

# PROGRAMME D'ACCÈS COMMUNAUTAIRE



## **ATELIER SUR LA PROTECTION D'UN ORDINATEUR** *(LES DANGERS DE L'INTERNET)*

---

**PAR JEAN RENAUD**  
*(MISE À JOUR EN JANVIER 2004 PAR ANN JULIE DESMEULES)*

## **TABLE DES MATIÈRES**

### **CHAPITRE 1 – LES LOGICIELS ANTIVIRUS**

SECTION 1 – DESCRIPTION DES TYPES DE VIRUS

PARTIE A - VIRUS DE SECTEURS D'AMORÇAGE

PARTIE B - VIRUS EXÉCUTABLES

(PARTIE C) – VIRUX MACRO

SECTION 2 – SCANNER UN FICHER

SECTION 3 – METTRE À JOUR LES SIGNATURES D'ANTIVIRUS

### **CHAPITRE 2 – LES LOGICIELS PARE-FEU (FIREWALL)**

SECTION 1 - QU'EST-CE QU'UN PARE-FEU?

SECTION 2 - LES TYPES DE PARE-FEU : LOGICIEL ET MATÉRIEL

SECTION 3 – SITES OÙ IL EST POSSIBLE D'AVOIR UN FIREWALL GRATUIT

SECTION 4 – UTILISATION DES FIREWALLS

SECTION 5 – SITES QUI TESTENT LES ORDINATEURS

### **CHAPITRE 3 – MISES À JOUR DES LOGICIELS**

### **CHAPITRE 4 – LES SPYWARES / ADWARES / COOKIES**

SECTION 1 – RETIRER LES SPYWARES AVEC SPYBOT

PARTIE A – TÉLÉCHARGER SPYBOT S&D

PARTIE B – INSTALLATION DE SPYBOT S&D

PARTIE C – PREMIÈRE EXÉCUTION DE SPYBOT S&D

PARTIE D – MISE À JOUR DE SPYBOT

PARTIE E –UTILISATION DE SPYBOT

SECTION 2 – RETIRER LES SPYWARES AVEC AD-AWARE

SECTION 3 – CONFIGURER LA GESTION DES COOKIES

PARTIE A – CONFIGURER LES COOKIES DANS  
INTERNET EXPLORER 6

PARTIE B – CONFIGURER LES COOKIES DANS  
NETSCAPE

### **CHAPITRE 5 –LES ATTRAPES SUR INTERNET**

### **CHAPITRE 6 – COMMENT EMPÊCHER LE POURRIEL**

SECTION 1 – QU'EST-CE QUE LE POURRIEL

SECTION 2 – LA NOUVELLE MENACE : LES WEB BUGS

### **CHAPITRE 7 – LE « PARENTAL CONTROL »**

SECTION 1 – QU'EST-CE QUE LE PARENTAL CONTROL ?

SECTION 2 – POURQUOI LE CONTRÔLE PARENTAL ?

SECTION 3 – COMMENT FONCTIONNENT LES LOGICIELS DE FILTRAGE?

SECTION 4 – COMMENT BIEN UTILISER SON LOGICIEL DE FILTRAGE ?

SECTION 5 – SITES SUGGÉRÉS POUR LE TÉLÉCHARGEMENT GRATUIT  
D'UN PROGRAMME DE « CONTROL PARENTAL »

## CHAPITRE 1 – LES LOGICIELS ANTIVIRUS

La plupart des personnes, même si elles ne sont pas vraiment expertes en informatique, savent toujours en gros ce qu'est un antivirus, soit un logiciel permettant de détecter les virus informatiques qui peuvent arriver sur nos ordinateurs. Les virus sont des petits programmes parasites qui s'accrochent à un fichier exécutable et qui se reproduisent dans les fichiers et la mémoire de nos ordinateurs, lorsqu'on exécute le programme exécutable infecté.

Les virus peuvent toutefois être la source de peurs injustifiées. Certaines personnes pensent que des virus peuvent arriver par courrier Internet et infecter l'ordinateur avant même qu'on ait fait quoi que ce soit; d'autres pourraient penser que les virus sur une disquette se propagent dès que la disquette est insérée. Mais cela est faux. Un virus contamine un objet, et il faut utiliser l'objet pour que le virus se transmette. Nous allons donc expliquer quels types de virus existent, et comment les déceler.

### SECTION 1 – DESCRIPTION DES TYPES DE VIRUS

#### (PARTIE A) - VIRUS DE SECTEURS D'AMORÇAGE

Dans le passé, certains ordinateurs avaient besoin d'une disquette pour démarrer. Quand un ordinateur a une disquette lors de son démarrage, il va lire une partie au début de la disquette qu'on appelle « Secteur de démarrage ». Des virus ont alors été créés pour prendre avantage de ce procédé. Lorsque l'ordinateur lit le secteur de démarrage de la disquette, il exécute le virus, et celui-ci va alors se copier sur le secteur de démarrage du disque dur. Mais aujourd'hui, les disquettes sont rarement utilisées pour démarrer un ordinateur, alors ce type de virus est de moins en moins présent. Le fait d'insérer une disquette dans l'ordinateur lorsque Windows est démarré ne contamine pas le disque, ni le fait de transférer des fichiers de la disquette vers l'ordinateur.

#### (PARTIE B) - VIRUS EXÉCUTABLES

Ce type de virus est l'un des plus présents aujourd'hui. Ce type de virus contamine plusieurs fichiers d'applications, comme les fichiers finissant par .EXE, .COM, et tous les autres fichiers que ces .COM ou .EXE exécutent. Lorsque le virus va être exécuté, il va attendre que vous lanciez d'autres applications pour les contaminer.

Ainsi, ce type de virus n'est dangereux que si on exécute le fichier concerné. Ainsi, un fichier infecté ne fera aucun mal si l'application n'est jamais démarrée.

#### (PARTIE C) - VIRUS MACRO

Ce type de virus est apparu avec l'avènement de certains logiciels de bureautique. Ces logiciels créent des types de fichiers qui contiennent une petite partie de code. Ce code peut alors être modifié par un virus, et le logiciel de bureautique va « Retenir » le virus. Chaque document qui sera ouvert par la suite sera infecté. Les fichiers .TXT et .RTF ne peuvent pas être infectés.

Si un document infecté n'est pas ouvert, le code ne s'exécutera pas.

## SECTION 2 – SCANNER UN FICHIER

Un antivirus, comme la plupart des gens le savent, est conçu pour scanner les fichiers au moment où on les exécute et où on les ouvre. Théoriquement, l'antivirus devrait être en mesure d'arrêter les virus avant qu'ils ne s'exécutent. Cependant, avec la création de plusieurs nouveaux virus à chaque jour, un nouveau type de virus pourrait être juste assez rapide pour déjouer l'antivirus, qui ne serait alors pas mis à jour.

Une solution pour être encore plus en sécurité est de scanner un fichier manuellement avant de l'exécuter. Par exemple, si vous téléchargez un fichier sur Internet, commencez par demander à votre navigateur d'enregistrer le fichier sur le bureau de Windows, plutôt que demander l'exécution immédiate du fichier. Lorsque le fichier est téléchargé, scannez-le avec votre antivirus; en général, lorsqu'on clique avec le bouton droit sur un fichier, un des choix du menu contextuel qui apparaît vous propose de chercher si des virus sont présents dans le fichier.

La même procédure peut être utilisée avec les logiciels de courrier électronique. Lorsque vous avez téléchargé les messages, scannez les pièces jointes avant de les ouvrir. Pour ce faire, enregistrez les pièces jointes sur le disque et scannez-les par la suite.

## SECTION 3 – METTRE À JOUR LES SIGNATURES D'ANTIVIRUS

Un antivirus, sans mises à jour, c'est comme ne pas avoir d'antivirus. Alors il est important de mettre régulièrement sa base de données d'antivirus à jour.

Aujourd'hui, la plupart des antivirus se mettent à jour automatiquement. Mais il peut être utile de vérifier si c'est le cas ou non. Pour cela, vous devez ouvrir la fenêtre principale de votre antivirus et aller dans la section de configuration de la mise à jour. Si vous ne savez pas comment, parcourez tous les menus jusqu'à ce que vous trouviez quelque chose y ressemblant. La plupart du temps, vous aurez à cocher une case pour lui dire de se mettre à jour automatiquement. Sinon, il est possible de mettre la base de données d'antivirus manuellement, en actionnant le bouton ou la commande correspondants.

## CHAPITRE 2 – LES LOGICIELS PARE-FEU (FIREWALL)

### SECTION 1 - QU'EST-CE QU'UN PARE-FEU?

Un pare-feu est un logiciel (ou pièce électronique) chargé d'empêcher l'accès non autorisé à un système informatique. Les gens responsables de ces tentatives, appelés « Pirates », exploitent des failles de sécurité d'un système pour y accéder.

La manière utilisée par le pare-feu pour bloquer l'accès à un pirate consiste avant tout à rendre le système informatique invisible. Chaque ordinateur, lorsque connecté à Internet, possède un identificateur numérique unique de type 000.000.000.000 appelé « adresse IP », et cela pour que l'ordinateur soit reconnu parmi les millions d'autres. Le pirate, lui, utilise une sorte de scanner, qui a pour effet de chercher des identificateurs commençant par certains chiffres au hasard. Si votre système a ces chiffres dans son identificateur, il va « répondre » au pirate, ce qui va inciter le pirate à attaquer. Si un pare-feu est présent sur votre ordinateur, le pare-feu va bloquer la réponse de votre ordinateur, et le pirate, n'entendant rien, va chercher ailleurs.

