

Internet : Le Web possède une mémoire d'éléphant, Danger

Internet

Posté par : JerryG

Publié le : 22/12/2008 0:00:00

La démocratisation de l'ADSL même au fin fond des campagnes, permet à tout un chacun de surfer et de partager ses connaissances sur le Net, mais **attention nous ne sommes pas des fantômes, nous laissons des traces indélébiles sur la toile qui au moment voulu saura les restituer à tort ou à raison.**

La grande mode du Web se veut aux réseaux sociaux, aux blogs, aux Forums de discussion et à bien d'autres choses encore, qui au fil de notre surf laisse nos empreintes, nos identifiants, nos photos et tout une foule de renseignements personnelles, professionnels et privés aux yeux de tous, attention Danger.



Sur le Web, il n'y a pas de frontières gardées avec des miradors et tout un chacun circule librement sans montrer patte blanche, mais cette libre circulation a un prix, celle de nos traces laissées sur les sites Web car entre notre vie privée et notre vie publique, le Web ne fait pas de différence.

Ainsi lors d'une visite sur un site Web, bien souvent on accepte les Cookies, des espioniciels comme on les appelle, mais ici pas de grands dangers, si ce n'est celui d'une pluie de spams bien ciblées qui va engorger notre BAM (Boîte A Mails).

Pour éliminer ces indiscrets, nettoyez votre PC via des logiciels tiers à l'instar de CCleaner, qui fera le ménage pour vous, ou des outils contenus dans Windows et mieux encore ceux contenus dans la dernière mouture des Editions-Profil, BitDefender Total Security 2009.

Si certains tentent souvent de naviguer en toute discrétion, pas facile de le faire, laissez un commentaire dans un forum, Tchatez sur un News-Groupe et laissez libre cours à votre verve et vous voilà fichés à jamais, tant par vos opinions que par vos réflexions

Le risque, à long terme, est la perte de la notion même de vie privée, expliquent les experts comme **Olivier Iteanu**, auteur de L'Identité numérique en question (Éd. Eyrolles), qui prône la création d'un droit à l'anonymat sur le Web.

Nos interventions, ou celles de nos amis, sur la Toile peuvent nous rattraper après des années.

Ainsi nos bons copains qui publient sur Face-book ou MySpace des images d'une fête bien arrosée, nous cause du tord. Bien sûr il n'y a rien d'illégal dans la mesure où la personne ne s'est pas opposée à cette communication et que le droit à l'image ait été respecté..

Selon une étude britannique, **37 %** des 18-24 ans (dixit **Le Particulier**) postent des photos de tiers sans leur consentement. Les générations à venir s'apprêtent innocemment à être entièrement fichées. Les jeunes se dévoilent aujourd'hui sans avoir conscience que, plus tard, leur futur employeur se renseignera sur eux via le réseau Facebook/MySpace. Ce que font déjà un tiers des recruteurs.

Inutile alors de recourir à des fichiers supplémentaires comme Edwige, nos amis et nous-même facilitons la tâche des besogneux de la police secrète.

Sachez qu'il est très difficile d'effacer ses traces sur le Net, comme ses réflexions personnelles ou ses prises de positions, sans parler de sa photo, bien souvent toutes ces informations sont stockées sur des serveurs étrangers (USA).

Certaines sociétés demandent même à leurs salariés d'éviter les réseaux sociaux, pour une parfaite confidentialité de leur fonction, ce qui évitera à des clients de ladite société et/ou des concurrents de se renseigner sur les compétences du salarié.

Les moteurs de recherches comme Google, Yahoo, MS-Search et les autres gardent en mémoire vos requêtes, d'ailleurs à ce propos de nombreuses associations demandent depuis des années à Google et aux autres de restreindre la rétention de données pour une meilleure transparence et un respect de la vie privée.

A titre d'exemple, Yahoo a collecté **110** milliards d'informations, soit 810 par individu, de quoi connaître une personne de A à Z et de 0 à 9.



Bien sûr, il existe un gendarme qui entend faire cesser ses rétentions de données, c'est la **Cnil**, qui dans son combat contre les géants du Web a obtenu que ces dites informations sur les internautes ne soient stockées que pour une durée de 18 mois en lieu et place des 30 ans couramment observés.

Il est aussi possible d'obtenir l'effacement de ses données via des entreprises spécialisées

contre monnaie sonnante et trébuchante ou en faire la demande aux sites concernés.

Alors pour surfer, Tchater en toute quiétude, adoptez un **pseudo** et utilisez un site plate-forme que l'on nomme "anonymiseur" une espèce de barrière qui ne livre pas votre adresse IP et ne laissez jamais vos noms, adresses, numéro de téléphone au grand jour.

Pour les paranos de la sécurité, Microsoft propose un logiciel gratuit d'encryptage des données (Microsoft Private Folder), mais ce logiciel est interdit en entreprise.

