INTERNET

MENU :

1. Structure physique d'Internet

Pour fournir des services comme le mail ou le surf sur Internet, un ensemble d'ordinateurs (machines dédiées à cette tâche) appelés « serveur » est mis en place et maintenu par des sociétés spécialisées. Par exemple, pour être accessible pour vous (client), un site web doit être hébergé sur un « serveur web » quelque part dans le monde .

2.SPYWARE :

Parmi les menaces les plus répandues sur Internet, les « spywares » figurent en bonne position. Comme son nom l'indique, un **spyware** est un petit logiciel (« ware » pour software) espion (spy) qui s'installe sur votre ordinateur à votre insu.

Ces logiciels sont souvent utilisés par les grands groupes à des fin marketing car cet outil leur permet de rassembler une multitude d'informations sur le comportement du consommateur (l'internaute) que vous êtes. Ainsi, périodiquement le logiciel va transmettre à son propriétaires une variété d'informations concernant votre utilisation d'Internet et de l'informatique en général : pages favorites, fréquence de connexion, durée moyenne des sessions de connexions, logiciels installés sur votre ordinateur. tout y passe. Ce transfert d'informations à la base de données de l'entreprise qui vous espionne participe donc à expliquer le ralentissement constaté par certains internautes sur leur connexion

3. Nettoyer le système en supprimant les spywares :.

Pour ce faire il vous faut installer des anti-spyware qui sont des logiciels spécialisés dans la désinfection des machines et la suppression des logiciels espions. Les anti-spywares fonctionnent tous sur le même principe, celui des bases de données. En effet, comme pour les anti-virus, le logiciel scanne un certain nombre d'endroits de votre machine en comparant leur contenu à une base de données qui recense tous les spywares connus. De ce fait, pour assurer le bon fonctionnement des anti-spywares et donc une protection optimale, il faut régulièrement mettre à jour cette base de données comme cela est le cas pour votre anti-virus.

Il existe un grand nombre d'anti-spywares , il est conseillé d'utiliser deux outils reconnus et testés pour leur efficacité j'ai nommé

Ad Aware SE et SpyBot Search&Destroy .

J'ai Ad-Aware dont la version SE est freeWare (gratuite)

J'ai aussi SpyBot Search&Destroy.

4. LES INTRUSIONS :

Autre risque majeur d'Internet, les intrusions sont le fait de personnes mal intentionnées appelées de manière génériques « pirates ». Il y a plusieurs niveaux d'intrusions,. les intrusions non destructrices qui ne consistent qu'à s'introduire dans un système pour y consulter des fichiers ou en prendre le contrôle, les intrusions destructrices qui causent la perte partielle ou totale des fichiers de la machine victime de l'intrusion et les intrusions destructrices de hardware souvent le disque dur

Pour vous prémunir de ce genre d'attaques, il s'agit d'abord de comprendre comment de telles intrusions sont possibles. Il existe principalement deux moyens de s'introduire dans un ordinateur distant via Internet : utiliser une porte dérobée préalablement ouverte par un petit logiciel appelé cheval de troye ou troyen (Trojan) que le pirate a réussi à installer sur la machine, attaquer directement la sécurité du système d'exploitation ou d'un logiciel (typiquement Internet explorer) et y exploiter une faille de sécurité.

Il importe donc de bien vérifier l'absence de chevaux de troye sur votre machine et de bloquer les portes d'accès de celle-ci en installant un mur de feu plus communément appelé « firewall ». D'ailleurs, Windows XP dans sa dernière version (Service Pack 2) intègre un tel logiciel en standard, il suffit donc d'en activer le fonctionnement. Malgré que ce dernier soit largement suffisant pour une utilisation de base, l'utilisateur averti pourrait vouloir se doter d'une solution plus pointue comme **Zone Alarm Pro** (programme sous license) .
Certains fournisseurs d'accès fournissent (en payant) des FireWall.
Comme son nom l'indique, un firewall va dresser un mur aussi bien à l'entrée qu'à la sortie de votre ordinateur en contrôlant les flux d'échanges de données depuis et vers Internet, vous serez alors averti de tout échange suspect et votre décision de bloquer ou non l'opération sera demandée.