Bien sûr, cette section du cours n'essaie pas de vous faire peur, car les attaques sont rarement faites envers des particuliers. Mais il n'est sûrement pas mauvais de s'installer un firewall, car il sert sûrement à quelque chose... En fait, certaines personnes peuvent être plus à risque que d'autres, comme les possesseurs de modems-câble, qui restent toujours branchés tant que l'ordinateur n'est pas éteint. Mais les firewalls peuvent jouer un rôle s'écartant un peu de leur but ultime, ce que nous allons voir plus loin.

### SECTION 2 - LES TYPES DE PARE-FEU : LOGICIEL ET MATÉRIEL

Maintenant que vous savez ce qu'est un Pare-feu (firewall), il en existe en gros deux types. Les pare-feu logiciels, et les pare-feu matériels. Un pare-feu matériel est souvent un boîtier extérieur à l'ordinateur, qui sert de diviseur de connexion Internet et de mini-réseau à domicile. Un grand constructeur dans ce type d'appareil est LINKSYS. D'une certaine manière, les firewalls matériels sont plus efficaces car ils ne s'occupent que de protéger, tandis que les firewalls logiciels sont contrôlés par un ordinateur occupé par autre chose. Cependant, un firewall matériel est plutôt une dépense inutile si vous n'avez qu'un ordinateur à la maison...

Les pare-feu logiciels, eux, ont certains avantages par rapport aux pare-feu matériels. Lorsqu'une attaque est menée contre votre ordinateur, vous pouvez choisir de faire afficher une boîte de dialogue vous en informant, ce qu'un firewall matériel ne fera pas nécessairement. De plus, lorsqu'une application se trouvant sur votre ordinateur essaie de se brancher à Internet, le firewall va vous demander votre permission avant de le laisser se brancher, à l'aide d'une boîte de dialogue. Vous avez alors le choix de permettre au logiciel de se brancher ou non, et en plus, dire au firewall d'autoriser automatiquement la connexion des logiciels de confiance, qui seront notés dans une liste de « Permissions ». En fin de compte, les firewalls personnels sont en fait des « filtres » de connexion.

Cette particularité peut être utilisée pour empêcher votre logiciel de lecture de CD de trouver les informations d'un CD de musique sur Internet, car ces bases de données ont parfois des erreurs. De plus, il est possible de bloquer les spywares (voir plus loin).

## SECTION 3 – SITES OÙ IL EST POSSIBLE D'AVOIR UN FIREWALL GRATUIT

Il existe plusieurs firewalls sur le marché, certains gratuits (et tout de même efficaces), d'autres payants. Les firewalls payants sont conçus en particulier par Norton, McAfee, et d'autres compagnies; il est possible d'en trouver chez notre vendeur d'ordinateurs.

Cependant, il peut être intéressant de se trouver un firewall gratuit. Ceux-ci se trouvent sur Internet. Certains firewalls gratuits vont être meilleurs que d'autres, alors on va parler ici des plus populaires.

ZoneAlarm [www.zonelabs.com](http://www.zonelabs.com)

Ce firewall est sans doute le plus populaire à cause de sa facilité d'utilisation. Le firewall peut nous dire à quoi sert une application qui veut se connecter via leur site Internet. Cependant, il ne permet pas de personnaliser les ports par lesquels chaque logiciel peut communiquer, ce qui peut être utile dans certains cas. Version française sur le site <http://www.traductionfrancaise.fr.st>

Sygate Personal Firewall <http://soho.sygate.com/free/default.php>

Ce firewall est aussi populaire que ZoneAlarm, malgré le fait qu'il soit disponible qu'en anglais. Il contient beaucoup plus de fonctions que zoneAlarm, par exemple la particularité de spécifier par quels ports une application a le droit de communiquer. Un port est une sorte de porte électronique par laquelle les informations passent, chaque porte ayant une utilité particulière. Des informations supplémentaires sur les ports seront abordées dans d'autres chapitres.

Kerio Personal Firewall [http://www.kerio.com/fr/kpf\\_download.html](http://www.kerio.com/fr/kpf_download.html)

En anglais, ce firewall contient autant de fonctionnalités que le Sygate, sans les fonctions barrées. Ce firewall semble être plus léger pour le système, ce qui est un avantage, surtout si votre ordinateur est plus ou moins fort. Ce firewall permet de spécifier les ports par lesquels un logiciel a le droit de communiquer, comme Sygate.

Voici quelques sites qui vous donnent quelques classements de firewalls :

<http://www.inoculer.com/firewall.php3>

<http://www.framasoft.net/rubrique55.html>

<http://www.sysopt.com/reviews/firewall/>

Pour installer les firewalls, ils suffit de cliquer sur tous les boutons « Next », « Install », « Finish », « I Agree » et « Yes », ou en français « Suivant », « Installer », « Je suis d'accord », « J'accepte », « Oui », « Terminer » que l'on peut trouver...

## SECTION 4 - UTILISATION DES FIREWALLS

Lorsqu'un firewall est démarré pour la première fois, il ne sait pas automatiquement quelles applications peuvent utiliser Internet. En fait, le ZoneAlarm est le seul qui va autoriser dès le début quelques applications sans vous le demander, et encore, c'est très peu. Dans le cas des autres applications, le firewall va afficher une boîte de message vous demandant quoi faire avec l'application : La laisser passer ou la bloquer, et se souvenir de cette

décision pour ne pas devoir la confirmer à chaque fois. La fenêtre peut avoir une apparence différente selon le firewall installé, donc voici un aperçu pour chaque firewall cité plus tôt.

Les firewalls ont été testés avec le logiciel WebWasher pour vérifier leur efficacité. Voir le dernier chapitre pour une explication sur ce logiciel.

## 1 – ZoneAlarm

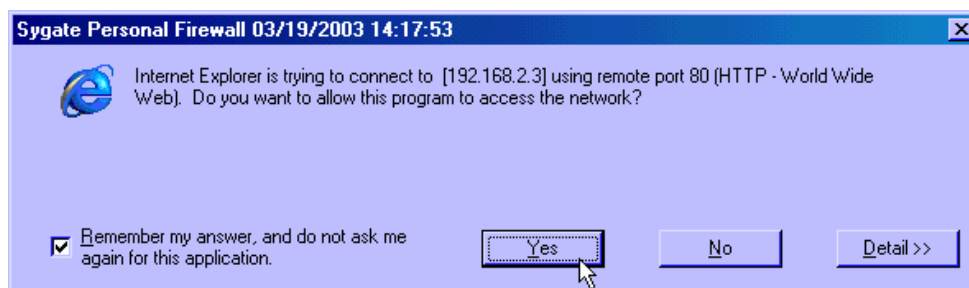
Pour avoir plus d'informations sur le programme en question, cliquez sur le bouton « Plus d'infos », ce qui vous amènera sur la page web de ZoneAlarm.

Avant de cliquer sur « Oui » pour autoriser l'accès ou « Non » pour bloquer l'accès, cochez la case à cocher « Se rappeler de cette réponse la prochaine fois que j'utiliserai ce programme » pour ne pas que la fenêtre de confirmation apparaisse à chaque fois pour l'application en question; cliquez ensuite sur « Oui » ou « Non ». Notez que ZoneAlarm voit les connexions passant par Webwasher (bien).



## 2 – Sygate Personal Firewall

Le bouton détail ne vous montrera aucune information que vous êtes en mesure de comprendre. La seule chose possible est de cocher la case à cocher pour ne pas que la question apparaisse à chaque utilisation de l'application, puis cliquer sur « Oui » ou « Non ». Ce firewall ne voit pas les applications qui se branchent à Internet via WebWasher (faille de sécurité).

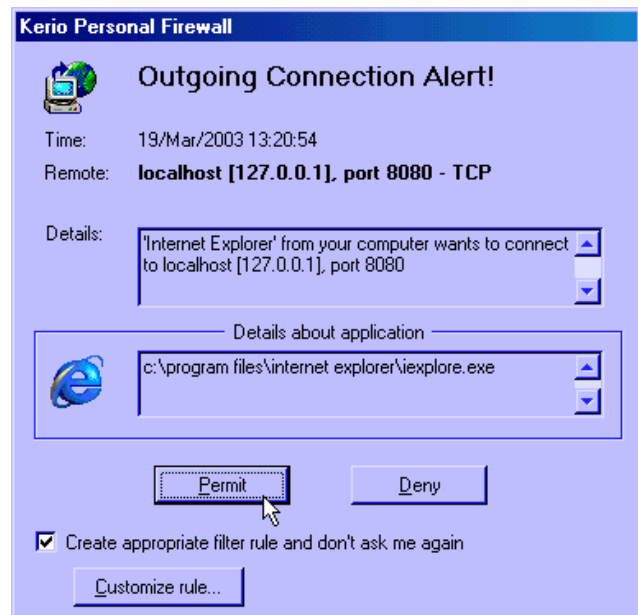


### 3 – Kerio Personal Firewall

Aucune information sur ce à quoi sert l'application interceptée. Cochez la case à cocher pour éviter d'autres questions sur l'application. Vous pouvez choisir via le bouton « Customize rule... » de cette fenêtre par quels ports vous voulez que l'application communique, ce qui peut être utile pour bloquer certains types de courrier non sollicité (voir le chapitre sur le courrier non sollicité).

Pour permettre l'accès à l'application, cliquez sur « Permit », sinon cliquez sur « Deny ».

Ce firewall détecte les applications qui se branchent à Internet via WebWasher.



