Sécuriser votre connexion Internet, c'est comme sécuriser votre maison.

Rien de ce que vous choisirez de faire ne pourra être à 100% fiable. Tout ce que vous pouvez faire c'est prendre les précautions raisonnables qui décourageront les intrus potentiels et faire en sorte de vous mettre en conformité avec la Loi. Si vous installez des serrures de qualité et un système d'alarme, vous vous protégez de façon raisonnable. La sécurisation de votre connexion Internet sans fil (Wifi) repose sur les mêmes principes.

Désormais la Loi française vous oblige à sécuriser votre connexion Internet.
Les 7 points ci-dessous constituent un guide simple et facilement compréhensible pour vous équiper et vous mettre en conformité avec les nouvelles exigences de sécurité.

1. La nouvelle loi HADOPI-2 est maintenant entrée en application. Cette loi a été élaborée pour punir les personnes qui téléchargent du matériel sous Copyright illégalement. Cette loi a de nombreuses implications pour nous tous qui avons une connexion Internet en Wifi (sans fil) car HADOPI-2 a introduit un nouveau délit, dit de "Négligence". En effet , si quelqu'un devait utiliser votre connexion pour commettre des actes illégaux, vous seriez reconnu comme étant responsable aux yeux de la loi car vous devez sécuriser votre connexion Internet. Notez bien que votre connexion et votre système Wifi doivent être sécurisés. Voyez le point 4 ci-dessous pour découvrir comment procéder. Avec des amendes pouvant atteindre les 30 000 E, ceci n'est pas à prendre à la légère. Pour une personne mal-intentionnée, rien de plus facile que d'utiliser une connexion non-sécurisée car elle est sure de ne pas être retrouvée. Donc protégez-vous.

2. Comment sécuriser ma connexion Internet? Tout d'abord pensez à votre connexion en Wifi car c'est la plus vulnérable. Si votre connexion est ouverte, alors n'importe qui peut utiliser votre Internet pour commettre des actes illégaux et vous n'aurez aucune preuve contre eux. La solution c'est le cryptage Wifi avec mot de passe, basé sur l'utilisation d'un code de sécurité comme celui que vous utilisez à la banque ou sur votre alarme domestique. Vous suivez les instructions de votre fournisseur d'accès Internet, vous choisissez un mot de passe pour votre boîte Internet (routeur) et vous entrez ce mot de passe sur votre ordinateur. Si vous utilisez un fournisseur d'accès comme SFR ou Orange, votre boîte Internet arrive avec un mot de passe pré-sélectionné. Aprés cette opération votre Wifi est protégé.

3. Si cela est si simple pourquoi tant de bruit? La Protection de votre signal Wifi est juste la première partie de votre processus de sécurité. Les ennuis commencent lorsque vous partagez votre mot de passe avec une autre personne. Votre mot de passe est comme la clé de votre maison. Si vous la donnez ou si vous la prêtez à quelqu'un, vous n'avez plus de contrôle sur qui l'utilisera ou la copiera, ou même encore sur toute autre personne à qui elle pourrait être prêtée. Si vous savez comment procéder, vous pouvez changer votre mot de passe mais comme

changer une serrure, cela prend du temps et vous ne le ferez peut-être pas. Donc ne partagez votre mot de passe qu'avec des gens en qui vous avez entière confiance et assurez-vous qu'ils comprennent la nécessité de protéger ce mot de passe. Si vous avez besoin de partager votre connexion Wifi, la seule façon de vous protéger est d'utiliser un Hotspot Wifi.

4. Nous avons parlé de la sécurisation de notre connexion Internet pas seulement de notre Wifi. Il ne faut pas oublier que même si on protège sa connexion Wifi, il est toujours possible de se connecter directement sur la boîte Internet avec un cable à notre insu. Assurez vous donc que votre boîte Internet est dans un endroit sûr. Ceci est tout particulièrement important dans le cas de locations saisonnières ou non, et dans le cas de lieux ouverts au public tels que cafés, bars, hôtels.

5. Alors que faire quand on veut partager sa connexion avec ses hôtes ou ses clients?
Ceci pose un réel problème car partager votre mot de passe avec d'autres personnes ouvre une brèche dans votre système de sécurité. Le fait de donner votre mot de passe peut vous rendre passible de poursuites pour Négligence dans le cadre de la loi HADOPI-2. C'est pour cela qu'un Hotspot Wifi est indispensable. Un Hotspot Wifi permet de contrôler l'accès à Internet au moyen de l'utilisation de 2 identifiants: un nom d'utilisateur et un mot de passe. Ces 2 identifiants sont uniques et permettent la traçabilité de l'utilisateur. De même, ils permettent de limiter le temps de connexion, la vitesse de téléchargement et leur importance. Ceci est parfait pour surfer sur l'Internet mais idéal pour décourager les utilisateurs souhaitant faire des téléchargements de fichiers lourds, monopolisant ainsi votre connexion Internet. Les malfaiteurs ne souhaitent pas laisser de traces et sont donc très méfiants des Hotspot Wifi. **Nos Hotspot Wifi sont simples à installer, faciles à utiliser pour un coût très abordable.**
De plus, si vous décidez de rendre votre accès Internet payant, le système s'autofinancera très rapidement et génèrera un revenu complèmentaire.

6. Une 2ème loi est à prendre en considération quand vous partagez votre Internet:
Il s'agit de la loi "Anti-Terrorisme" qui exige que toute connexion ouverte au public soit équipée d'un journal de connections. Toutes les données en rapport avec l'utilisateur, son ordinateur, ses dates et heures de connexion... devront être conservées pendant un an et devront être fournies aux autorités en cas de nécessité. Nos Hotspot enregistrent toutes ces données et plus. Nous avons développé un système qui vous permet de les télécharger régulièrement sous forme de tableaux qui pourraient être soumis aux autorités si besoin était.

7. En résumé, si vous avez une connexion Internet privée, protégez votre Wifi à l'aide d'un mot de passe, mettez votre boîte Internet en lieu sûr, et ne partagez votre mot de passe qu'avec vos proches. **Si vous souhaitez partager votre connexion, utilisez un Hotspot Wifi qui donne des identifiants uniques à chaque utilisateur et garde un journal de connexions.**
En suivant ces recommandations, vous pouvez vous protéger raisonnablement d'actes illégaux commis par le biais de votre connexion Internet.

Pour toute information complémentaire contacter info@UBI-WIFI.com
www.UBI-WIFI.com
* J'ai lu et j'accepte les Termes & Conditions de Vente (ouvrir dans une nouvelle fenêtre)