

La sécurité des réseaux sans fil sur la route

par Martin Felsky
Novembre 2009

Table des matières

Introduction.....	1
L'accès à Internet sans fil sur la route	2
Quels réseaux sans fil sont légitimes et lesquels sont des pièges?	4
En supposant que vous utilisez un point d'accès à Internet sans fil légitime, est-il bien protégé?.....	5
Sommaire des meilleures pratiques	5

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 lorsque vous voyagez.

Cet article traite de la sécurité des réseaux sans fil de manière pratique et en langage clair. Les mesures faciles, gratuites et sensées qui y sont décrites assureront à vos communications sans fil une protection raisonnable contre les intrusions. Sachez, cependant, que même si vous suivez toutes les meilleures pratiques recommandées, vos activités de navigation dans Internet et le contenu de vos courriels ne seront *jamais* parfaitement protégés. Pour cette raison, toutes les données confidentielles devraient être chiffrées lorsqu'elles sont transmises, ce qui exige l'utilisation d'un réseau privé virtuel.

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

L'accès à Internet sans fil sur la route

De nombreux juges doutent de la sécurité des réseaux sans fil, mais ils n'ont pas les connaissances techniques voulues pour pouvoir s'en assurer. Les points d'accès à Internet sans fil qu'on trouve dans les aéroports, les hôtels et les cafés offrent peu ou point d'information sur la sécurité.

Une connexion sans fil non protégée peut être interceptée à l'aide d'outils spécialisés, même si les paramètres de sécurité du réseau sont relativement bien configurés. Une grande partie du contenu des communications entre votre appareil et Internet – y compris le courriel – est transmis en texte clair et peut être intercepté, lu et saisi.

Une façon plus sûre de se connecter à Internet au moyen d'un ordinateur portatif est d'utiliser un modem cellulaire, comme la clé Internet sans fil de Rogers² ou le modem sans fil USB de Bell. Le réseau téléphonique cellulaire est relativement sûr (bien qu'il ne soit pas invulnérable) comparativement aux points d'accès à Internet sans fil. Cependant, même la sécurité des appareils cellulaires n'est pas parfaite. Par exemple, lorsque vous vous connectez à Internet au moyen d'un modem sans fil ou d'un appareil mobile de poche relié au réseau cellulaire, la connexion au réseau s'établit par la voie d'un processus d'authentification.

Selon les experts, il est possible pour un malfaiteur de se faire passer pour un fournisseur de services Internet. De plus, les appareils mobiles reliés au réseau téléphonique cellulaire sont exposés aux risques habituels que posent les virus informatiques et les logiciels espions. Sachez que certains appareils mobiles, comme le Blackberry, peuvent se connecter à Internet au moyen du réseau téléphonique cellulaire ou d'un réseau sans fil. Il y a donc autant de risque à utiliser un appareil mobile de poche Blackberry ou un téléphone cellulaire pour se connecter à Internet que de se servir d'un ordinateur portatif, à moins de choisir un réseau sans fil protégé.



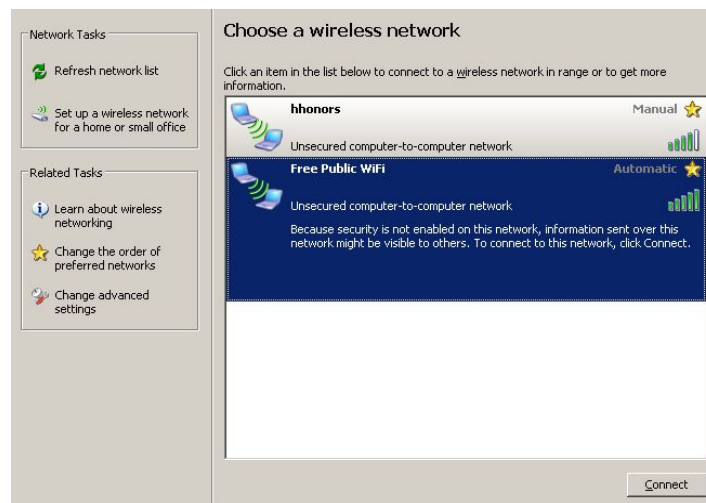
La clé Internet sans fil de Rogers

² Le site Web de Rogers contient très peu d'information sur la sécurité de la clé Internet sans fil.

Il y a deux points essentiels à retenir lorsque vous utilisez un point d'accès sans fil à Internet public :

1. dans de nombreux lieux publics, votre appareil mobile détectera plusieurs réseaux sans fil accessibles (voir l'écran illustré ci-dessous). La première question qui se pose est de savoir quels réseaux sans fil sont légitimes et lesquels sont des pièges;
2. en supposant que vous utilisez bel et bien un point d'accès à Internet sans fil légitime, il faut savoir s'il est bien protégé.

Note : La liste des réseaux sans fil accessibles peut avoir l'air différente, selon le système d'exploitation de votre ordinateur. Les deux illustrations ci-dessous montrent la liste qui s'affiche selon que vous utilisez Windows ou Mac.