## SECTION 5 - SITES QUI TESTENT LES ORDINATEURS :

Certains sites vous proposent de tester votre firewall (ou votre ordinateur SANS firewall), pour révéler certaines failles de protection. Les sites n'essaieront pas de prendre le contrôle de votre ordinateur, mais vont juste envoyer une demande de connexion à votre ordinateur (qui va refuser ou se taire), et n'essaieront pas de contourner la protection.

<http://www.pcflank.com/>  
<http://grc.com>

Si vous avez passé avec succès les tests des sites indiqués ci-dessus, vous devrez déjà faire face à la dure réalité : des gens ont déjà trouvé une manière d'outrepasser les firewalls personnels. Comme mentionné plus tôt, les firewalls personnels sont des filtres, qui laissent passer ce qui a la permission de passer, et bloque ce qui n'a pas la permission. Pour ce qui est des attaques extérieures, le procédé est efficace à 100%. Cependant, pour ce qui est des connexions de l'intérieur vers l'extérieur, ça se corse. Partons du fait que vous téléchargez sur votre ordinateur sans le savoir un petit programme encore inconnu des antivirus, qui est chargé de communiquer à un pirate des informations critiques de votre système. Vous allez dire que ce programme va être détecté parce qu'inconnu du firewall. Mais le programme pirate va demander à Internet Explorer de transmettre les informations à sa place... Internet Explorer étant un logiciel de confiance, le firewall sera déjoué...

Heureusement, il n'y a pas encore de trojans (le terme qui désigne les virus qui transmettent des informations sans consentement à un pirate) qui utilisent ce procédé.

Voici un lien vous permettant de télécharger un programme qui vous fera la démonstration de cette faille :

<http://keir.net/firehole.html>

Un moyen de réduire les risques de cette attaque est de ne pas faire enregistrer votre navigateur comme logiciel de confiance, de cette manière à chaque démarrage de Internet, une fenêtre vous demandera si vous voulez donner accès au navigateur. De plus, il existe une fonction dans Sygate qui permet de faire demander l'accès pour les fichiers DLL, mais ceci va faire apparaître plus de fenêtres de confirmation, et il faut savoir reconnaître chaque DLL indiqué par les fenêtres de confirmation, ce qui n'est pas donné à tout le monde... De toute manière, Sygate a montré un manque du côté de WebWasher... On ne pourrait conseiller que ZoneAlarm et Kerio.

En fin de compte, les firewalls protègent plus qu'un ordinateur sans firewall, mais il faut être tout de même prudent. Beaucoup de personnes expertes en la matière disent que ces appareils de protection donnent un faux sentiment de sécurité. L'important, c'est qu'il faut faire attention à ce qu'on télécharge, et aux sites que l'on visite. Rappelons que si on peut éteindre notre firewall avec le menu du firewall, un logiciel méchant pourrait aussi fermer le firewall en simulant un clic de souris sur la commande de fermeture du firewall. Par contre, aucun logiciel ne peut débrancher un firewall matériel de la prise électrique...

## CHAPITRE 3 - MISES À JOUR DES LOGICIELS

Pour ce qui est de la sécurité, ce sont surtout les logiciels conçus pour utiliser l'Internet qui sont à risque. Ces logiciels peuvent comporter des failles de sécurité, et à un moment ou l'autre, les programmeurs de ces logiciels vont les trouver, et fabriquer une mise à jour pour combler ces failles. Certaines corrections sont plus pratiques que d'autres. Par exemple, Microsoft va corriger les failles de sécurité de Internet Explorer en créant des petits fichiers qui vont corriger localement le bobo, tandis que Netscape va appliquer les corrections de son navigateur seulement dans la prochaine version, ce qui nous oblige à faire durer le problème et à télécharger un gros fichier lors de la sortie de la nouvelle version.

Des mises à jour sont aussi disponibles pour Windows, bien que les plus anciennes versions ne soient plus vérifiées par les programmeurs (dont Windows 95 et IE 4).

Pour les mises à jour de Windows et d'Internet Explorer, les mises à jour sont disponibles au site <http://v4.windowsupdate.microsoft.com/fr/thanks.asp>. Ce site nécessite la version 5 d'Internet Explorer ou plus récent. Si vous avez une version moins récente d'Internet Explorer, vous devez télécharger la nouvelle version 5.5, qui est disponible à l'adresse suivante : <http://www.microsoft.com/downloads/search.aspx?displaylang=fr>. Il ne sera pas expliqué ici comment installer la version 5.5, si vous avez des questions, posez-les moi.

Lorsque vous arrivez dans le site de Windows Update, il y a deux volets. Dans le volet de gauche, il y a les différentes fonctions, et la section de droite affiche le contenu de la fonction activée à gauche. Dans les premières secondes, le serveur de Microsoft va faire une vérification de votre moteur de mise à jour, et va peut-être mettre à jour le moteur de mise à jour. Si c'est le cas, répondez positivement aux questions posées, et vous devrez peut-être redémarrer Internet Explorer ensuite.

Si le moteur de mise à jour est à jour, vous aurez différentes fonctions accessibles dans le volet de gauche. Les deux plus importantes sont « **Sélectionner les mises à jour à installer** » et « **Examiner les mises à jour et les installer** ».

Premièrement, cliquez sur « **Sélectionner les mises à jour à installer** ». Les mises à jour seront recherchées et listées (si il y en a). Trois catégories de mises à jour sont possibles : les mises à jour critiques (de sécurité), les mises à jour de Windows (nouvelles applications et fonctionnalités de Windows) et les mises à jour de pilotes (rares, vous trouverez plus de mises à jour sur les sites des constructeurs de vos périphériques). Ces trois catégories seront affichées sous la fonction « **Sélectionner les mises à jour à installer** ». Cliquez sur chacune de ces catégories dans le volet de gauche pour voir toutes les mises à jour trouvées de chaque catégorie dans la section de droite. Chaque mise à jour est décrite et comporte deux boutons, l'un pour ajouter à la liste de téléchargement, l'autre pour retirer de la liste de téléchargement. Les mises à jour critiques seront ajoutées par défaut pour l'installation, mais certaines pourraient nécessiter d'être téléchargées seules. Dans ce cas, cliquez sur « Supprimer » de cette mise à jour et téléchargez-la une autre fois. Pour les mises à jour non critiques, cliquez sur les boutons « Ajouter » pour les ajouter à la liste de téléchargement. Lorsque vous êtes prêts à les télécharger, cliquez à gauche sur « **Examiner les mises à jour et les installer** », puis dans la section de droite, cliquez sur le bouton « **Installer maintenant** ». Dans la boîte de contrat d'utilisateur, cliquez sur « J'accepte ». Le téléchargement s'effectuera, et vous devrez ensuite redémarrer Windows.

## CHAPITRE 4 – LES SPYWARES / ADWARES / COOKIES

Les spywares et adwares sont un fléau de plus en plus grave aujourd'hui. Avec la quantité de logiciels gratuits qui se font aujourd'hui, il est de plus en plus difficile de faire des profits. Des créateurs (peu scrupuleux) ont donc eu l'idée d'incorporer des bannières publicitaires d'un annonceur dans leur logiciel. Lorsque la bannière est affichée dans le logiciel, l'annonceur de la bannière envoie un montant d'argent au créateur du logiciel. Mais comment fait l'annonceur pour savoir que sa bannière publicitaire est affichée? En fait, le créateur du logiciel a programmé son logiciel pour qu'il lui envoie des statistiques d'affichage, statistiques qui sont ensuite envoyées à l'annonceur.

Donc, pendant que vous utilisez le logiciel, celui-ci envoie plein d'informations, ce qui n'est pas toujours à votre connaissance. Le fait que des données seulement sur l'affichage des bannières sont envoyées n'est pas effrayant en soi; cependant, il arrive souvent que plus que des statistiques sur les bannières sont envoyées. En général, les adwares vont noter tous les sites Internet que vous visitez et vont envoyer ces informations au concepteur du logiciel. Rendu à ce point, il est plus raisonnable de parler d'espionnage, de là l'autre appellation « Spyware », où Spy signifie « Espion ». De par les sites que vous visitez, ils peuvent déduire quels sont vos centres d'intérêts et vos opinions, ce qui est en sorte une atteinte à la vie privée.

Les cookies sont différents, car ils sont créés en ligne pendant que vous visitez un site Internet. Les cookies sont des traces qu'un site va laisser sur votre ordinateur lorsque celui-ci doit choisir quelle page vous envoyer. Par exemple, si les différentes parties d'un site doivent être affichées dans un seul ordre précis, comme lorsque vous avez plusieurs étapes pour l'inscription à un site, un cookie va être créé. Quand vous remplissez un formulaire d'inscription, les données du formulaire sont gardées dans un cookie. Aussi, si vous avez quitté le site Internet et que vous y revenez plus tard, le cookie pourra dire au site où vous étiez rendu dans le site.

Les cookies ne sont généralement pas une atteinte à la vie privée, car les informations restent en fait sur votre ordinateur, et seul le site ayant créé votre cookie pourra consulter ce cookie. Ce type de cookie est un cookie « interne ». Cependant, il existe de grandes compagnies qui font des bannières publicitaires pour plusieurs sites. Ainsi, lorsque vous cliquerez sur un lien de publicité, vous ferez créer un cookie contenant le nom du site annoncé. Après plusieurs clics à différents endroits, la compagnie aura plusieurs cookies à elle mais qui leur montre quels sites vous avez visité, et pourra ainsi tracer votre profil... Ces cookies sont créés à partir d'un site autre que celui de la compagnie en question, c'est pourquoi on les appelle des cookies « tiers » (tierces personnes). Il existe aussi des cookies non satisfaisants, qui peuvent contenir des informations personnelles, mais sont généralement bloqués par défaut par les navigateurs.

