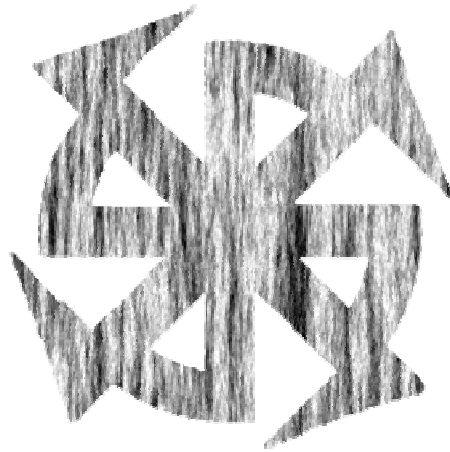


# Confédération Aime et Sers



<http://www.aime-et-sers.com>

## Anonymat sur Internet

### Les adresses IP

Beaucoup de personnes pensent à tort que sur Internet on peut faire ce que l'on veut sans danger. Et puisque il est assez risqué de distribuer des tracts et de peindre des slogans NS dans la rue, on s'imagine que faire de la propagande sur Internet est un moyen plus discret et moins dangereux. C'est une grossière erreur, et voila pourquoi :

En informatique, toute activité laisse des traces. A chaque fois que vous vous servez de votre ordinateur, celui-ci enregistre à votre insu quantité d'informations qui peuvent éventuellement vous compromettre si les autorités procèdent à la saisie et à l'étude minutieuse de votre matériel. La police a des experts informaticiens d'excellent niveau !

Autre chose : Sur Internet personne n'est jamais totalement anonyme. Il est possible de dissimuler son identité, mais dans une certaine limite seulement et à la condition d'utiliser les bons outils pour cela, comme nous allons le voir ci-dessous.

Si vous pensez que vous pouvez surfer sur un site ou bien en créer un tout en restant anonyme parce que vous ne communiquez pas d'informations personnelles vous concernant, vous êtes dans l'erreur. Car pour être vraiment anonyme sur Internet il ne suffit pas de taire sa véritable identité : L'informatique vous trahit sans même que vous vous en rendiez compte...

Si, par exemple, lors de votre inscription à un forum de discussion, à un service de blog etc... vous déclarez vous appeler Madame X âgée de 56 ans et habitant à telle adresse à Lyon alors qu'en réalité vous êtes Monsieur Y âgé de 18 ans et habitant Paris, vous ne serez absolument pas anonyme pour autant.

En effet, et sans entrer trop dans le domaine de la technique, à chaque fois qu'un ordinateur se connecte à Internet il lui est automatiquement attribué une adresse IP temporaire, valable pour

toute la durée de la session en cours. Cette adresse IP sert à ce que votre ordinateur soit reconnu par le Réseau, et c'est elle qui vous permet d'accéder aux sites web que vous désirez consulter. Elle est donc indispensable.

Une adresse IP ressemble à ce genre de chose : 280.168.80.77 (adresse fictive donnée pour l'exemple). Il n'y a pas, en théorie, à l'instant T deux ordinateurs qui partagent la même adresse IP. C'est une identité personnelle pour chaque ordinateur. Si moi j'ai 280.168.80.77 mon voisin de palier aura peut-être l'adresse IP 268.168.92.24.

Les adresses IP transitent et sont automatiquement collectées par les Fournisseurs d'Accès à Internet (AOL, Orange, Free etc...). Elles sont enregistrées dans de grands listings informatiques appelés "logs" (journaux d'information pour les administrateurs réseaux).

La loi française oblige les FAI à conserver les logs des connexions à Internet pendant une durée qui, à ce qui m'a été rapporté, serait désormais de 5 ans (contre 1 an encore récemment). Dans quel but ? Officiellement afin de lutter contre les terroristes qui utilisent beaucoup Internet. Officieusement, pour mieux traquer la population et tous les opposants au Système dont nous faisons partie en tant que NS.

Que se passe-t-il si la "Justice" veut s'en prendre à un internaute NS ? il suffit que la police demande au fournisseur d'accès de l'internaute le log de toutes ses connexions et il apparaîtra très clairement qu'à telle heure de tel jour, l'internaute en question a consulté tel site, pendant tant de temps, qu'il a lu telle page, qu'il a téléchargé tel fichier etc... Rien ne passe au travers du système...

Puisqu'il n'y a qu'une adresse IP par ordinateur de connecté, il n'est pas possible de prétendre que l'on n'est pas l'internaute qui a visité le site en question. C'est imparable ! A moins d'avoir fait le grand ménage et en profondeur sur son ordinateur et de n'avoir absolument aucune trace "douteuse" sur sa machine, vous êtes pris la main dans le sac si j'ose dire.

Lorsque la "Justice" veut s'en prendre à tous les visiteurs d'un site web donné, elle récupère le log des connexions sur le serveur hébergeant le site en question. Elle a ainsi une longue liste d'adresses IP avec les heures exactes de connexion pour chaque ordinateur. Comme nous venons de le voir, à chaque adresse IP son ordinateur unique. Il est donc facile de remonter jusqu'au FAI de chaque internaute, et de là obliger légalement l'entreprise à communiquer les coordonnées de son client.

En résumé : Log sur le serveur > Liste d'adresses IP > Liste de clients de FAI > Liste de noms et d'adresses d'internautes.

Les fournisseurs d'accès à Internet n'ont pas le droit de refuser de communiquer à la police les coordonnées exactes de clients suspectés de telle ou telle chose par la Justice. Ne comptez donc pas sur eux pour vous protéger.