5.Les virus et assimilés :

Parmi toutes les menaces d'Internet, les virus sont certainement les plus connus car les plus médiatiques. Signalons d'abord que les infections virales ne sont en aucun cas spécifiques à Internet et n'importe quel support (tel Clé USB , CD , DVD ….) infecté peut transmettre le virus, Internet n'étant qu'un des moyens privilégiés de propagation dudit virus, contrairement aux autres menaces qui elles sont bien plus spécifiques à la toile mondiale.
Il existe aussi une grande diversité de virus qui n'a pas de véritable intérêt pour l'utilisateur débutant. Ce qu'il vous faut savoir c'est qu'un virus est avant tout un petit programme informatique dont la finalité n'est jamais bien intentionnée qui vise à se répandre sur un maximum de machines. Ils sont dans plusieurs cas le fait de petits génies de l'informatique qui les conçoivent plus par défi que par envie de faire du mal à l'utilisateur final, la cible étant plutôt les éditeurs de systèmes d'exploitation qui se battent pour défendre la sécurité de leur systèmes et finissent parfois par embauches les auteurs de virus ayant connu le plus de succès. Au centre de cette guerre technologique, se trouve l'utilisateur et les éditeurs de logiciels anti-virus.

Le Premier n'y connaît pas grand chose et souhaite pouvoir utiliser son ordinateur sans encombres et sans perdre ses données (certains virus détruisent les données), les éditeurs eux proposent des solutions anti-virales et ont tout intérêt à ce que les virus

continuent à faire peur pour vendre leurs logiciels, d'ailleurs certains les accusent d'être eux même producteurs de virus qui leur assurent la prospérité du business !

Pratiquement, pour se protéger il faut disposer d'un antivirus mais surtout d'un antivirus dont la base de données est à jour. Parmi les solutions les plus populaires nous citerons l'excellent McAfee, le très utilisé Norton Antivirus, PC cillin, AVG antivirus , Avast.

J'ai Avast.

6. Problème de Avast sous Vista :

Avast est constitué de plusieurs modules .
Si on perd l'accès à internet au bout de quelques minutes , il y a conflit entre un module de Avast et Windows.
Ouvrir Avast
Rechercher le module (service installé) **Bouclier Web** , et cliquer sur terminer.

Pour les autres modules j'ai la sensibilité élevée.

7. AD-Aware Pro :

En plus de la version de base , il comporte le module Ad_Watch
Ce module demande une autorisation avant de modifier une zone sensible du PC.
Cela évite des modifications à notre insu.
Mais contrairement à la version SE , la version Pro est sous licence (à payer)

8. Organiser ses favoris :

Il est intéressant de mémoriser l'adresse d'un site.
Pour cela on peut le mettre dans ses favoris Intenet
Quand on est sur la page d'accueil du site (ou une page qui nous intéresse) cliquer sur Favoris
Et on peut enregistrer l'adresse du site.

Mais il est conseillé de ne pas les enregistrer n'importe où (difficulté pour les retrouver) , mais par thème (comme le bureau etc….)
Quand on clique sur Ajouter aux favoris , cliquer ensuite sur Créer dans , puis choisir le thème.
Si le thème n'existe pas , cliquer sur nouveau Dossier et alors donner un nom à ce dossier.
Puis ajouter le favori en lui donnant un nom évocateur.
Nota : on peut aussi faire des sous-dossiers

L'explorateur permet aussi d'organiser ses favoris (déplacer , renommer , supprimer)
De temps en temps il faut faire le ménage.

9. NETTOYER INTERNET EXPLORER :

Quand on navigue sur Internet, on intercepte beaucoup d'informations qui sont stockées par l'ordinateur. Ces informations sont:
- des cookies
- des adresses internet visitées (URL)