Il serait donc utile de filtrer ces cookies, en laissant passer les cookies internes et en bloquant les cookies tiers et non satisfaisants. Cependant, ce n'est pas tous les logiciels qui sont capables de filtrer les cookies par type. En général, c'est tout ou rien. Cependant, Microsoft a nouvellement incorporé cette fonctionnalité dans Internet Explorer 6, ainsi que Netscape dans sa version 7.

## SECTION 1 – RETIRER LES SPYWARES AVEC SPYBOT

Le logiciel « **Spybot Search & Destroy** » est, bien que un peu moins connu, le plus complet disponible sur Internet, et surtout gratuit. Contrairement à son concurrent « **Ad-Aware** » dont il est question plus loin, Spybot S&D ne nous demandera pas d'acheter la version Pro pour avoir plus de fonctionnalités, car la seule version qu'il possède est la gratuite et toutes ses fonctionnalités sont accessibles en tout temps.

De plus, Spybot S&D ne fait pas qu'enlever les spywares, il peut régler certains problèmes système, vider l'historique d'ouverture de fichiers de plusieurs logiciels (ce qui peut être utilisé par des spywares), et plus.

En outre, certains spywares sont nécessaires au fonctionnement des logiciels qui les ont installés. Pour pallier à ce problème, Spybot contient des faux spywares qui seront substitués aux originaux. Le logiciel parent aura alors une fausse impression d'intégrité, mais le faux spyware ne communiquera rien à l'Internet.

### (PARTIE A) - TÉLÉCHARGER SPYBOT S&D

Le site Internet du logiciel est <http://security.kolla.de/index.php?lang=fr>

Dans la partie de gauche, cliquez sur « **Téléchargement** »;

Faites défiler la page vers le bas jusqu'à ce que vous voyiez plusieurs boutons « **Download here** ». Ces boutons vont aller soit sur un autre site où vous pourrez télécharger le fichier, soit télécharger directement le fichier du site sans afficher le site. Pour plus de commodité, cliquez sur le bouton qui a la mention « **download here** » en dessous, pour télécharger directement le fichier.

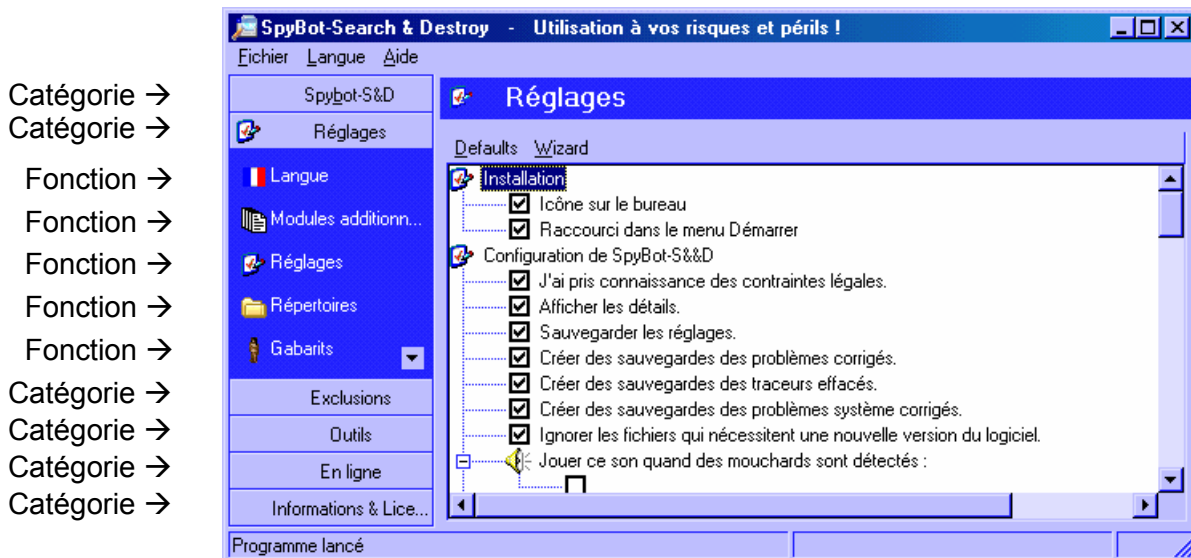
### (PARTIE B) - INSTALLATION DE SPYBOT S&D

Une fois téléchargé, exécutez le fichier d'installation de Spybot S&D. Différentes étapes seront affichées, mais en résumé vous devrez cliquer sur tout bouton qui porte un des noms suivants : « **Oui** », « **Next** », « **Install** » et « **Finish** ». À un moment, vous devrez cliquer dans un bouton d'option appelé « **I accept the agreement** »

Spybot S&D est maintenant installé. Un raccourci pour l'exécuter sera placé sur le bureau de Windows ainsi que dans le menu démarrer.

## (PARTIE C) - PREMIÈRE EXÉCUTION DE SPYBOT S&D

- 1) Double-cliquez sur un des icônes de raccourci pour exécuter Spybot S&D.
- 2) Dans la première fenêtre qui apparaît, vous devez cliquer sur le drapeau représentant votre langage. Les composants principaux de Spybot seront traduits.
- 3) Dans la deuxième fenêtre nommée « **Infos légales** », cochez la case « Ne plus afficher ce message, puis cliquer sur « **OK** ».
- 4) La troisième fenêtre nommée « **Information** » vous conseille de faire des mises à jour de temps en temps, cliquez sur « **OK** ».
- 5) Deux fenêtres vont apparaître. Dans la fenêtre du dessus, nommée « **Spybot S&D Wizard** », plusieurs étapes seront passées à l'aide de boutons rectangulaires au milieu de la fenêtre et un bouton « **Next** » en bas. Contentez-vous de toujours cliquer sur « **Next** » tant qu'il y en a, car cette partie est écrite en anglais. Les parties non traduites le seront en faisant une mise à jour plus loin.
- 6) À un moment donné, il n'y aura plus de bouton « **Next** ». À ce moment, cliquez sur le bouton du milieu « **Start using the program** ».
- 7) La fenêtre principale de Spybot apparaîtra. Comme sur l'image ci-dessous :



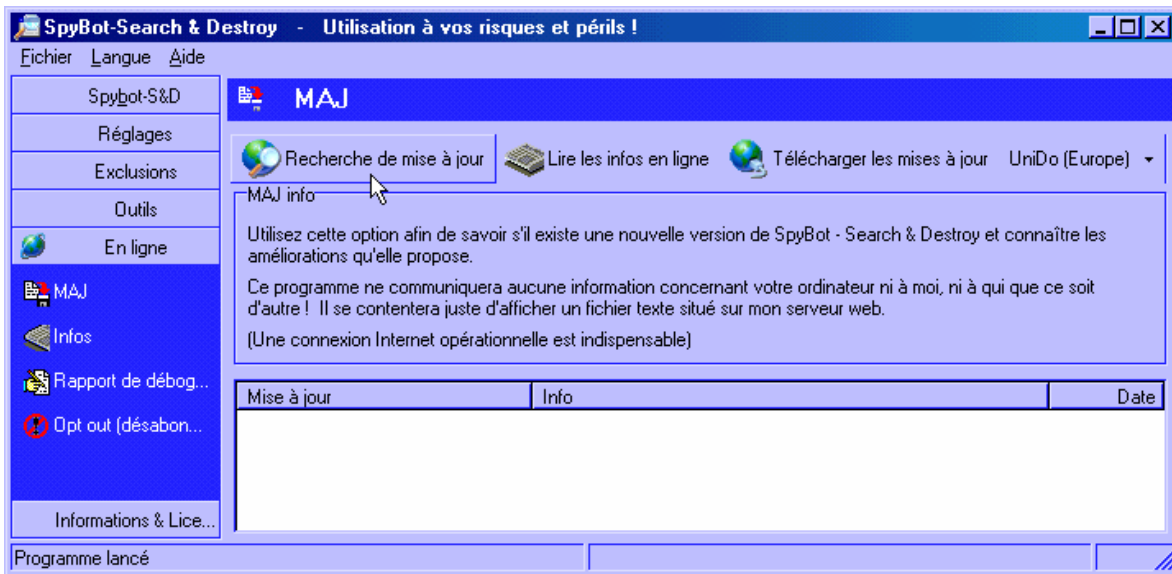
Dans cette fenêtre, la partie de gauche contient six boutons représentant chacun une catégorie de fonctions. En cliquant sur ces boutons, les fonctions de cette catégorie sont affichées sous le bouton. Il est ensuite possible de cliquer sur une fonction pour que ses composants soient affichés dans la partie de droite de Spybot.

Dans l'image ci-dessus, la catégorie « Réglages » est sélectionnée, et la fonction « Réglages » de cette catégorie est affichée. Cet affichage est celui que vous voyez dans la première utilisation du logiciel. Dans cette fonction, vous pouvez cocher ou décocher des options diverses.

