

COMMENT SE PROTÉGER SUR DES RÉSEAUX Public OU Hotspots WiFi

Si vous devez utiliser la WiFi à l'aéroport ou à l'hôtel ? Tout d'abord, tenir compte de ces points.

Quels sont les risques de sécurités réelles ?

Le courriel est la chose qui nous sont le plus souvent, il est important de réaliser que les fournisseurs de messagerie Web, tels que Google et Yahoo n'utilisent pas le cryptage HTTPS/SSL pour l'accès par courrier électronique par défaut. Cela signifie que le réseau public Wi-Fi peut potentiellement saisir votre journal en détails, ainsi que voir vos messages électroniques.

|-----|
CHOIX #1
|-----|

===== **MODIFIER LES PARAMÈTRES DE VOTRE CONNEXION RÉSEAU DANS WINDOWS 7** =====

comment rester sécuritaire tout en surfant sur un hotspot public?

1. Vous devez changer vos paramètres de connexion réseau domestique pour un réseau PUBLIC

Pour ce faire:

- a) Ouvrez le **Centre de réseau et partage**
- b) cliquez sur **RÉSEAU DOMESTIQUE**
- C) dans la fenêtre qui s'affiche, cliquez **sur RÉSEAU PUBLIC**

Choisissez **Réseau public** pour les réseaux se trouvant dans des lieux publics (tels que des cybercafés ou des aéroports). Cet emplacement est conçu pour empêcher que votre ordinateur soit visible par les autres ordinateurs qui vous entourent et pour vous aider à le protéger contre tout logiciel malveillant sur Internet. Le groupe résidentiel n'est pas disponible sur les réseaux publics et la découverte de réseau est désactivée. Il est également recommandé de choisir cette option si vous êtes connecté directement à Internet sans utiliser un routeur ou si vous avez une connexion haut débit mobile.

Remarque:

Si vous savez que vous n'aurez pas besoin de partager des fichiers ou des imprimantes, le choix le plus sûr est **Réseau public**.

Comment le Pare-feu Windows affecte les emplacements réseau:

=====
L'emplacement **Réseau Public** bloque l'exécution de certains programmes et services, pour protéger votre ordinateur contre tout accès non autorisé lorsque vous êtes connecté à un réseau dans un endroit public. Si vous êtes connecté à un réseau public et que le Pare-feu Windows est activé, certains programmes ou services risquent de vous demander de leur permettre de communiquer à travers le pare-feu, afin qu'ils puissent fonctionner correctement.

Lorsque vous autorisez un programme à communiquer à travers le pare-feu, cette autorisation vaut pour chaque réseau ayant le même emplacement que le réseau auquel vous êtes actuellement connecté. Par exemple, si vous vous connectez à un réseau depuis un cybercafé et que vous choisissez Réseau public comme emplacement, puis que vous débloquez un programme de messagerie instantanée, ce programme est alors débloqué pour tous les réseaux publics auquel vous vous connectez.

Si vous prévoyez de débloquer plusieurs programmes alors que vous êtes connecté à un réseau public, pensez à modifier l'emplacement réseau en Réseau domestique ou en Réseau de bureau. Il est peut-être plus sûr de modifier ce réseau spécifique que d'affecter chaque réseau public auquel vous vous connectez à partir de ce point. Rappelez-vous cependant que si vous effectuez cette modification, votre ordinateur sera visible par les autres ordinateurs du réseau, ce qui constitue un risque de sécurité.

CONSEILS:

=====

- Lorsque vous surfez sur le Web, Utilisez le **SSL** autant que Possible (ex: **https://**)
- Les cartes de crédit et autres informations sensibles sont complètement à l'abri des curieux.
- Si vous devez malgré tout entrer votre numéro de carte de crédit sur un réseau public sans fil, **vérifiez qu'une icône de cadenas verrouillé** apparaît en bas à droite de la fenêtre du navigateur, puis assurez-vous que l'adresse du site Web commence par

https: (« s » pour sécurisé).



- Fermez la connexion **WIFI** lorsque vous ne l'utilisez pas.

|-----|
CHOIX #2
|-----|

Cacher un ordinateur sur le réseau local

Si vous vous baladez de **wifi public** en **wifi public**, vous avez probablement remarqué que vous pouvez voir les noms des machines des autres personnes connectées à ce réseaux, voir même explorer les répertoires que ces derniers ont partagés sur le réseau.

Cacher votre ordinateur sur le voisinage réseau (réseau local) est possible !

Attention quand même car même si le nom de votre machine n'est plus visible dans le voisinage réseau des autres, elle reste quand même « **pingable** » et trouvable pour ceux qui chercheront un peu ou qui connaissent le nom de votre ordi.

Voici comment sous Windows 7 :

1. il faut ouvrir l'éditeur de base de registre:
 - cliquez sur (**Démarrer / Exécuter** et tapez: **Regedit**
2. puis vous rendre sur la clé suivante :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters
3. et créez une nouvelle valeur: **DWORD 32 bits**
 - que vous nommerez « **Hidden** » avec une valeur de « **1** »
4. **Redémarrez le PC** et le tour est joué !
5. **Pour le rendre à nouveau visible**, supprimez simplement cette clé et rebootez.

|-----|
CHOIX #3
|-----|

CRÉER UN RÉSEAU VIRTUEL (VPN) AVEC "TOR" OU "HOTSPOT SHIELD"

=====

CRÉER UN RÉSEAU VIRTUEL (VPN) AVEC "TOR"

=====

Sécuriser sa navigation sur les réseaux publics en utilisant un réseau **VPN** (réseau privé virtuel)

"**Tor**" se présente sous la forme un package sans installation (portable) comprenant le **client VPN** (pour créer un tunnel VPN sécurisé), Firefox (navigateur Web).

