Informations personnelles et anonymat sur Internet/ comment prendre de bonnes habitudes.

Introduction: Quelles traces sont enregistrées sur internet?

Se connecter à un réseau informatique quel qu'il soit laisse des traces. A plus forte raison lorsque vous êtes sur Internet, le réseau des réseaux, vous devez savoir que chaque fois que vous visitez un site web, quel qu'il soit, des données vous concernant sont enregistrées: le numéro unique de votre ordinateur sur internet attribué par votre fournisseur d'accès (adresse IP), et le moment précis de votre passage (date, heure), ainsi que des coordonnées du fournisseur d'accès et de la ville par lequel vous êtes « envoyé » sur le web. Sauf si vous passés par un proxy (voir plus loin) on peut donc savoir depuis quelle région du monde vous accédez à internet (pensez-y si vous faites des déclarations sur des sites d'institutions tels que la caf ou d'autres administrations qui pourraient un jour avoir la désobligeance de vous demandez de vous justifier sur vos déplacements...)
D'autres infos basiques sur votre ordinateur sont également transmises et enregistrées, comme le type de navigateur que vous utilisez (Firefox, Inetrnet Explorer, Safari...) et il est même possible de savoir quelle est la dernière page ou site web que vous avez visité.
Tout cela ne demande aucun effort de surveillance particulier de la part des administrateurs/trices de sites web, quels qu'ils/elles soient. Ca fait maintenant partie des fonctions statistiques de base d'un service d'hébergement de site web.
A l'inverse, les sites web que vous visitez laissent eux aussi des traces sur votre ordinateur. Votre navigateur va garder un historique de toutes les pages que vous avez vues au cours d'une session de navigation sur internet, et pourra les conserver dans une liste pendant plusieurs semaines si vous le ne configurez pas. Mais en plus de cela il y a un système de fichiers plus ou moins temporaires appelés « cookies » qui s'installent à un endroit précis de votre système lorsque vous allez sur un site, cookies qui permettront au site de vous reconnaître lors d'une prochaine visite ou simplement pour que votre navigateur n'ait pas à recharger deux fois une même page déjà vue il y a peu de temps.
Les cookies peuvent être plus ou moins intrusifs et malveillants, mais les réglages de votre navigateur internet vous permettront de les effacer après chaque session (préférez Mozilla Firefox pour ça, dans « outils », « effacer mes traces »).
La législation actuelle prévoit que les fournisseurs d'accès à Internet et les éditeurs et hébergeurs de sites web doivent conserver toutes les données de connexion pendant une durée minimum d'un an, pour les fournir sur demande des autorités .
Pour en savoir plus sur votre adresse IP vous pouvez visitez cette page qui vous renseignera :
http://anonymat.org/vostraces/index.php

Concernant les informations personnelles, il faut savoir que le fichage est une pratique banale. Tout ce qui peut permettre de dresser des profils consommateurs est une véritable mine d'or pour les sociétés sur internet, comme les réseaux « sociaux » et autres portails communautaires et blogs gratuits, Myspace, Facebook, skyblog etc... Car la gratuité de ces services n'empêche pas leur nature fondamentalement commerciale. Ce sont d'ailleurs les nouveaux modèles économiques du « web 2.0 », comme on dit dans le marketing. Et dans la nouvelle économie des services gratuits il n'y a pas beaucoup de place pour le respect de la vie privée, croyez-moi...

Petit MANUEL de sécurité et d' ANONYMAT sur INTERNET:

Ce qui suit est un petit manuel pratique pour avoir un minimum de contrôle et de vie privée (certain-e-s vont rigoler...) en navigant sur internet. Et pour une fois ce manuel s'adresse en premier lieu aux utilisateurs-trices d'ordinateurs qui fonctionnent sous Windows (là aussi y'en a qui vont se moquer). Car si en matière de sécurité informatique il est largement préférable d'utiliser un système d'exploitation libre Linux avec des versions gratuites et très accessibles comme Ubuntu (http://www.ubuntu-fr.org), il serait dommage de ne pas prendre de bonnes habitudes aussi sous Windows, car on a pas toujours une machine libre sous la main, et puis il vaut mieux commencer par là que ne rien changer du tout. Attention les informations et exemples à propos de l'adresse IP et du fichage sur internet sont aussi valables pour les bienheureux et les bienheureuses sous Linux.
Pour partir sur de bonnes bases, on ne le répétera jamais assez, **il est plus que fortement conseillé d'installer Firefox** de Mozilla, qui est beaucoup plus fiable en matière de securité qu' Internet Explorer, plus vulnérable face aux logiciels espions (spyware) qui s'installent sur votre ordinateur comme des virus via internet et détournent vos informations privées. Le navigateur gratuit Firefox lui, en plus de sa fiabilité beaucoup plus importante sur