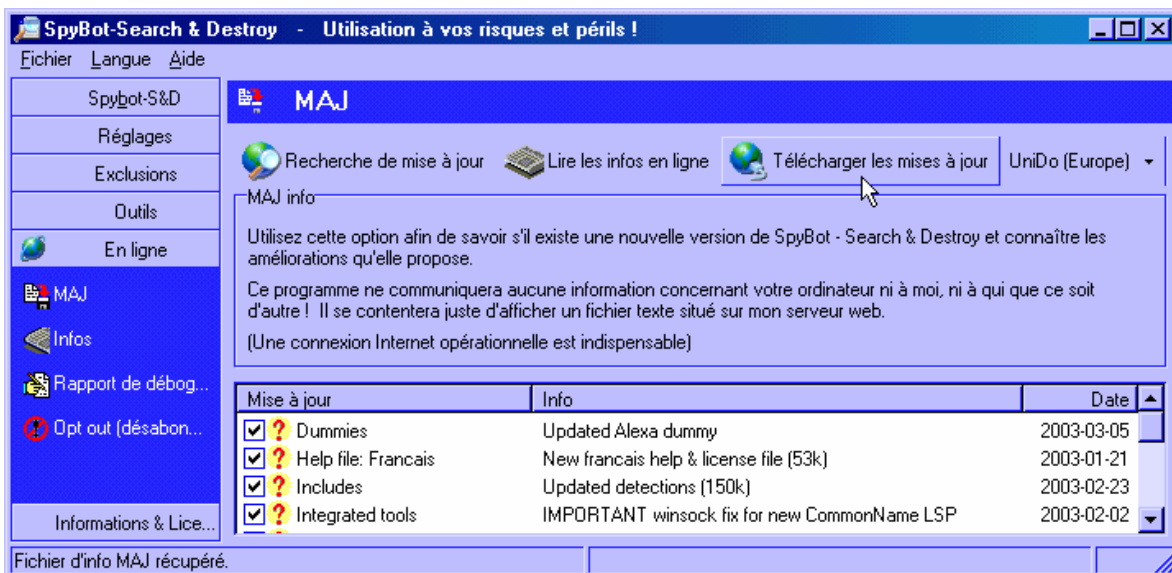
## (PARTIE D) - MISE À JOUR DE SPYBOT

Maintenant, pour que le logiciel soit à son meilleur, vous devez mettre à jour sa liste de référence. Cette liste dit à Spybot quoi chercher sur votre disque dur, car Spybot ne peut pas vraiment deviner sans indice si un tel fichier est suspect. Voici la procédure :

- 1) Dans la section de gauche de Spybot, cliquez sur le bouton « **En ligne** ». Les fonctions de « **En ligne** » seront affichées sous le bouton, et la fonction « **MAJ** » (mise à jour) sera affichée dans la section de droite, comme sur l'image suivante :



- 2) Vers le haut de la fenêtre, cliquez sur « **Recherche de mise à jour** ».
- 3) Si des mises à jour sont trouvées, il va apparaître dans la liste du bas des éléments avec des cases à cocher, chacun représentant une mise à jour. Cochez toutes les cases à cocher sauf les « **Skins** » (cocher seulement le skin « **Default** »), puis cliquez sur le bouton « **Télécharger les mises à jour** », comme sur l'image ci-dessous :



- 4) À la fin du téléchargement, Spybot va se fermer et va faire apparaître des fenêtres MS-DOS, qui elles vont appliquer les mises à jour sur Spybot, puis faire redémarrer Spybot ensuite. Vous pouvez refaire une autre mise à jour pour les autres Skins.

## (PARTIE E) - UTILISATION DE SPYBOT

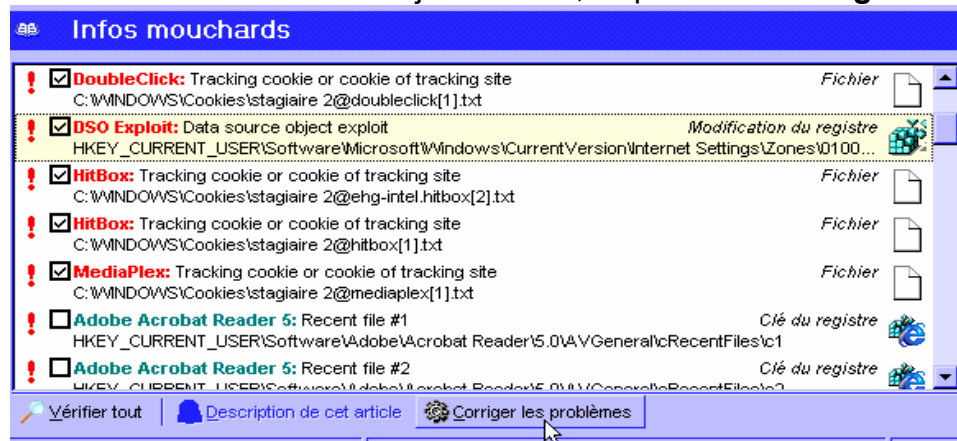
Les mises à jour terminées, il est maintenant temps de connaître le fonctionnement du reste du logiciel. Pour cela, vous pouvez utiliser le fichier d'aide, qui reste toutefois un peu vague. Le point le plus important est l'examen du système pour trouver les spywares (n'est-ce pas pour ça que nous l'avons téléchargé...). Voici la procédure :

- 1) Dans la section de gauche, cliquez sur le bouton « **Spybot S&D** ». Le contenu apparaîtra en dessous du bouton, et la fonction « **Search & Destroy** » sera affichée dans la section de droite. La fenêtre aura cette apparence :



- 2) En bas de la fenêtre, cliquez sur le bouton « **Vérifier tout** » pour débiter l'examen du système. L'opération sera indiquée complètement en bas de la fenêtre, et pourrait prendre plusieurs minutes pour s'effectuer. Les spywares et autres objets suspects seront ajoutés au fur et à mesure de leur découverte dans la liste de la section de droite.
- 3) À la fin de l'examen, vous pourrez voir un ou plusieurs éléments dans la liste, certains comprenant des caractères en rouges et d'autres en vert et peut-être d'autres couleurs. Les rouges sont cochés par défaut et représentent les spywares et autres menaces. Les verts ne sont pas cochés, et représentent par exemple les entrées de fichiers récents de beaucoup de logiciels, ce qui peut constituer une trace d'utilisation sujette à vérification, mais rarement. Pour effacer les objets cochés, cliquer sur « **Corriger les problèmes** ».

Dans certains cas, les objets seront remplacés par des faux pour berner les logiciels qui ont besoin de leur spyware pour fonctionner, comme Kazaa.



## SECTION 2 – RETIRER LES SPYWARES AVEC AD-AWARE

Le logiciel le plus populaire ces temps-ci est Ad-Aware, bien que un peu moins complet que Spybot. Ce logiciel gratuit a comme but de rechercher tout spyware et adware sur votre ordinateur (incluant les cookies), puis de vous proposer de les supprimer.

### → Télécharger Ad-Aware

- 1) Ouvrir votre navigateur Internet préféré.
- 2) Rendez vous sur le site du fabricant, soit [www.lavasoftusa.com](http://www.lavasoftusa.com)
- 3) Dans la section de gauche de la page principale du site, cliquez sur « Download ».
- 4) Dans la page de download, faites défiler la page vers le bas et cliquer sur un des liens portant la mention « Ad-Aware 6 » (la version 6 étant celle présente en date du 25 février 2003).
- 5) Dépendamment du lien choisi (plusieurs endroits sur Internet où le fichier d'installation se trouve), le téléchargement va soit débiter, ou vous aurez à cliquer, dans la page qui va apparaître, sur un lien de téléchargement. Lorsque Windows vous le demande, choisir d'enregistrer le fichier dans votre répertoire préféré (Fichiers téléchargés, Bureau de windows, etc).

### → Installer Ad-Aware

- 1) Quand le téléchargement est terminé, exécutez le fichier d'installation en double-cliquant dessus.
- 2) Dans la fenêtre qui apparaît, cliquez toujours sur « **Next** », puis enfin sur « **Finish** ».

### → Traduire Ad-Aware en Français

Des fichiers de traduction en français sont disponibles pour Ad-Aware, soit la traduction du logiciel lui-même et la traduction du fichier d'aide. Vous pouvez avoir la traduction sur le site suivant :

<http://www.networkingfiles.com/Cookie/adaware.htm>

Dans ce site, vous devrez cliquer sur les liens se nommant « **Ad-Aware 6 Language pack** » et « **Ad-Aware 6 French user manual** », puis les enregistrer dans votre répertoire de download favori.

### → Installer les fichiers de traduction de Ad-Aware 6

Pour le Language Pack, après avoir double-cliqué sur le fichier, vous ne devrez qu'appuyer sur les boutons « **Next** » tant qu'il y en a puis sur le bouton « **Finish** ».

Pour le « **User manual** », le fichier étant en .ZIP, vous devez l'ouvrir en double-cliquant dessus, ce qui fera apparaître WinZIP ou équivalent. Dans la fenêtre de WinZip, cliquez sur le bouton « **Extract** », sélectionnez le répertoire de Ad-Aware (habituellement « **C:\Program Files\Lavasoft\Ad-Aware 6** ») dans le volet de sélection de dossier puis cliquez sur l'autre bouton « **Extract** ». Lorsque effectué, vous pourrez quitter WinZIP.