Petits conseil d'amis pour éviter le pire:

1^{er}) Lorsque vous faites suivre un message, après avoir fait un clic gauche dans la case « Transmettre », c'est ce que vous devez faire disparaître tous les Noms et les Adresses Email des personnes qui ont reçu le message. Vous les « noircissez » et les supprimez avec la touche « Suppr », ou si vous préférez, effacez lettre par lettre, en reculant progressivement. Toutes les manières sont bonnes, mais il est IMPERATIF de faire disparaître les noms et adresses de tout autre personne que vous, et celui à qui vous envoyez le message.

Seul le texte ou bien le « Lien » à re-transmettre doit figurer sur la page, Vous pouvez y ajouter votre propre texte, par ex. : Bonne Journée, et votre Signature, mais encore une fois il est essentiel de faire disparaître tous les noms et adresses Email des personnes qui apparaissaient précédemment sur cette page.

2nd) Lorsque vous faites un envoi groupé de Mails à plusieurs personnes, d'abord, vous avez intérêt à constituer un « groupe » dans votre carnet, mais surtout, ne positionnez pas vos adresses dans la case « A » ou « Cc », mais prenez plutôt l'habitude d'employer la case « Cci » (Copie Carbonne Invisible) d'nommée quelque fois « Bcc ».

De cette manière, seule la personne à qui vous écrivez verra son Nom et son Adresse, mais pas celles des autres. Personne ne pourra relever ces adresses. Il est évident que si vous désirez que les destinataires soient tous au courant des personnes à qui vous adressez ce message, n'utilisez pas cette disposition, mais soyez conscient qu'elle comporte un risque;

3rd) Dans la ligne « Sujet », enlevez toutes abréviations telles que « FW » ou « Réf » ou « Rép » ou autres, mais par contre, vous pouvez renommer le sujet si vous le désirez. Dans la ligne « pièces jointes » vous pouvez en supprimer certaines que vous ne voudriez pas envoyer et surtout la fiche « contact Outlook » de votre précédent correspondant qui pourrait y figurer.

4th) Utilisez toujours le bouton « Transmettre », de la page sur laquelle vous lisez votre message, vous éviterez ainsi à votre correspondant d'avoir à passer en revue toutes les autres pages adressées précédemment.

5th) Avez-vous reçu un Mail sous forme de pétition ? Il y a une liste de noms, et l'on vous demande d'y ajouter le votre en dernier et de re-transmettre ce message à 10 ou 15 personnes de votre carnet d'adresses. Ce Mail pourra être re-transmis et re-re-transmis à l'infini, et réunir ainsi des centaines de Noms et d'Adresses Email. En fait cette pétition vaut quelques Dollars ou quelques Euros pour un professionnel des « SPAMS » à cause des Noms et Adresses Email « VERITABLES » qui la composent.

Si vous désirez vraiment défendre cette pétition, faites une lettre personnelle à son initiateur, celle-ci aura plus de poids qu'une liste de noms, qui peut être inventée de toutes pièces, mais comme par hasard, le nom et adresse de l'initiateur n'y figure jamais...

Ne croyez pas lorsqu'il est écrit que ce Mail sera repris utilement par telle ou telle Station :

C'est impossible si l'on n'envoie pas de copie directement à la Station mentionnée.

6°) Le message le plus détestable est celui qui vous demande d'envoyer votre Email à 5, 10, ou 15 personnes, et que si vous le faite, il vous arrivera un bienfait quelconque, ou alors que vous verrez apparaître quelque chose sur votre écran, ou bien encore que vous recevrez carrément une caisse de champagne ! Soyez certain que rien de cela n'arrivera !.

Ce genre de Mails revient régulièrement chaque année ! Une seule attitude à avoir :

Destruction immédiate sans compromis.

7°) Avant d'envisager de faire suivre un message d'alerte sur un quelconque Virus, une recherche de personne, ou la propagation d'une histoire à dormir debout, il y a un [site Internet en France à consulter impérativement](#) :

Ce site répertorie, analyse et informe sur la véracité du contenu de ces messages :

VRAI ou FAUX !!!

S'ils sont réels, vous pouvez les faire suivre si vous le désirez, mais avec les précautions élémentaires prises au début de ce texte.

8°) Attention aux pièces jointes que vous envoyez, celles dont la référence de fichier se terminent par : « .exe », sont les plus vulnérables et souvent détruites d'office par un bon nombre d'antivirus. Si vous êtes certains de leur « bonne santé » et que vous vouliez impérativement les faire parvenir à quelqu'un, prenez la précaution de « Zipper » votre dossier, qui voyagera ainsi en toute sécurité !

Fort de cet enseignement, vous serez alors, quasiment invisible, enfin presque !

[**Plus d'info sur Le Particulier**](#)