internet, vous permet également d'effacer de façon complète et rapide votre historique de navigation et de téléchargement, les cookies laissés par les sites visités, d'effacer les mots de passe éventuellement enregistrés sur l'ordinateur, et autres sessions d'identification. Pour cela, **aller dans la barre du haut de navigateur, « outils », puis cliquer sur « effacer mes traces »** . Vous pouvez aussi configurer les options de « outils » pour que les traces s'effacent automatiquement lorsque vous fermez firefox (« outil », « options », « vie privée », cochez la case « toujours effacer mes informations à la fermeture de firefox »).
Noter que Internet explorer propose aussi dans ses options d'effacer ce genre de traces, mais c'est moins complet, l'historique de navigation ne disparaît pas complêtement, et il n'y a aucune raison de faire confiance à Microsoft, leur culture d'entreprise étant basée en grande partie sur des pratiques de vente qui ne font pas grand cas des choix des utilisateurs.
(lire par exemple sur les mises à jours à votre insu: http://www.vulgarisation-informatique.com/actualite-23.php)

1_Sécurité de base sur votre ordinateur: antivirus et Pare-feu (Firewall)

Avant d'envisager de vous connecter sur internet vous devez installer deux sécurités indispensables sur votre ordinateur, qui vous éviteront bien des soucis:
-Premièrement un **antivirus** vous évitera d'être contaminé-e par les virus et applications espionnes les plus courantes sur le web: cheveaux de troie, malware, spyware, qui dérèglent progressivement votre ordinateur, en prenent le contrôle à distance, ou interceptent les données sensibles comme votre numéro de carte bancaire lorsque vous payez en ligne.
Il existe plusieurs antivirus très utiles que vous pouvez télécharger gratuitement dans une version de base appelées aussi versions « familiales » ou « démos » et qui mettront à jour régulièrement leur liste d'infos sur les nouveaux virus recensés (du moment que vous êtes connectés régulièrement à internet)
-Avast antivirus:
http://www.avast.com/fre/download-avast-home.html
-AntiVir
http://free-av.com
-Avira:
http://avira-antivir.info/fr

-Deuxièmement, installer un **pare-feu** efficace et plus fiable que celui existant par défaut (pour les utilisateurs de PC et de Windows particulièrement). Il s'agit d'un programme qui va controler le trafic de votre ordinateur et les échanges de données qui y entrent ou en sortent. Ainsi chaque fois qu'un site web ou qu'une application voudra communiquer avec votre PC de façon inhabituelle sur internet, vous aurez un petit message vous avertissant et vous demandant si vous voulez autoriser l'échange. En configurant les programmes et sites sûrs vous n'aurez pas à autoriser à chaque fois, mais le pare-feu bloquera d'éventuelles attaques extérieurs sur votre ordinateur, ou de simples intrusions et visites non-sollicitées.
-Pare-feu Zone alarm :
http://www.zonealarm.com

-**Réseaux Peer To Peer**
Pour les personnes qui se connectent régulièrement sur des réseaux d'échanges de Particulier à particulier (Peer to Peer) tels que Emule, Kazaa, Soulseek etc. il y a un danger particulier d'intrusion de personnes mal intentionnés qui cherchent à « scanner » votre disque dur, pour repérer notamment les gros consommateurs d'oeuvres protégées par copyright. Le site blocklist manager proposent des listes noires à télécharger et à intégrer à Emule notamment (dans Préferences/sécurite), pour que l'accès de certaines adresses d'ordinateurs soient bloquées pendant que vous échangez sur le réseau. Dans cette liste à mettre à jour de temps en temps on trouve des adresse IP officielles d'institution et de services de renseignements...
-Site Officiel pour télécharger blocklist :
http://www.bluetack.co.uk/
-Un tutoriel pour installer les listes nires de blocklist:
http://www.6ma.fr/tuto/blocklist+manager+filtre+anti+ips-83
-Il existe aussi Peer Guardian dans le même genre, c'est un mini pare-feu dédié au filtrage pour le Peer to Peer:
http://www.numerama.com/telecharger/6488-PeerGuardian.html

