La sécurité des réseaux sans fil sur la route

par Martin Felsky
Deuxième édition, 17 janvier 2014

Table des matières

Introduction

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 doivent 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 mobiles une protection raisonnable contre les intrusions. Sachez cependant que même si vous suivez toutes les meilleures pratiques recommandées, vos activités de navigation sur Internet et le contenu de vos courriels ne seront jamais parfaitement protégés. Pour cette raison, toutes les données confidentielles doivent être chiffrées lorsqu'elles sont transmises, ce qui exige l'utilisation d'un réseau privé virtuel (RPV) ou chiffrement SSL.

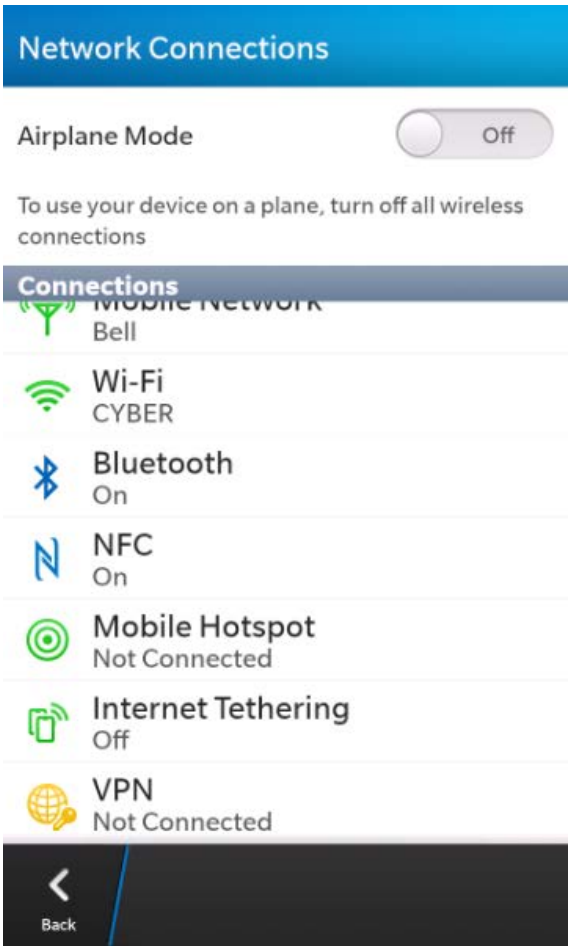
L'accès à Internet sans fil sur la route

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 cafés, les hôtels et les centres de conférences offrent peu ou point d'information sur la sécurité.

Une connexion sans fil non protégée peut être interceptée à l'aide d'outils appropriés, même si les paramètres de sécurité du réseau sont relativement bien configurés. La plus

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. De plus, vous pourriez vous-même, par inadvertance, configurer votre appareil mobile en point d'accès, auquel un étranger pourrait alors se brancher.

Une façon plus sûre de se connecter à Internet consiste à éviter le Wi- Fi complètement et à utiliser un modem cellulaire ou à relier votre ordinateur portable à un appareil cellulaire (par Bluetooth) en utilisant les réglages réseaux de l'appareil. L'écran ci-dessous montre les réglages Blackberry, y compris « mobile Hotspot », qui vous permet de créer votre propre point d'accès pour plusieurs appareils, et « Internet Tethering », qui vous permet de relier un appareil (comme un ordinateur portable) au Blackberry pour obtenir un accès Internet. L'utilisation de l'un ou l'autre de ces services doit se faire avec soin pour éviter les accès non autorisés, et vous devez les mettre hors circuit lorsque vous avez terminé de vous en servir.



En comparaison des points d'accès Wi-Fi, le réseau de téléphonie mobile est plus sûr, mais n'est pas imperméable aux attaques.

La navigation Web sur téléphone mobile est aussi exposée aux risques habituels que posent les virus et les logiciels espions. Sachez que plusieurs téléphones intelligents et

tablettes électroniques 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 pour se connecter à Internet que de se servir d'un ordinateur portatif, à moins de choisir une connexion réseau appropriée.

Il y a deux points essentiels à retenir lorsque vous utilisez un point d'accès sans fil à Internet public, et plus particulièrement dans le cas des points d'accès gratuits :

1. quels points d'accès Wi-Fi sont légitimes, et lesquels sont des pièges;
2. en supposant que vous utilisez vraiment un point d'accès légitime, est-il bien protégé?

Quels points d'accès Wi-Fi sont légitimes et lesquels sont des pièges?

Toute personne qui a une connexion à Internet et un appareil mobile peut créer un point d'accès Wi-Fi (voir ci-dessus) et lui donner n'importe quel nom, par exemple « Point d'accès Wi-Fi gratuit » ou « Point d'accès à Internet de l'hôtel Marriott ». Par analogie, imaginez que vous déposez un projet de jugement dans une boîte aux 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 ouvre le courrier. Ou encore, imaginez qu'un messager portant l'uniforme de FedEx se présente au palais de justice et prend livraison de tous vos envois urgents, 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. En fait, si votre appareil mobile est configuré pour se connecter automatiquement aux réseaux disponibles, vous pourriez être branché sur un réseau malfaisant sans même le savoir.

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.

Dans de nombreux hôtels et centre de conférences, le fournisseur de services Internet officiel ne porte pas le même nom que l'établissement. Plusieurs signaux peuvent être disponibles dans votre chambre. 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.

Selon une étude menée en 2008 par AirTight Networks[1], 77 p. 100 des réseaux sans fil accessibles dans 27 aéroports des États-Unis, de l'Europe et de l'Asie n'étaient pas des points d'accès à Internet sans fil « officiels ».

[1] 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 vraiment un point d'accès légitime, est-il bien protégé?

Selon l'étude réalisée par AirTight Networks, 97 p. 100 des utilisateurs étaient connectés à des réseaux sans fil non protégés. De plus, 80 p. 100 des réseaux protégés utilisaient la clé de sécurité WEP peu sûre (en 2008). 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 efficacement pour détecter les intrusions.

Sommaire des meilleures pratiques

1. Utilisez le réseau cellulaire intégré à votre appareil et mettez le Wi-Fi hors fonction en l'absence d'un point d'accès sécurisé.
2. Dans les réglages de votre appareil mobile, désactivez la connexion automatique aux réseaux ouverts lorsque vous vous déplacez.
3. Désactivez le mode de « dépistage » de Bluetooth, ou désactivez la fonction Bluetooth de votre appareil si vous ne l'utilisez pas pour un clavier, un casque d'écoute ou le mode modem.
4. Dans un hôtel, consultez la documentation sur les services Internet ou appelez la réception ou le centre de conférences pour connaître le nom du réseau sans fil légitime de l'hôtel
5. Utilisez uniquement une connexion RPV fournie par la cour pour accéder aux données d'un réseau judiciaire.
6. Si vous n'utilisez pas un RPV, utilisez seulement des sites Web protégés (par exemple, ceux dont l'adresse débute par https://...) (plusieurs sites web sont accessibles des deux façons).
7. Si vous n'utilisez pas un RPV, assurez-vous que les services que vous utilisez sont protégés (par exemple, JUDICOM est protégé, tandis que Yahoo Mail ne l'est pas).
8. Désactivez la fonction de partage des services, des répertoires et des fichiers de votre ordinateur – cette fonction est généralement activée par défaut (demandez de l'aide).
9. Utilisez un logiciel de pare-feu personnel et configurez-le (vous pourriez avoir besoin d'aide pour ce faire).
10. 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