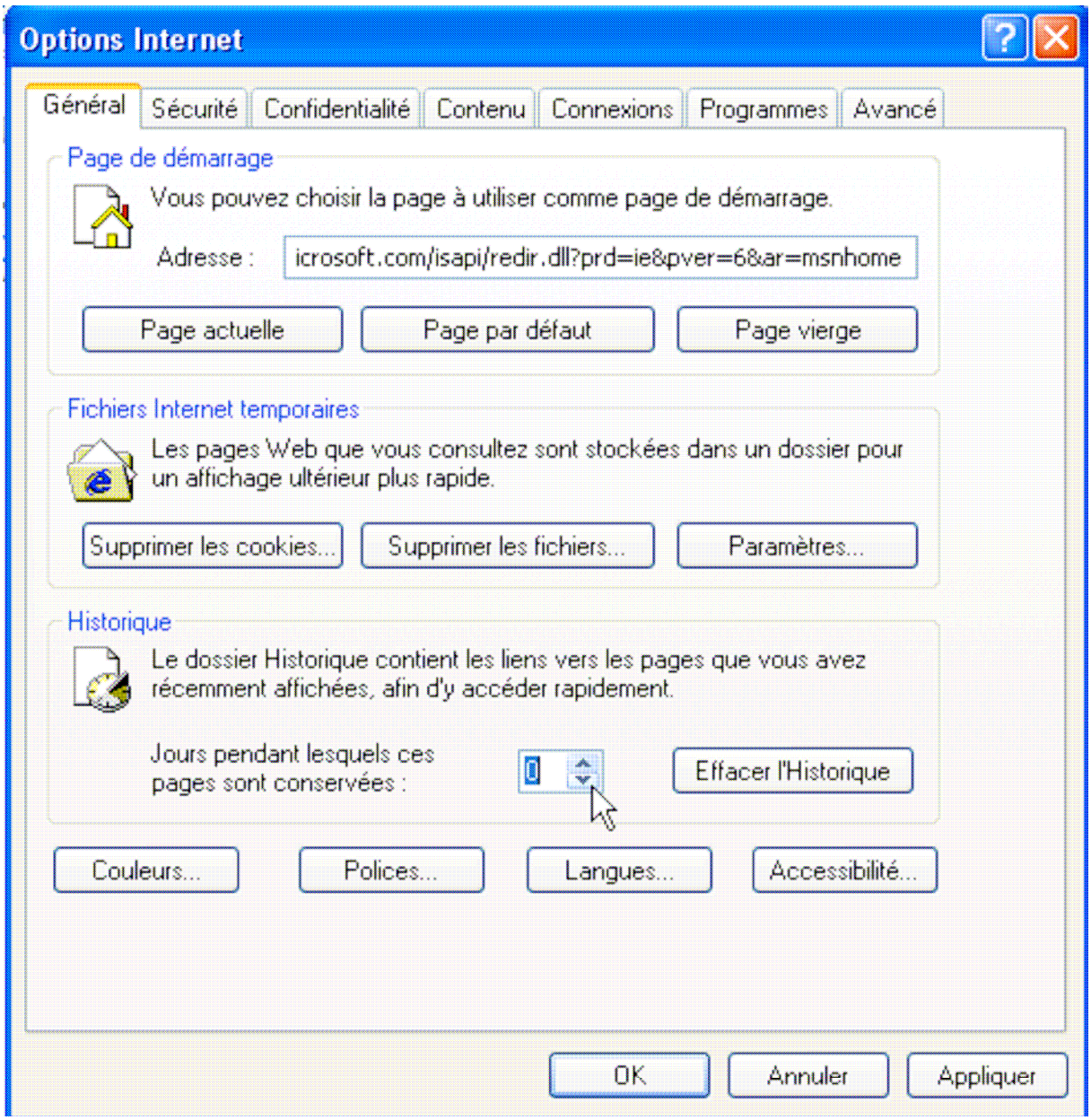
Ces informations sont mémorisées dans le fichier "Temporary internet files" (Fichiers temporaires internet). En plus des activités sur Internet, notre ordinateur crée des fichiers temporaires lors des sessions sous Word®, Excel® et d'autres logiciels (programmes). Ces informations sont mémorisées dans le fichier "Temporary files" (fichiers temporaires). Avec le temps, ces deux fichiers gonflent et occupent de l'espace superflu sur le disque dur. L'ordinateur ralentira, sa puissance de travail sera réduite!

Pour remédier à cette action, nous devons faire la maintenance de l'ordinateur

Pour Cela dans l'explorateur Internet :
Outils
Supprimer l'historique de navigation
Tout supprimer (ou bien suppression sélective par les différents boutons de suppression)

On peut aussi faire ce ménage avec Ccleaner et Glary Utilities

Afin de ne pas avoir trop de mémoire gaspillée,
régler l'historique à *0 jours*.
Dans IE , outils , Options Internet et cliquer sur le bouton paramètres de Historique de Navigation.