→ Configuration de la langue de Ad-Aware

Lorsque Ad-Aware sera installé, exécutez-le à l'aide du raccourci qui a été créé sur le bureau de windows ou à l'aide de son groupe de programmes dans le menu démarrer. La fenêtre principale apparaîtra comme suit :




Vous constaterez que Ad-Aware n'est pas en français bien que les traductions sont installées. Pour mettre la traduction en fonction, vous devez cliquer sur l'image (🔧) dans le haut de la fenêtre, pour faire apparaître la fenêtre de configuration que voici :

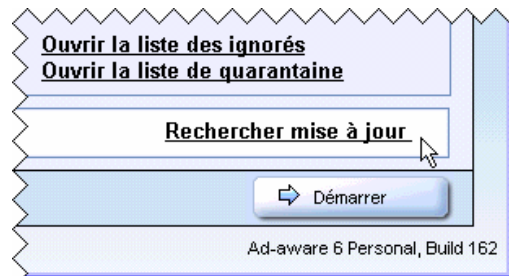
Dans cette fenêtre, cliquez sur la liste défilante identifiée « **Language file** », puis sélectionnez « **Français** » dans cette liste. Ensuite, cliquez sur le bouton « **Proceed** » en bas de la fenêtre. La fenêtre de configuration disparaîtra, et la traduction s'effectuera.



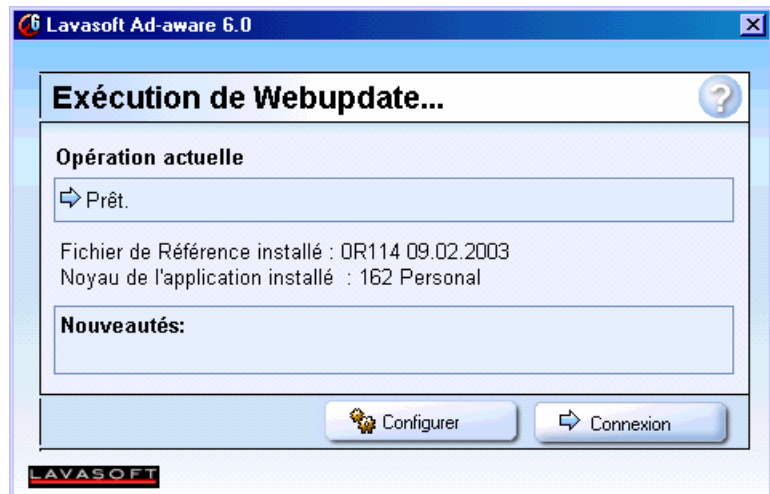
→ Mise à jour de la liste de références de Ad-Aware

Si à ce moment vous n'êtes pas connecté à Internet, faites-le.

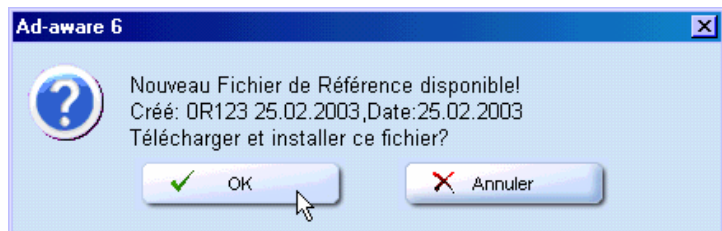
Ad-Aware reconnaît les Spywares en les comparant avec une liste qu'il possède, appelée la « **Liste de références** », et dont le principe est le même que les antivirus. Pour vous assurer que Ad-Aware est à son meilleur, vous devez mettre à jour cette liste. Pour cela, cliquez sur le lien « **Rechercher mise à jour** », près du coin inférieur droit de la fenêtre, ou sur l'image (  ) dans le haut de la fenêtre.



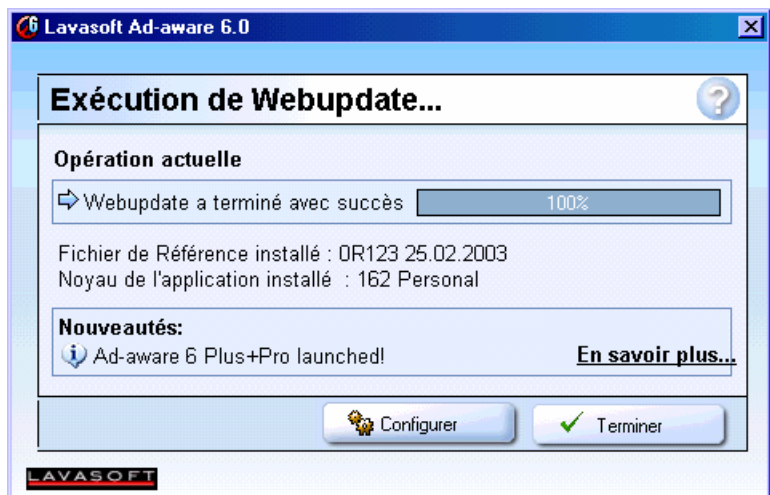
La fenêtre de mise à jour « **Exécution de WebUpdate...** » apparaîtra. Dans cette fenêtre, cliquez sur le bouton « **Connexion** ».



Après s'être connecté sur le serveur de Ad-Aware, une fenêtre vous indiquera si une mise à jour est disponible ou non. Dans les deux cas, cliquez sur « **OK** ».



À la fin de la mise à jour (dont la progression s'affiche dans la zone sous « **Opération actuelle** »), ou si aucune mise à jour n'est disponible, cliquez sur le bouton « **Terminer** » pour fermer la fenêtre de WebUpdate.



Notez qu'il peut être une bonne idée de vérifier les mises à jour une fois par semaine.

→ Retrait du spyware de Kazaa

Déjà, on peut noter un certain manque dans le logiciel Ad-Aware. La raison est que le logiciel d'échange de musique Kazaa et tous ses clones (Morpheus et Grokster) contiennent un Spyware nécessaire au fonctionnement. Ad-Aware va détecter le spyware de Kazaa et va l'enlever, ce qui va rendre Kazaa inutilisable. Il existe, dans ces circonstances, un faux spyware qui n'espionnera pas mais qui fera croire à Kazaa qu'il le fait. Malheureusement, Ad-Aware ne prend pas en charge le remplacement du spyware par un faux. Par contre, Spybot peut le remplacer.

Pour trouver le faux fichier en question « **CD\_CLINT.DLL** », branchez-vous à Internet et faites une recherche sur Google ou tout autre moteur de recherche. Allez ensuite voir la procédure de remplacement du fichier.

→ Analyse du système avec Ad-Aware

Maintenant que vous avez traduit et mis à jour Ad-Aware, il est temps d'analyser le système. Si ce n'est pas fait, démarrez Ad-Aware. Dans la section de gauche de la fenêtre principale, cliquez sur le bouton « **Examiner** ». La fenêtre aura alors l'apparence suivante :

Si le bouton d'option « **Options d'examen par défaut** » n'est pas celui choisi à ce moment, cliquez dessus pour le choisir. Juste en dessous, si « **Activer l'examen en profondeur** » est précédé d'un X, cliquez dessus pour qu'une coche sur fond vert apparaisse. Cliquez ensuite sur le bouton « **Suivant** »; l'examen du système va démarrer, et peut prendre plusieurs minutes.

**Préparation de l'examen du système**

Examinez votre système maintenant

➔ Veuillez choisir un mode d'examen, puis cliquer sur "suivant" pour continuer

**Sélectionner le mode d'examen:**

- Options d'examen par défaut **Personnaliser**
- Sélection des lecteurs\dossiers **Sélectionner**
- Effectuer une vérification rapide du système

Activer l'examen en profondeur

0 Eléments. ➔ Suivant

Lorsque la vérification est terminée, la mention « **Examen effectué** » s'affichera dans la fenêtre. À ce moment, cliquez sur le bouton « **Suivant** » dans le coin inférieur droit.

**Examen effectué**

**Opération actuelle**

Examen terminé. Objets examinés: **27210**

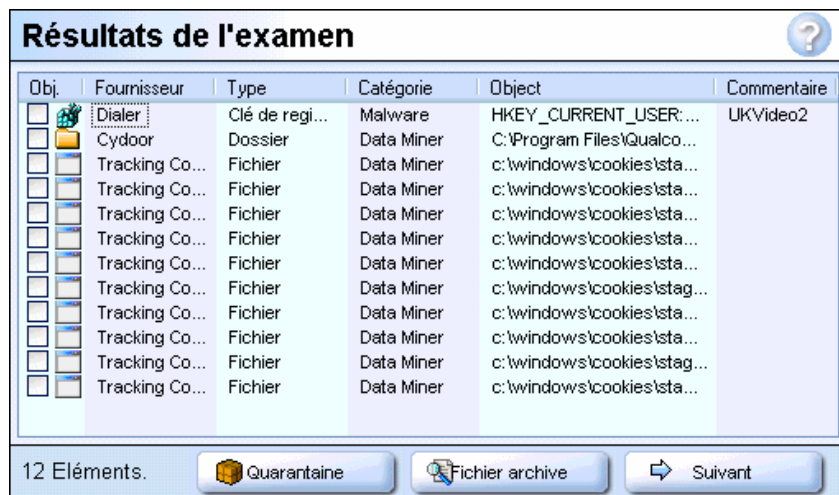
➔ C:\DocsPartagés\

**Résumé**

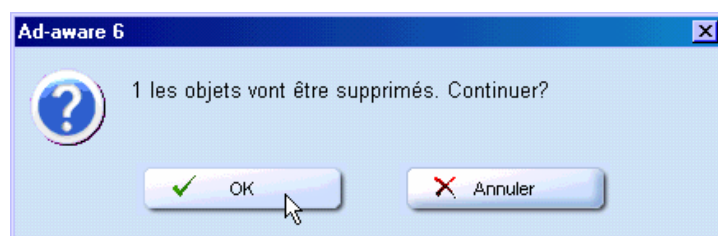
<b>21</b> Processus actifs	<b>0</b> Processus identifiés
<b>12</b> Objets reconnus	<b>1</b> Clés de Registre identifiées
<b>0</b> Objets ignorés	<b>0</b> Valeurs de Registre identifiées
<b>12 Nouveaux objets</b>	<b>10</b> Fichiers identifiés
	<b>1</b> Dossiers identifiés

12 Eléments. Fichier archive ➔ Suivant


La fenêtre affichera « **Résultats de l'examen** », avec une liste de tous les spywares et cookies trouvés. Droite-cliquer à n'importe lequel endroit dans la liste, puis dans le menu contextuel cliquez sur « **Sélectionner tous les objets** ». Une coche se mettra à coté de chaque objet. Cliquez ensuite sur le bouton « **Suivant** ».