Liste des réseaux sans fil accessibles (Windows)



Liste des réseaux sans fil accessibles (Mac)

Quels réseaux sans fil accessibles sont légitimes et lesquels sont des pièges?

Toute personne qui a une connexion à Internet et un routeur sans fil peut créer un réseau sans fil et lui donner n'importe quel nom, par exemple « Point d'accès à Internet sans fil gratuit » ou « Point d'accès à Internet de l'hôtel Marriott ». Par analogie, imaginez que vous déposez un projet de jugement dans une boîte à lettres qui ressemble en tous points à celles de Postes Canada, mais qu'il s'agit en fait d'une fausse boîte placée par un malfaiteur qui vole le courrier. Ou encore, imaginez qu'un messenger portant l'uniforme de FedEx se présente au palais de justice et prend livraison de tous les envois, mais que cette personne est en fait un imposteur. Les réseaux-pièges peuvent ne comporter aucune mesure de sécurité, ce qui veut dire qu'on peut s'y connecter très facilement et gratuitement. Lorsque votre ordinateur portable ou votre appareil mobile de poche détecte les réseaux sans fil accessibles, il peut être très tentant de se connecter à de tels réseaux puissants, gratuits et apparemment légitimes.

Le problème est que si ce réseau sans fil d'accès facile a été créé par un malfaiteur, tous vos renseignements – y compris vos mots de passe, votre courriel et votre historique de navigation dans Internet – lui sont accessibles en forme lisible, à moins que vous utilisiez un réseau privé virtuel qui chiffre toutes les données.

De nombreux hôtels ont recours à des fournisseurs de services Internet externes. Il peut y avoir plusieurs réseaux sans fil accessibles dans votre chambre d'hôtel. Il est important de consulter la documentation de l'hôtel sur les services Internet ou, si vous n'en trouvez pas, il suffit d'appeler la réception pour connaître le nom de réseau exact (SSID) du fournisseur de services Internet légitime de l'hôtel.

Il n'est pas toujours possible de savoir si un réseau sans fil est légitime ou non. Je pourrais créer moi-même un réseau sans fil dans un aéroport et lui donner le même nom que la compagnie qui fournit des services Internet dans les salons Feuille d'érable d'Air Canada, soit « Datavalet ».

Selon une étude menée en 2008 par *AirTight Networks*³, 77 % des réseaux sans fil accessibles dans vingt-sept aéroports des États-Unis, de l'Europe et de l'Asie n'étaient pas des points d'accès à Internet sans fil « officiels ».

³ D'après un reportage de Steven Kotler, intitulé *Wireless Cybercriminals Target Clueless Vacationers*, présenté au réseau *Fox News* le dimanche 12 juillet 2008.

En supposant que vous utilisez un point d'accès à Internet sans fil légitime, est-il bien protégé?

Selon l'étude réalisée par *AirTight Networks*, 97 % des utilisateurs étaient connectés à des réseaux sans fil non protégés. De plus, 80 % des réseaux *protégés* utilisaient la clé de sécurité WEP peu sûre. Cela signifie que même lorsque vous êtes connecté à un réseau commercial ou public légitime, la sécurité de ce réseau dépend du matériel, du logiciel, de la configuration et des politiques et procédures du fournisseur. Par exemple, il se peut que le fournisseur :

- n'utilise pas la technologie de chiffrement la plus récente;
- n'utilise pas le matériel informatique offrant la meilleure protection en matière de sécurité;
- ne vérifie pas les antécédents du personnel qui a accès aux comptes des clients;
- ne surveille pas son réseau suffisamment pour détecter les intrusions.

Les politiques et procédures des fournisseurs de points d'accès à Internet sans fil devraient être beaucoup plus transparentes. Par exemple, le site Web de Datavalet, une entreprise hautement respectée, ne contient pas le moindre renseignement sur les mesures employées pour assurer la sécurité des clients des services sans fil.

Sommaire des meilleures pratiques

1. Désactivez la fonction de connexion automatique à des réseaux accessibles.
2. Désactivez le mode de « dépistage » de Bluetooth, ou désactivez la fonction Bluetooth de votre appareil si vous ne l'utilisez pas.
3. Dans un hôtel, consultez la documentation sur les services Internet ou appelez la réception pour connaître le nom du réseau sans fil légitime de l'hôtel.
4. Utilisez seulement un réseau privé virtuel judiciaire pour obtenir accès aux données 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, assurez-vous que les services que vous utilisez sont protégés (par exemple, JUDICOM est protégé, tandis que Yahoo Mail ne l'est pas).
7. Désactivez la fonction de partage des services, des répertoires et des fichiers de votre ordinateur – cette fonction est généralement activée par défaut (au besoin, demandez de l'aide).
8. Utilisez un logiciel de pare-feu personnel.
9. 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=6uR0VkWUXrI>.