10 . LE PHISHING

De nos jours les internautes s'exposent à un nombre infini de dangers, parmi lesquels on compte le phishing.
C'est quoi le "*phishing*"?
Le phishing, appelé encore "*hameçonnage par courrier électronique*" désigne une forme d'escroquerie en ligne qui a pour but d'obtenir par Internet et par des moyens détournés, en trompant la vigilance des utilisateurs, des informations personnelles et confidentielles telles que des informations relatives aux comptes bancaires et aux codes de cartes bancaires.

Comment cela fonctionne-t-il ?
Les internautes sont avertis par courrier électronique falsifié que leur compte bancaire et/ou leur compte chez un vendeur (par exemple Ebay) ne fonctionne plus correctement dû à une panne du système informatique.
Un autre truc consiste à faire croire que les coordonnées de facturation du vendeur sont périmées et qu'on doit saisir à nouveau les données endéans les 24 heures, autrement le compte sera éliminé (comme montré dans la figure ci-dessous)!
Le courrier électronique contient toujours un lien sur lequel on demande de cliquer pour arriver au site d'administration qui, à première vue, est tout à fait semblable au site web original et qui en plus fait croire qu'il s'agit d'une connexion sécurisée en indiquant le début du lien avec **https://**.
Ce que vous ne voyez pas (si vous n'avez pas installé de **barre antiphishing**) c'est que (l'adresse IP) **l'URL est différente**!
Si maintenant on saisit les données dans les champs de texte (**User ID et Password**), le criminel informatique les intercepte et réagit instantanément.
Dans le cas de ce vendeur il aura les coordonnées d'accès et il pourra faire autant d'achats que possible qui seront facturés aux utilisateurs ainsi attaqués!
Le site truqué n'est en principe opérationnel que pendant 24 heures et hébergé la plupart du temps sur des serveurs en Russie et Ukraine, ce qui rend très difficile et/ou presque impossible de le retracer et de prouver son existence.

Comment se protéger contre le phishing?
D'abord une bonne portion de vigilance (méfiance) est de rigueur; c.-à-d.: aucun établissement, qu'il soit bancaire et/ou gouvernemental, ni commercial n'enverra par courrier électronique une telle demande pour renouveler des données confidentielles!
Ces actions, pour garder la confidentialité et la protection de la vie privée, se font d'office par courrier normal!

11. OPTIMISER SES RECHERCHES SUR INTERNET

Utiliser un moteur de recherche, c'est bien, apprendre à s'en servir, c'est parfois une question de survie si vous ne voulez pas être submergé par un flot de réponses ou vous égarer dans des voies sans issue. Alors que faire pour atteindre rapidement votre cible ? Nous vous rappelons ici quelques précautions élémentaires à observer pour gagner du temps qui marchent avec Google et tous les autres moteurs :

- **Bien penser au(x) mot(s)-clé(s)** avant de vous lancer dans une recherche, la qualité des réponses dépend d'abord de la qualité des mots choisis. Par exemple, "tabac" ne donne pas les mêmes résultats que "cigarette" : le premier est plus synonyme de danger pour la santé tandis que l'autre symbolise plus le plaisir de fumer.

- **Taper les mots en minuscule** pour vous donner toutes les chances de ne pas manquer une référence importante.

- **Faites attention à l'ordre des mots** que vous utilisez. Sur certains moteurs, cette occurence a son importance; Exemple, "paris dakar" ne donne pas le même résultat que "dakar paris".

- **Utilisez les guillemets** si votre recherche comporte plusieurs mots : taper par exemple "mairie de paris" afin que le moteur prenne bien en compte tous les mots.

- **Utilisez la syntaxe pour affiner votre recherche** : les outils les plus couramment utilisés sont les "+" et les "-" qui ajoutent des contraintes à votre recherche. Par exemple, vous pouvez rechercher des documents sur George Lucas qui ne parlent que de Star Wars (george lucas +star wars) ou au contraire qui ne parlent pas du film (george lucas -star wars).