La version de Firefox est déjà préconfigurée pour utiliser le VPN et la connexion sécurisée. Vous pourrez donc surfer sur Internet en toute sécurité lorsque vous êtes connecté à un réseau public. Sachez que cette sécurité a tout de même un prix : la navigation sur Internet est alors beaucoup plus lente.

Sur les **réseaux filaires publics** sur lesquels vous connectez votre ordinateur, c'est un peu plus compliqué pour attraper vos données, mais un administrateur réseau peut facilement voir les échanges non sécurisés sur le réseau et voir exactement ce que vous faites sur Internet.

La solution pour surfer en toute sécurité sur Internet et ne pas risquer de se faire voler des informations lorsque vous souhaitez vous connecter à un réseau public est d'utiliser un réseau privé virtuel, appelé communément **VPN**.

Un **VPN** est une sorte de tunnel crypté entre deux points (votre ordinateur et un serveur distant) où toutes les données qui transitent sont entièrement cryptées et protégées. Ainsi, lorsque vous êtes connecté à un réseau public, personne ne peut voir les données que vous échangez.

TÉLÉCHARGER "TOR"

<http://www.torproject.org/>

http://www.torproject.org/dist/torbrowser/tor-browser-1.3.24_fr.exe

1. Une fois le téléchargement terminé, cliquez sur le bouton **Exécuter**.
2. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Extract**.
3. L'archive contenant **Tor, Firefox et Pidgin** est alors décompressée. Lorsque c'est terminé, vous disposez du dossier **Tor Browser** à l'endroit où vous avez

téléchargé le **pack Tor**. Ce dossier contient le **client VPN Tor** ainsi que les versions adaptées de **Firefox et de Pidgin**.

Créer un tunnel VPN sécurisé:

=====

Dans un premier temps, vous devez créer un VPN sécurisé avec Tor. Une opération très simplifiée avec **Vidalia**.

1. Dans l'explorateur Windows, ouvrez le dossier où vous avez téléchargé et décompressé **Tor**, votre clé USB par exemple, et double cliquez sur le dossier **Tor Browser**.
2. Double cliquez sur le **fichier Start Tor Browser.exe**.
3. Dans la fenêtre **Vidalia** qui s'ouvre, une connexion sécurisée avec **Tor** est initialisé.
4. Au bout de quelques secondes, la connexion est faite et vous êtes connecté à **Tor**.

Surfer et discuter en toute confidentialité:

=====

Firefox est adapté à Tor est alors ouvert.

1. Vous pouvez surfer en toute sécurité et confidentialité avec Firefox.
2. Notez l'information "**Tor Actif**" en bas de la fenêtre qui vous garantie anonymat et confidentialité des données que vous échangez.
3. Même votre véritable **adresse IP est masquée**. Vous êtes anonyme.
4. Lorsque vous avez terminé votre navigation sécurisée, cliquez sur le bouton **Arrêter Tor** de la fenêtre Vidalia.
5. **Tor** est arrêté. Vous pouvez fermer Vidalia.

Seule la version adaptée à Firefox passe par le VPN sécurisé et vous garanti sécurité et confidentialité. Si vous utilisez d'autres versions, vos échanges ne seront pas cryptés et protégés.

VPN et vitesse

=====

Le fait de passer par de multiples noeuds sécurisés et d'encapsuler vos données dans un tunnel crypté impacte forcément votre vitesse de navigation sur Internet. C'est le prix de la confidentialité. A réserver donc à la navigation sur Internet, à l'échange de mails et à la messagerie instantanées. Ne comptez donc pas (pour le moment ou du moins sur les VPN gratuits) vous lancer dans le téléchargement de fichiers du fait des débits vraiment trop faibles.

=====

CRÉER UN RÉSEAU VIRTUEL (VPN) AVEC "HOTSPOT SHIELD"

=====

La solution la plus simple et abordable est de mettre en œuvre un réseau privé virtuel (VPN). La connexion à un serveur VPN vous permettra de chiffrer tout votre trafic Internet, donc les pirates du WiFi ne pourront pas saisir vos informations. La solution est d'utiliser le logiciel gratuit "**Hotspot Shield**" de AnchorFree.

- > Accès à tous vos contenus préférés privé
- > Sécurisez votre session Web avec cryptage HTTPS
- > masquer votre adresse IP de votre vie privée en ligne
- > Protégez-vous des fouineurs de hotspots Wi-Fi, hôtels, aéroports, bureaux administratifs et FAI.
- > Sécurisez vos données & informations personnelles en ligne

TÉLÉCHARGER "HOTSPOT SHIELD"

<http://www.anchorfree.com/hotspot-shield/>
<http://anchorfree.com/downloads/hotspot-shield/>