



Comment se protéger, les dangers, ce qu'il faut savoir.....

Dès que vous êtes connecté..... on vous espionne !!!!

Attention aux informations qui sont collectées lors de vos connexions à Internet (adresse électronique, centres d'intérêt, sites et pages visités...) Ces informations servent souvent à alimenter les fichiers d'entreprises commerciales (vos habitudes sont une mine d'or pour ceux qui veulent faire une étude de marché)

Si en quelques clics, vous pouvez vous rendre sur n'importe quel site, télécharger des fichiers, participer à des "groupes de discussion".. ; Toutes ces activités laissent des traces.

Comment cela se fait il ?????

Chaque fois que vous vous rendez sur un site, votre navigateur (Internet Explorer, Netscape, Firefox...) lui communique l'adresse IP (Internet Protocol), l'identifiant de votre connexion au réseau Internet. Ce numéro IP permet de connaître votre fournisseur d'accès, les caractéristiques de votre ordinateur, etc.

Par ailleurs, dans la "mémoire cache" de votre ordinateur sont stockées les données auxquelles le système fait le plus souvent appel, ce qui permet de réduire les temps d'attente du microprocesseur. Ce sont souvent les images volumineuses de certains sites. La "mémoire cache" garde aussi la trace de tout l'historique de votre navigation sur le Web.

Cela signifie par exempleque

Dans un cybercafé, l'utilisateur suivant peut ainsi voir quels sont les sites que vous avez consultés.

Tous les propos que vous avez tenus sur les forums de discussion sont archivés et accessibles.

Les moteurs de recherche des "newsgroups" permettent de retrouver toutes les interventions de tous les internautes.

CONCLUSION..

Pour participer à des débats sur la politique, la religion ou la musique, mieux vaut donc utiliser un pseudo, car n'importe qui peut collecter des précisions sur vos centres d'intérêt et obtenir un profil de votre personnalité.

les "cookies" c'est quoi ça !!!!!

Lorsque vous vous connectez à Internet, des fichiers d'informations "cookies" - sont enregistrés et stockés, sur votre ordinateur par votre navigateur à la demande du site Web que vous visitez.

Ils permettent de vous attribuer un profil, le temps de la connexion ou parfois indéfiniment. Ils peuvent contenir vos pseudonymes et mot de passe, un numéro de session (pour conserver le contenu de votre "panier" d'achat virtuel) ou des informations que vous avez transmises au cours d'une commande (numéro de carte bancaire, centres d'intérêt...).

Ces fichiers sont très utiles pour mémoriser vos achats sur un site marchand, mais leur contenu peut être utilisé à des fins commerciales, pour vous adresser de la publicité ciblée par exemple. (SPAM)

Adware , spyware , keylogger.... Qu'est ce que c'est que ces machins là !!!!

Plus dangereux et illégal, l'"adware" est un logiciel qui s'installe, souvent à votre insu, en même temps que vous téléchargez, entre autres, des programmes gratuits. Il délivre des informations personnelles (sites visités, liste de vos logiciels, centres d'intérêt...) à un serveur distant qui alimente les fichiers d'agences spécialisées dans le marketing.

Détourné de cette finalité par une entreprise ou un individu malhonnêtes, l'"adware" devient un "spyware", qui vole des données sensibles comme le numéro de licence d'un logiciel ou le code d'une carte bancaire.

Vous pouvez également être victime d'un "keylogger ", un logiciel qui enregistre toutes vos frappes au clavier. Sa fonction est de mémoriser vos pseudonymes et vos mots de passe pour les transmettre à un pirate.

Oups.....mais que faire ????

La première précaution consiste à utiliser la version récente d'un navigateur.. Les dernières versions bloquent les "pop-up", ces fenêtres publicitaires qui apparaissent à l'ouverture d'une page Web.

Dans le menu "Préférences" du navigateur, on peut vider l'historique de navigation, supprimer les "cookies", limiter la capacité de stockage de la "mémoire cache" et la vider complètement.

Il est primordial d'équiper votre machine de versions à jour de logiciels antivirus et pare-feu qui bloquent les "spywares" et les "adwares".

Pour augmenter la protection, on peut installer sur son ordinateur un "proxy d'anonymat" (par exemple, Provoxy), un logiciel qui supprime toutes les informations nominatives que l'utilisateur laisse fuir sur Internet sans le savoir.

Il faut bien réfléchir avant d'installer des outils destinés à améliorer les fonctionnalités des moteurs de recherche (Yahoo barre, Google barre...) ou certains logiciels gratuits de source inconnue. Lorsque l'on reçoit des courriels indésirables, il faut jeter la pièce jointe à la poubelle sans l'ouvrir.

Quid de la messagerie ????

Il est préférable de créer deux adresses, une privée et une publique, car cela permet de filtrer les messages non souhaités. L'adresse publique, qui sert à acheter en ligne, à discuter sur les forums, est souvent capturée. Aussi, n'utilisez votre adresse électronique personnelle que pour votre correspondance privée et vos connexions importantes (impôts, banque en ligne...).

Ces quelques conseils ont été repris de divers sites spécialisés. J'ai résumé tout ceci pour que cela ne soit pas trop ardu. Sans entrer dans les détails, il faut être conscient que si Internet est un super outil, c'est également un moyen très efficace pour les pirates de détourner vos données. Il suffit de prendre conscience de cela et de se montrer un peu prudent pour limiter les risques....

GF . Webmaster provincial.