ce guide s'adresse surtout aux utilisateurs/trices de base, utilisant m\$windows ..

POURQUOI SE PROTEGER. il est désormais possible pour tout fournisseur d'accès de loguer des informations de sites que vous avez visités, le temps que vous passiez dessus, les horaires auxquels vous vous connectez etc. les emails contiennent tous un header RFC et un numéro unique d'identification, invisible à l'utilisateur non-averti. Ces headers donnent des informations sur votre fournisseur d'accès, car c'est à travers son réseau que passe le mail, cela se passe surtout si vous utilisez des clients email tels que outlook, apple mail, eudora ou autres. Il est donc tout à fait possible de retracer le chemin d'un mail jusqu'à chez vous..

de plus, chaque page sur le web que vous visitez peut vous tracer de façon très simple: le chemin que vous avez pris pour arriver chez eux, votre adresse ip. le système d'exploitation que vous utilisez, le client email, le serveur par lequel vous envoyez d'habitude vos mails etc. ceci se passe par des cookies, des petits scripts ou des compteurs invisibles de clicks (pour les pubs surtout) afin d'évaluer vos données et de les transformer en profils d'utilisateur, pour faire des analyses de marché par exemple. il n'est donc pas seulement question içi de se protéger contre des intrusions illicites sur votre ordinateur, mais de refuser le fichage de données privées. Mais, surtout si votre système d'exploitation est m\$windows, ceci n'est pas du tout évident.

Pour voir quels données vous transmettez visitez les sites suivants qui vont analyser la connexion:

http://tools-on.net/privacy.shtml ou bien http://privacy.net/analyze. Vous allez être surpris. tools-on.net accède même au disque c: si vous êtes sous m\$windows. Ceci par un simple script fonctionnant sur une pagec http, donc même pas un grand outil de ceux et celles que l'on appelle communément "hackers" (en fait des gens qui s'intéressent à la sécurité des réseaux comme ils l'affirment - s'ils ne sont pas du côté obscur de la force..)

ANONYMITY IS NOT A CRIME

QUE FAIRE? premiers pas: refusez les cookies là où c'est possible. Configurez votre browser de façon à qu'il détruise tous les cookies lorsque vous quittez le programme. si vous utilisez windows xp ou 2000 securisez vos donnees avec xp antispy, disponible sur http://xp-antispy.org. utilisez un firewall tel que zoneAlarm, disponible chez http://zonelabs.com. mac osx a une firewall intégré (voir: system preferences). empéchez surtout le partage de fichiers et de disques durs (click droit dans windows -> partage -> ne pas partager ce dossier).

LES MAILS. désormais http://no-log.org est un des seuls services gratuits d'email en france fournissant et une adresse mail et un accès internet par téléphone sans pour autant stocker ni même demander vos données personnelles, en ce moment ils se trouvent dans des difficultés financières, donc si vous voulez les soutenir, svp visitez leur site. si vous utilisez un client mail il semble presque indispensable d'utiliser un remailer qui envove vos mails directement de chez vous en agissant comme un propre serveur smtp (protocole d'envoi de mails). malheureusement ces outils là sont assez difficiles à gérer, même vont déformer les ID des mails ce qui va obligatoirement mener à la considération de votre mail comme spam. donc la plupart des mails ainsi envoyés n'arriveront pas chez le destinataire. pour envoyer tout de même des mails de façon anomyme, par exemple pour poster sur des forums

en restant inconnuE, utilisez le remailers en ligne: https://mixmaster.autistici.org/cgi-bin/mixemail-user.cgi ou le remailer de http://tools-on.net/privacy.shtml?2.

CRYPTER SES MAILS. il est aujourd'hui dans beaucoup de pays autorisé de crypter ses mails et ainsi, pour visualiser la chose:, d'envoyer quelque chose dans une enveloppe plutôt qu'une carte postale, qui serait potentiellement lisible par tous les gens qui arrivent à l'intercepter (le facteur, la concierge..) comment ça marche? que vous soyez sur mac, m\$windows ou linux, vous pouvez utiliser

des outils tels que PGP ou GPG. vous allez générer un trousseau de clés pour votre adresse mail. Dans le trousseau il v a une clé publique, qu'il faudra pour vous envoyer un mail cryptée (donc vous devez la donner aux personnes qui veulent vous écrire), et une clé privée qu'il vous faut pour crypter un mail et l'envoyer à quelqu'un ainsi que pour décrypter les mails qui vous sont adressés. donc, on l'aura compris: les messages ainsi cryptées sont destinés vraiment à la personne particulière qui possède et l'adresse email et sa clé privée et publique ainsi que son mot de passe pour appliquer le dé-/cryptage. Il v a même plusieurs algorithmes pour les clés, dont le plus courant sont IDEA et RSA legacy. Vous pouvez créer des clés avec divers taux d'encryptage, en allemagne étant autorisé un taux de 1024 bit, en france (à vérifier!) un taux de 128 bit. Les clés pouvants expirer à une certaine date, un organisme autorisé ne pourra même plus vous faire décrypter des anciens messages une fois la date d'expiration atteinte.. important: si vous envoyez un mail crypté à quelqu'un et les autres mails à cette personne ne sont pas cryptés, rendez vous compte que cela peut paraître bizarre au grand frère. mieux: toujours crypter vos mails si vous communiquez avec cette personne pour télécharger les logiciels adaptés et/ou des plugins pour votre client email visitez http://www.papi.org.