De plus, bon nombre d'administrateurs réseaux chez les FAI sont tout sauf des pro NS. Pour consulter un site web vous passez parfois par des dizaines de serveurs intermédiaires, ce qui donne l'occasion à des dizaines et des dizaines de personnes d'intercepter votre adresse IP. Ces techniciens sont capables de vous tracer, c'est leur métier. Rien n'interdit de penser qu'un jour on peut se faire tracer par un juif, un hallogéne, un marxiste, un anarchiste...

Alors faut-il renoncer à Internet lorsque l'on est NS ? PAS DU TOUT ! Il faut simplement prendre ses précautions :

Il existe un moyen de dissimuler son adresse IP lorsque l'on surfe sur Internet, c'est utiliser un serveur proxy. Grosso modo, un serveur proxy est un serveur informatique qui va accueillir différents ordinateurs et leur redistribuer à tous la même adresse IP. De la sorte, si 1 000 internautes se connectent en même temps au proxy, 1 000 ordinateurs auront la même adresse IP. Très pratique n'est-ce pas ?...

Il y a quatre avantages à cela :

D'une part vous n'êtes plus désigné d'office comme celui qui s'est connecté à tel site du fait de votre adresse IP. Le serveur que vous utilisez est généralement situé à l'autre bout de la planète et il n'est plus celui de Club Internet ou de 9 Télécom par exemple. C'est celui d'une obscure entreprise informatique située à Hong Kong ou ailleurs, et a priori vous n'avez aucun lien avec cette société.

Deuxièmement si la police interroge votre FAI celui-ci lui indiquera simplement qu'à telle heure de tel jour vous utilisiez un proxy et donc qu'il ne lui est pas possible de dire quels sites vous avez consulté après vous être rendu anonyme. Le proxy est un écran de fumée derrière lequel tout ce que vous faites est opaque pour votre FAI.

Troisièmement, si la police saisit le log d'un site sur lequel elle enquête, vous apparaîtrez non pas sous la forme de votre véritable IP mais sous celle d'un Malaysien, d'un Chinois, d'un Russe etc... en fonction du pays dans lequel se trouve le serveur proxy. Ca brouille encore plus les pistes...

Et quatrièmement, si la police vient à vous demander ce que vous faisiez à tel moment en étant caché derrière une adresse IP fournie par un proxy, elle n'a aucun moyen de prouver que vous étiez bien sur un site "compromettant". Il est légal d'utiliser un serveur proxy, du moins pour l'instant, et vous n'avez pas à vous justifier de cela.

Au moment en question il y avait de par le monde des centaines, voire des milliers d'internautes ayant la même adresse IP. Il est donc impossible de prouver que c'était vous qui étiez à telle date et à telle heure sur le site internet intéressant la "Justice".

A savoir qu'il existe également des proxies gratuits mais leur disponibilité n'est pas excellente (fréquentes interruptions de service) et généralement ils ralentissent énormément la connexion à Internet. Les proxies payants ralentissent aussi la connexion, mais dans une moindre mesure.

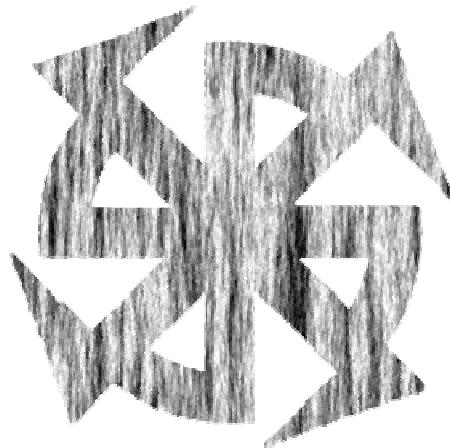
Pour utiliser un proxy commercial il faut souscrire un abonnement payant. Comptez environ 100 euros à 150 euros par an pour un service de qualité. C'est assez cher, mais ça en vaut le coup : Car la liberté n'a pas de prix ! Mieux vaut s'arrêter de fumer ou de sortir trop souvent pour se payer son proxy, on fait ainsi d'une pierre deux coups !

La plupart des sociétés proposant un service de proxy proposent des abonnements trimestriels et même souvent mensuels. Ca revient plus cher mais ça permet de tester le service. Il faut parfois tester plusieurs offres pour trouver celle qui nous convient le mieux.

A ma connaissance il n'existe aucune société française proposant un service de proxy. De toute manière ce serait très dangereux d'y recourir. Il faut donc comprendre un minimum l'anglais pour trouver un tel service sur le web et souscrire un abonnement.

Autre précision d'ordre général : La "faille" en matière de proxy c'est la société gérant le serveur de proxy : En effet, dans la chaîne des serveurs vous permettant de vous connecter de manière anonyme à Internet, ce prestataire est le seul à connaître à la fois votre véritable adresse IP et celle vous servant de masque sur le réseau.

Cependant un serveur de proxy vraiment professionnel ne conserve pas de logs de connexion, ceci afin de protéger l'anonymat de ses clients. Au pire il les efface au bout de 24h ou de 48h, ce qui est trop rapide pour permettre à la police de remonter jusqu'à vous. Veillez bien à ce détail lors de votre abonnement à un proxy commercial.



Pour tout contact :  
[secretariat@aime-et-sers.com](mailto:secretariat@aime-et-sers.com)  
ou  
[herr-wolf@aime-et-sers.com](mailto:herr-wolf@aime-et-sers.com)