Le principal risque des réseaux Peer to Peer cités, outre les possibilités de virus dans les fichiers, c' est que vous vous connectez directement sur un réseaux où votre adresse IP (votre identité sur internet) n'est pas masquée. C'est là une fois connecté et une fois que vous avez choisis des serveurs un peu plus spécifiques

parmi la liste proposée que vous cherchez directement vos fichiers parmi la masse énorme mise en échange. Mais vous êtes constamment présent de façon publique sur un réseau gigantesque en libre accès, bien que vous téléchargiez les fichiers directement sur les ordinateurs des autres personnes présentes, et non sur un serveur central.
Vous avez donc le risque d'être repéré par des autorités présentes elles aussi sur le réseau, et d'être traduit en justice si vous télécharger des « oeuvres protégées par copyright »
Pour contourner un peu le problême, le système d'échange **Bit Torrent**, lui, fonctionne de façon légèrement différente en vous permettant de chercher d'abord sur des sites spécialisés des lien « torrent » de films musique ou autre, puis après avoir téléchargé ce simple lien de l'utiliser en vous connectant avec le logiciel Bit Torrent sur un réseau ouvert uniquement entre les personnes qui téléchargent le même fichier que vous.
C'est lorsque que vous cherchez des liens de fichiers à télécharger qu'il sera le plus prudent de masquer votre identité comme expliqué après.
La solution ultime pour le Peer to Peer sans aucun risques reste l'utilisation de logiciels P2P cryptés, mais ce n'est pas le sujet de ce document.

2_L'anonymat « léger » pour une simple navigation rapide sans laisser de traces

Pour éviter de laisser votre identité en passant sur un site sensible, vous pouvez utiliser un site « anonymiser » (en anglais) ou « proxy », sans installer quoi que ce soit sur votre ordinateur.
Il suffit de vous rendre sur un premier site web qui vous proposera de taper l'adresse du site sur lequel vous désirez vous rendre de façon anonyme, et le « proxy » (serveur intermediaire) par lequel vous serez redirigé communiquera au site une adresse IP qui n'est pas la votre.
Ca dépanne bien au quotidien, mais en général ces sites ne permettent pas d'aller sur une page de connexion (login/mot de passe) ou de remplir un formulaire d'inscription à un service. Et attention, si vous avez besoin d'une solution de simple navigation occasionelle absolument sure, choisissez bien votre service, car rien ne vous garantit qu'en cas de procédure policière exceptionnelle le service d'anonymat utilisé ne divulguera pas votre vraie adresse aux autorités.
Dans ce cas-là, une autre option qui peut vous permettre occasionnellement un très bon anonymat est de vous rendre en plus dans un cyber-café ou un taxiphone. Vous saurez alors que si le proxy utilisé est harcelé par les autorités suite à votre utilisation, tout ce qu'ils pourront leur communiquer sera une adresse IP impersonnelle... mais là on parle d'utilisations vraiment exceptionnelles qui sortent du cadre courant, et dans ce domaine rien ne garantit que vous ne soyez pas en plus enregistré-e par la vidéo surveillance de la boutique ou simplement dénoncé-e par le patron ou par les autres clients. C'est vous qui voyez...

