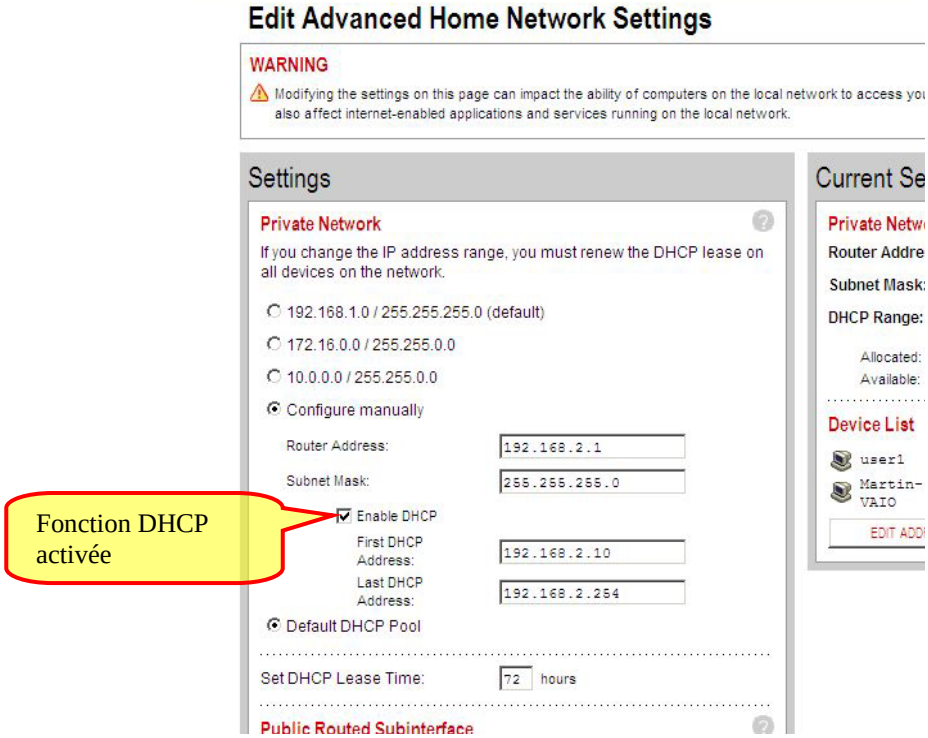



**Fonction « Diffusion SSID » activée**

## Les adresses IP dynamiques

Pour pouvoir partager les ressources du réseau (comme le routeur, une imprimante ou des fichiers partagés), chaque ordinateur relié à votre réseau à domicile doit avoir sa propre adresse IP (***I**nternet **P**rotocol*), tout comme un site Web. Votre routeur a sa propre adresse IP. Au moyen d'une fonction appelée DHCP (***D**ynamic **H**ost **C**onfiguration **P**rotocol*), une adresse IP peut être attribuée automatiquement à tous les appareils reliés à votre réseau à domicile, ce qui est très pratique.

Chaque fois qu'un ordinateur se connecte à votre réseau à domicile, la fonction DHCP lui attribue automatiquement une adresse IP. Il est donc facile pour un intrus d'obtenir une adresse IP valide pour accéder à votre réseau. Par conséquent, il est préférable d'attribuer manuellement une adresse IP à chaque ordinateur relié à votre réseau. À l'écran illustré ci-dessous, la fonction DHCP est activée par défaut.




Fonction DHCP activée

## 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).
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. Choisissez un nom de réseau qui n'a aucun rapport avec vous, votre famille ou votre domicile.
5. Utilisez seulement un réseau privé virtuel judiciaire pour accéder aux fichiers d'un réseau judiciaire.
6. Si vous n'utilisez pas un réseau privé virtuel, utilisez seulement des sites Web protégés (par exemple, ceux dont l'adresse débute par https://...).
7. Si vous n'utilisez pas un réseau privé virtuel, assurez-vous que les services que vous utilisez sont protégés (par exemple, JUDICOM est protégé, tandis que Yahoo Mail ne l'est pas).
8. Utilisez les clés de sécurité les plus récentes (n'utilisez pas la clé de sécurité WEP).
9. Entrez un mot de passe d'administrateur sûr pour configurer votre routeur.
10. Désactivez la fonction DHCP et attribuez une adresse IP statique à chaque ordinateur relié à votre réseau sans fil à domicile.
11. Activez le pare-feu de chaque ordinateur relié à votre réseau et celui du routeur lui-même.
12. Débranchez votre routeur si vous vous absentez de votre domicile pendant une longue période.
13. Désactivez la fonction de partage des services, des répertoires et des fichers de votre ordinateur – cette fonction est généralement activée par défaut (au besoin, demandez de l'aide).
14. 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.broadbandreports.com/faq/wifisecurity |
| Rogers | http://downloads.rogershelp.com/UG/RogersHomeNetworkingUG.pdf |
| Bell | http://internet.bell.ca/img_gallery/2701_UserGuide_2wire_FR.pdf |
| Telus | http://www.telus.com/portalWeb/inlineLink/CP_SCS/Help/Internet_Help/High_Speed/Step_by_Step_Description/Wireless_Networking_Installation_additional/Windows_2000/?_region=AB |
| Bell Aliant | http://nsegainkc1.aliant.net/knowledge/Docs/Internet/Conn/6520/EnableWireless/EnableWireless.htm |
| Shaw | http://start.shaw.ca/Start/enCA/Customer+Service+Centre/Internet+Safety/SecuringWireless.htm |