un autre procédé de cryptage de messages est la stéganographie qui insère votre texte dans une image ou un fichier ascii.

LE SURF ANOMNYME. pour surfer anonymément je vous conseille de partir de http://the-cloak.com même si l'accès y est limité si on l'utilise gratuitement. cliquez sur "surf" à gauche et configurez la session. un autre outil online est http://rewebber.de. si vous utilisez internet explorer il y a aussi http://rewebber.de. si vous utilisez internet explorer il y a aussi http://anonymization.net qui marche en ligne mais qui vous fournit directement une barre d'adresse sécurisée et gratuite pour l'explorer. de plus, http://tools-on.net/pivacy.shtml?2 met à disposition un outil de surf anonyme, puis aussi des adresses mails gratuits et anonymes. En fait ces outils là marchent comme un proxy.

UTILISER UN PROXY. qu'est-ce que c'est? un proxy est un serveur de proximité sur lequel vous pouvez vous connecter et grâce auguel votre adresse IP personnelle reste anonyme vis-à-vis les scripts de divers sites qui voudront bien vous connaître. Les proxies peuvent être configurés dans les préférences de votre browser et directement à la connexion de votre modem, on trouve des listes de proxys anonymes par exemple sur http://toolson.net/privacy.shtml . On peut désormais utiliser un proxy aussi pour faire du ftp (file transfer protocol). l'inconvénient est désormais la configuration manuelle de ces outils, mais si vous surfez beaucoup, prenez le temps nécessaire. sous windows allez dans les paramètres internet dans le panneau de configuration, dans connexions sélectionnez votre fournisseur d'accès, puis cliquez sur paramètres --> utiliser un serveur proxy puis entrez y l'adresse et le port du proxy, comment configurer proxy un sur mac: http://www.helpdesk.uconn.edu/trouble/proxy/proxm an.html (il faut bien sûr que vous utilisez le proxy de votre choix). l'utilisation de proxys peut ralentir le taux de transmission.

un autre outil est JAP, dévéloppé par l'université technique de Dresde qui fonctionne en gros comme une chaine de serveurs proxy et qui protège bien vos données. JAP existe pour windows (téléchargez l'installation entière), mac osx, mac os9 (quelques manips à faire), linux, os/2 et pocket pc (version beta). après l'installation vous devez configurer vos browsers et clients ftp. Il existe une très bonne documentation et des tests en ligne. Le site de JAP est http://anon.inf.tu-dresden.de/index_en.html. le logiciel existe en allemand, anglais et français.

et enfin le dernier outil pour surfer de façon anonyme est AnoNet, un browser gratuit pour windows, téléchargeable sur http://www.wettenberg-online.de/download/anon.exe et dévéloppé par http://aborange.de

plus de liens concernant la sécurité et la protection de la vie privée peuvent être trouvés sur http://419scambuster.cjb.net/. des informations sur les lois et le dévéloppement du sujet en france sont disponibles sur http://vie-privee.org

INFO WEBHOSTING. un dernière information importante: chaque site que vous hostez dans les domaines .com, .org, .net, .fr, .info, .biz et bien d'autres est référencée avec nom et adresse de la personne qui enregistre cette page, parfois même avec nom et adresse de la personne qui paye ce hosting. vérifiez pour des pages dont vous avez toujours voulu savoir qui les fait ;) sur: http://whois.worldsearch.com. désormais il est des fois quand même possible de donner de fausses informations, juste pour dire: faut pas tout croire ce qui est écrit dans les whois.

FOR FURTHER QUESTIONS ASK YOUR LOCAL GEEK.

Utilisez les logiciels présentés prudemment, ne spammez pas le monde, vérifiez les circonstances juridiques concernant l'utilisation de ces logiciels dans votre pays, même si, à priori, tout est complètement légal au moment où cette brochure apparaît.

LE INFORMATION N'A PAS DE PRIX.

soutenez la personne qui a imprimé ce fly si vous le pouvez. si vous voulez traduire ce texte n'hésitez pas.

ctrl Z 02/2004

PETIT GUIDE POUR LA SECURITE ET LA PROTECTION DE LA VIE PRIVEE SUR LE NET à l'aide du non-geek