-Quelques sites proxy bien utiles:
http://www.surrogafy.com *(celui-ci permet aussi de se logger à une boite email ou autre, mais par contre il ouvre des fenêtres de pub...)*
http://www.the-cloak.com
http://www.silentsurf.com
http://pici.picidae.net/index.php

3_L'anonymat complet, pour créer des profils, s'inscrire à des services internet et poster des articles

Lorsque vous créez un profil ou vous inscrivez sur un service tel que blog ou autre, votre adresse IP est enregistrée et servira à vous identifier si vous mettez en ligne des contenus illégaux, tenez des propos diffamatoires, ou êtes simplement un peu trop critiques.
Pour éviter d'être fichés vous veillerez donc à être anonymes lorsque vous vous inscrivez et vous connectez à votre blog ou autre profil. Utiliser un site proxy comme proposé au paragraphe 2. n'est pas toujours efficace car ces sites ne permettent pas tous de valider une page de connexion avec login et mot de passe ou un formulaire d'inscription en javascript. C'est là que vous aurez besoin de Tor.
Firefox vous permet d'intégrer l'application Tor, qui sert à masquer votre adresse IP, en installant un « bouton Tor » (Tor button) dans votre navigateur, bouton qui permet d'activer ou désactiver Tor, et donc de devenir anonyme quand vous en avez besoin.
C'est une très bonne solution pour vous créer un blog anonyme, ou une adresse email par exemple. Mais l'utilisation de Tor peut ralentir fortement votre vitesse de navigation. Utilisez Tor également lorsque vous poster des article sur votre blog ou envoyez des emails, car vous êtes aussi enregistré-e-s à ces moment là.

-Pour installer Tor et TorButton (après avoir installé Firefox), allez voir ici:
http://www.torproject.org/download.html
-Guide plus complet pour installer et blogguer anonymement avec Tor
http://advocacy.globalvoicesonline.org/projects/guide/guide-fr/

4_Les moteurs de recherche, Google et compagnie...

Le principe du traçage avec adresse IP est le même lorsque vous utilisez des moteurs de recherche comme google et yahoo. Mais la grosse variante est que ceux-là gardent en plus les informations que vous avez recherchées, histoire de faire de beaux profils de consommateurs pour la publicité ciblée ou de renseigner les autorités qui auraient besoin de savoir qui a l'habitude faire des recherches sur tel ou tel mot-clé, ou même sortir votre historique de recherches sur plusieurs années dans le cadre d'une enquête de police. Google par exemple, a racheté le n°1 de la publicité en ligne Doubleclick, et si vous lisez leur politique de confidentialité (http://www.google.fr/intl/fr/privacy.html) vous vous rendrez compte que rien ne les empêchent de vous ficher pour vous cibler avec de la pub qui correspond à votre profil consommateur, un marché plein d'avenir sur internet (mais qui existe déjà en dehors: les cartes de fidélités des supermarchés par exemple, vous ne vous êtes jamais demandées à quoi cela pouvait bien leur servir?)

Vous pouvez alors utiliser des moteurs de recherche alternatifs aux 3 géant dans le domaine que sont Google, Yahoo et MSN etc. mais sans réelle garanties de ne pas être fiché-e-s aussi. Pour des recherches délicates, ou simplement pour prendre une bonne habitude que vous ne regretterez pas, utilisez donc les sites de proxy décrit en chapitre 2 ou Tor comme expliqué en chapitre 3.
Et vous pouvez également utiliser des moteurs de recherches qui vont vous « anonymiser » en utilisant google, comme http://www.scroogle.org/cgi-bin/scraper.htm
-*Voir aussi: Google rachète Double Click, le géant de la publicité sur internet:*
http://www.iris.sgdg.org/info-debat/comm-pi-merger1107.html

5_Les logiciels Microsoft et leurs mouchards

Lorsque vous créez des documents avec des logiciels comme ceux de microsoft par exemple, les plus répandus en matière de traitement de texte (Word, Office etc...), vous intégrez également sans le savoir un code d'identification caché, et vous archivez les modifications et les transits dans une partie cachée de votre document.
C'est une pratique habituelle de Microsoft, à qui on ne peut décidément pas faire confiance, n'est-ce pas. Mais rien ne vous garantis qu'une autre société commerciale qui édite son propre logiciel de traitement de texte ne fasse pas la même chose (ce serait d'ailleurs aussi le cas avec Photoshop notamment, un logiciel de graphisme).
-*A propos du traçage sur les document Word lire:* http://www.zataz.com/index.php?action=news&id=2389

Prenez donc l'habitude de réaliser vos documents avec des logiciels libres dont l'éthique est justement à l'opposé de ces pratiques de traçage à l'insu du « client ».
-Du traitement de texte
Abi Word: http://www.abisource.com/download/
...à la mise en page plus complète pour l'édition:
Scribus: http://www.scribus.fr/
Open Office: http://fr.openoffice.org/
The Gimp: http://www.gimp-fr.org/