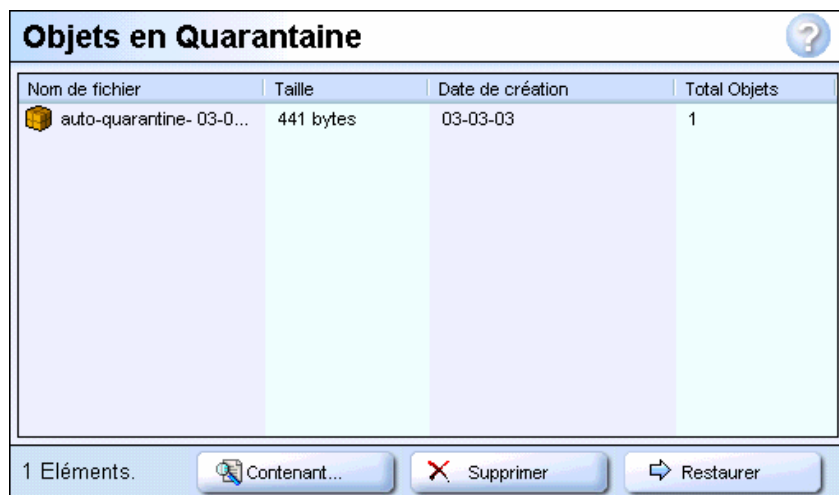
Lorsque vous aurez appuyé sur « **Next** », une fenêtre de confirmation vous demandera si vous êtes sûr de vouloir supprimer les objets; cliquez sur le bouton « **OK** ».



De retour à la fenêtre principale, cliquez sur le bouton « **Terminer** ».

Maintenant que les objets sont supprimés, ils sont envoyés dans la « **Quarantaine** » de Ad-Aware, l'équivalent de la corbeille de Windows. Si vous voulez définitivement supprimer les objets, cliquez sur l'image (  haut de la fenêtre. La section de droite de la fenêtre aura alors l'apparence suivante :

Dans la liste d'items, droite-cliquez dans la liste et, dans le menu contextuel, cliquez sur « **Supprimer toute les archives** ». Dans la fenêtre vous demandant si vous êtes sûr de vouloir supprimer toutes les archives, cliquez sur « **OK** ». Vous pourrez par la suite quitter Ad-Aware.



## SECTION 3 – CONFIGURER LA GESTION DES COOKIES

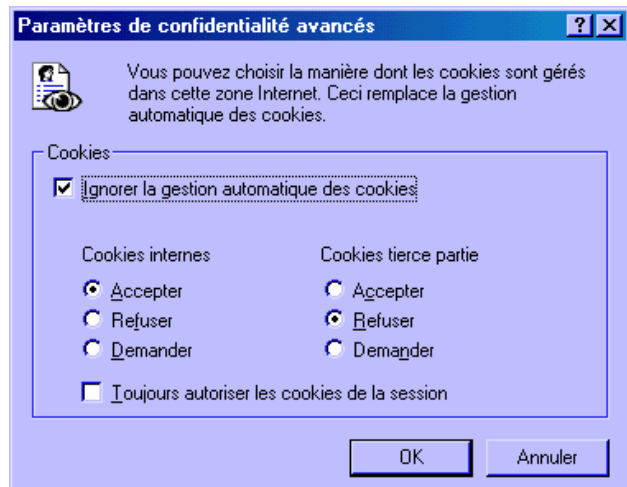
Comme mentionné au début du chapitre, il y a des cookies internes (appartenant au site visité) et des cookies tiers (appartenant à des sites autres que le site visité). Les cookies tiers sont ceux dont on veut se débarrasser. Voici comment procéder pour les deux navigateurs les plus populaires soit Internet Explorer et Netscape.

### PARTIE A – CONFIGURER LES COOKIES DANS INTERNET EXPLORER 6

Dans Internet Explorer 5 et plus ancien, on ne peut pas différencier le type des cookies. Par contre, la version 6 le peut. Allez dans le menu Outils / Options Internet. Une fenêtre apparaîtra. Dans cette fenêtre, cliquez sur l'onglet « **Confidentialité** », puis cliquez sur le bouton « **Avancé** », comme dans l'image suivante :



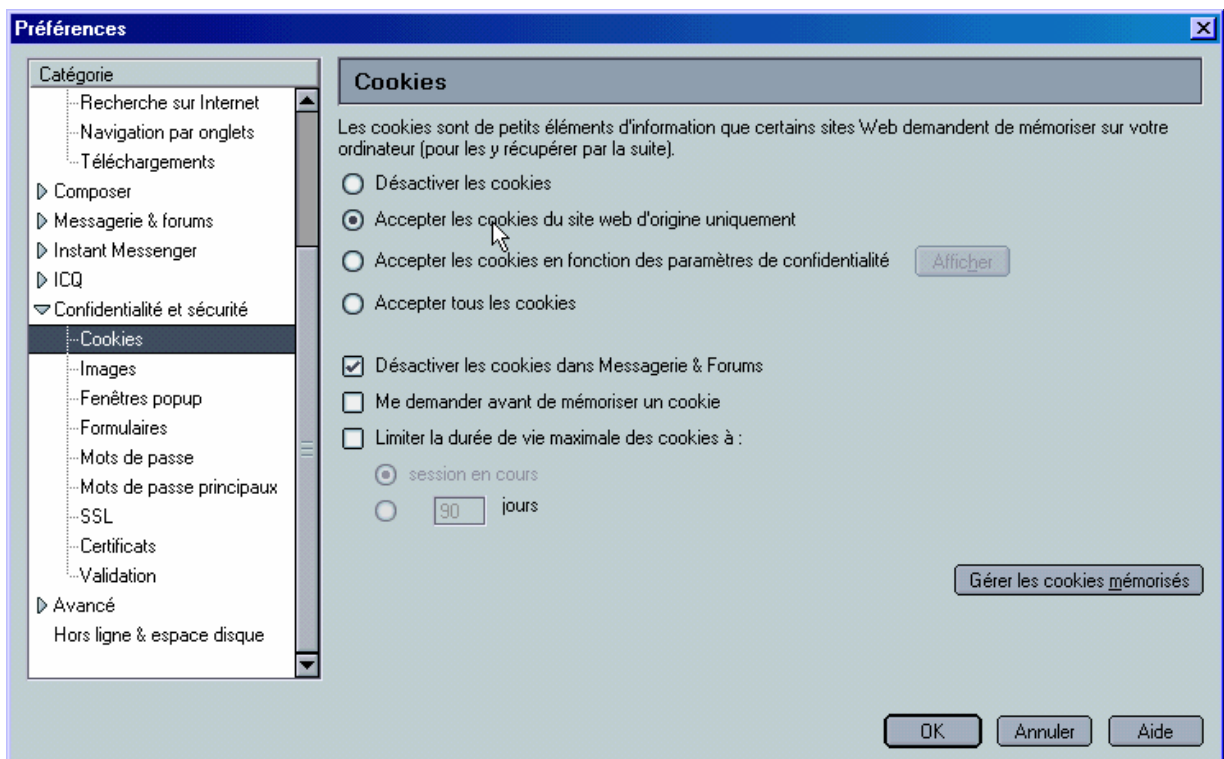
Dans l'autre fenêtre qui apparaît, cliquer dans la case à cocher « **Ignorer la gestion automatique des cookies** », cliquer dans le bouton d'option « **Refuser** » (celui sous « **Cookies tierce partie** »), puis cliquer sur les boutons « **OK** » des deux fenêtres de configuration ouvertes.



## PARTIE B – CONFIGURER LES COOKIES DANS NETSCAPE

Netscape a rendu possible de choisir le type de cookie à accepter dès le début, du moins depuis la version 4 (gageons que personne n'a une versions moins récente que 4...). Pour désactiver les cookies tiers, suivez la procédure suivante :

- 1) Démarrez le navigateur Netscape.
- 2) Cliquez sur le menu « **Édition** ».
- 3) Dans le menu « **Édition** », cliquez sur « **Préférences** ». Une fenêtre ressemblant à celle plus bas apparaîtra.
- 4) Pour Netscape 4, double-cliquez sur « **Avancé** » dans la section de gauche, ou pour Netscape 6 et plus récent, cliquez sur « **Confidentialité et sécurité** ».
- 5) Des sous-options apparaîtront dans la section de gauche. Cliquez sur « **Cookies** », ce qui fera apparaître dans la section de droite les réglages des cookies.
- 6) Cliquez sur le bouton d'option « **Accepter les cookies du site Web d'origine uniquement** ». Cliquez ensuite sur « **OK** » pour fermer la fenêtre de préférences.