6_La confidentialité des emails

En ce qui concerne les emails, si vous avez un compte chez un gros fournisseurs commercial comme yahoo, hotmail, laposte, Gmail (google) etc... vous devez bien avoir à l'esprit que la confidentialité n'est plus à la mode.
Toujours est-il que lors de la création d'une adresse email et de la consultation de vos messages vous laissez également vos informations personnelles, conservées pendant un an. Dans le cadre d'une procédure de police, c'est en général l'adresse IP enregistrée à la création de l'adresse email qui va déterminer l'identité réelle aux yeux de la justice.
Veillez donc à vous rendre anonyme également vis-à-vis de votre service d'email si vous avez tendance à envoyer ou recevoir des informations délicates. Mais si c'est le cas évitez les services commerciaux cités plus hauts qui n'hésiteront pas à vous dénoncer.
Par exemple:*Yahoo dénonce un utilisateur chinois dissident à la dictature:*
http://www.lesmotsontunsens.com/yahoo-chine-denonce-collabore-avec-le-gouvernement-chinois-mais-soutient-les-condamnes
Dans tous les cas, le fait que les messageries email qui sont de la correspondance privée soient centralisées sur de gros serveur commerciaux posent un problème de confidentialité des données. Une véritable solution, comme pour d'autres des questions soulevées ici, résideraient dans le fait de monter des services d'hébergements alternatifs, chez des personnes et des collectifs plutot que dans des gros datacenter où la

police n'à qu'à se présenter à la porte pour saisir beaucoup trop d'informations, même sans autorisation spéciale...

7_Le filtrage présent et à venir

Techniquement les fournisseurs d'accès à internet ne peuvent pas contrôler de façon systématique tous les fichiers de toutes les connexions internet qui transitent par leurs services, cela représente une masse beaucoup trop importante de données à traiter, et demanderai des installations techniques spécifiques, couteuses. Mais cela pourrait changer.
De manière générale internet à tendance à être de plus en plus centralisé sur des gros sites qui concentrent les contenus (Myspace, Youtube, Dailymotion, Blogspot etc.) et quelques gros fournisseurs d'accès/hébergeurs qui peuvent survivre à des frais de justice pour des litiges de droits d'auteurs de plus en plus fréquents. Ce mouvement général, outre qu'il est en train de tuer le principe d'internet de particulier à particulier, et qu'il va contre les logiciels libres et les formats ouverts qui ont permis son développement, va inévitablement rendre le web et internet beaucoup plus contrôlables qu'il ne l'a jamais été, si l'on ne prend pas des habitudes différentes pour utiliser internet.
Lire un texte très complet sur les solutions de filtrage hybride envisagées par le gouvernement:
http://www.laquadrature.net/files/note-quadrature-filtrage-hybride.pdf
-Pour se tenir au courant des mesures appliquées ou en projet:
http://www.laquadrature.net/
- Une vidéo de conférence à propos de la centralisation d'internet:
http://www.fdn.fr/internet-libre-ou-minitel-2.html
-Sur l'extension du type de données personnelles conservées par les Fournisseurs d'Accès à Internet (FAI), lire:
http://www.pcinpact.com/actu/news/41881-donnees-connexions-retention-decret-contenu.htm

---

8_Les messageries de type Chat

Le problème de la centralisation est le même lorsque vous chattez avec une autre personne avec un petit logiciel messenger installé sur votre ordinateur. Si vous utilisez MSN, ICQ, AIM ou autres, utilisés par des millions de personnes dans le monde, tout ce que vous échangez passera par les serveurs de ces sociétés, et donc laissera aussi des traces.

>>A développer, Pidgin, Kopete

//
Pour une approche plus large du sujet:
-La révolution numérique, 3e révolution industrielle:
http://www.ladocumentationfrancaise.fr/rapports-publics/044000180/index.shtml
-Les « classes informationnelles » selon Verzola
http://ressources.samizdat.net/tiki-read_article.php?articleId=4
-La créature du réseau social:
http://www.creaturereseausocial.wordpress.com

//
Document réalisé avec Open Office, en Aout 2008
//