## CHAPITRE 5 - LES ATTRAPES SUR INTERNET

L'Internet est un monde en soi. Comme dans le monde réel, il y a des bonnes personnes, et des mauvaises. Certaines personnes vont vouloir profiter du fait que la plupart des utilisateurs d'ordinateurs ne se méfient pas assez, et vont alors essayer de partir des rumeurs, nous envoyer des virus, ou même tenter de nous frauder.

Dans chaque cas, ces avis arrivent par email, et les responsables nous demandent de d'envoyer le message à tout le monde qu'on connaît, ce qui crée une chaîne de diffusion. Il y a alors une épidémie de mensonges, ou de dommages.

Pour visualiser ces attrapes, nous conseillons de visiter le site <http://www.secuser.com>, un site spécialisé dans les informations sur la sécurité informatique. Dans le haut de ce site, vous verrez une barre de liens. Dans cette barre, cliquez sur le mot HOAX (en vert). Le mot « hoax » signifie escroquerie, ou canular.

Dans la section hoax, il y a un tableau, accessible en descendant dans la page. À gauche du tableau se trouve le nom du hoax (sur lequel on clique pour lire ce qu'il est), suivi du type de hoax, de sa date de parution puis enfin une couleur représentant la fréquence d'apparition de ce hoax (voir légende au-dessus du tableau).

Voici une description des types de HOAX.

### → Les faux virus

Les personnes responsables de ces attrapes vont envoyer un message pour dire qu'un virus se propage présentement. Ils vont souvent dire que le virus arrive par un email comportant un titre en particulier, ou ils vont dire qu'il ne faut pas télécharger un certain fichier. Ces alertes ne sont pas physiquement dommageables, le seul inconvénient est la diffusion à grande échelle de ces messages.

### → La désinformation

Il s'agit d'une fausse information sur l'actualité générale, par exemple des offres commerciales, des événements publics qui se sont produits ou qui vont se produire. Par exemple, une future grève, une fusion commerciale, un accident, etc.

### → Les légendes urbaines

Il s'agit de courriels visant surtout à nous faire peur : nourriture empoisonnée, des dangers publics, etc.

### → Les chaînes

Il s'agit de courriels parlant de quelqu'un ayant besoin d'argent, et disant qu'à chaque lettre que vous envoyez à d'autres, une organisation donnera un certain montant à cette personne.

→ Les histoires vraies

Il s'agit d'avis de recherche qui sont réglés (la personne a été retrouvée), mais dont le message circule encore. En d'autres mots, des avis de recherches passés date.

→ Les viroax

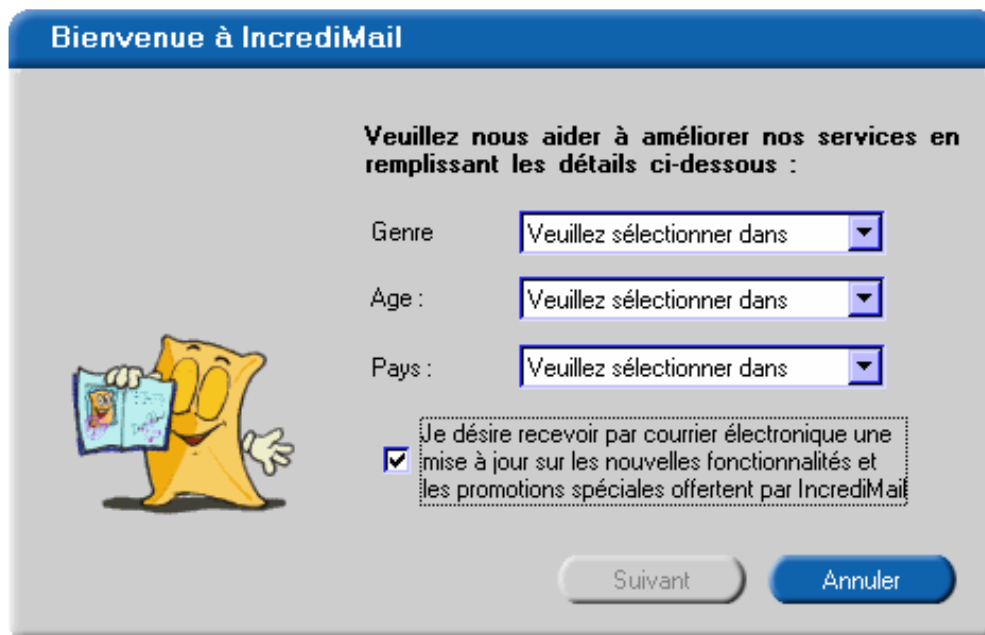
Les viroax sont relativement récents. Un viroax est un canular, mais qui cause des dommages sur vos disques durs. Comment? Un email va vous être envoyé, disant qu'un certain fichier de votre disque dur est un virus. Le fichier existe réellement, mais il n'est pas un virus. Mais le email vous demandera d'effacer le fichier, ainsi si vous n'êtes pas méfiant, vous allez l'effacer, et créer vous-même un problème sur votre système d'exploitation. Plus d'informations sont présentes sur le site de Secuser.com; pour les consulter, cliquez sur un des mots « viroax » dans le tableau de la section hoax.

## CHAPITRE 6 – COMMENT EMPÊCHER LE POURRIEL

### SECTION 1 – QU'EST-CE QUE LE POURRIEL?

Le pourriel est du courrier non sollicité. Il vous parvient pour plusieurs raisons, souvent suite à un abonnement à un site Web ou à l'installation d'un logiciel. Pendant la procédure d'abonnement / installation, le site ou le logiciel pourraient vous demander si vous voulez recevoir des publications et des offres et si vous voulez que vos coordonnées soient transmises à des tiers (ou questions similaires). En répondant oui ou en cochant l'option « envoyer mes coordonnées à des tiers », vos coordonnées seront mises sur une liste virtuelle publique. De cette manière, n'importe laquelle entreprise sera en mesure d'utiliser votre email pour du pourriel.

Par exemple, lorsqu'on installe le logiciel de courrier électronique Incredimail, une fenêtre apparaît au premier démarrage, nous demandant des informations particulières. Notez la case à cocher au milieu de la fenêtre, qui vous offre de vous envoyer des promotions spéciales par email. Ceci pourrait potentiellement constituer une source de pourriel.



Bienvenue à Incredimail

Veillez nous aider à améliorer nos services en remplissant les détails ci-dessous :

Genre : Veuillez sélectionner dans

Age : Veuillez sélectionner dans

Pays : Veuillez sélectionner dans

Je désire recevoir par courrier électronique une mise à jour sur les nouvelles fonctionnalités et les promotions spéciales offertes par Incredimail

Suivant Annuler

Dans ce cas, si vous ne voulez pas recevoir de pourriel, vous devez décocher la case à cocher.

Un point important à savoir est que, dans le cas des cases à cocher, il est très probable que ces cases soient cochées par défaut. Les propriétaires des sites et logiciels en questions savent que la plupart des gens ne vont pas se fatiguer à cocher les cases, donc ils le font à notre place. Ils savent aussi que, en conséquence, ces mêmes personnes ne se fatigueront pas à **décocher** les cases. Mais, il faut bien le répéter, il **faudrait** se fatiguer pour décocher ces cases.

À titre d'exemple, nous vous proposons d'aller visiter le site de Hotmail pour constater à quel type de questions vous êtes confrontés. Dans le site (<http://www.hotmail.com/>), vous

devrez premièrement cliquer sur le lien **inscrivez-vous**, dans le haut de la page. Vous serez dirigés vers le formulaire d'inscription. Veuillez vous rassurer qu'à ce point, vous n'êtes pas inscrit, car pour vous inscrire, vous devez cliquer sur le bouton « J'accepte », mais ne le faites pas! Descendez plus bas dans la page avec la barre de défilement pour visualiser les cases. Notez que les cases sont cochées par défaut...

Un autre exemple serait à propos des logiciels qui vous offrent de vous envoyer du courrier. Ici on peut voir une fenêtre de paramétrage du logiciel de courrier Incredimail.

Veuillez noter qu'ici aussi la case est cochée par défaut. On comprend que pour être rentable, une entreprise doit faire de la pub, mais si de toute manière vous ne la lisez pas...

Encore une fois, **fatiguez-vous** à décocher cette option...

Maintenant que nous vous avons montré comment empêcher l'apparition du pourriel, vous devez vous demander quoi faire pour l'arrêter si il est déjà en action...

Il est possible de l'arrêter, si l'expéditeur de ce pourriel est de confiance. Mais il faut savoir juger selon le type de pourriel envoyé. Si les messages viennent du site d'un fabricant de logiciels, d'un site populaire de nouvelles ou de tout autre site de confiance, il y a généralement un lien en bas du message qui vous permet de vous « Désabonner de la liste ».

Cependant, il existe des sites plus « underground », du genre sites pirates et pornographiques. Certains expéditeurs plutôt mal intentionnés vont insérer un lien de désabonnement qui, en cliquant dessus, va leur confirmer que votre adresse est bel et bien active, et ils vont intensifier leur pollution. Si à vos yeux l'expéditeur n'est pas digne de confiance, attendez quelques temps, et si il n'y a pas d'autres messages de sa part, vous n'aurez pas à cliquer sur son lien de désabonnement.

## SECTION 2 – LA NOUVELLE MENACE : LES WEB BUGS

Les auteurs de spam ont toutefois trouvé un moyen de savoir si vous avez lu son courrier sans que vous lui répondiez. En effet, le simple fait d'afficher le message dans votre lecteur de courrier va suffire à ce qu'il sache que vous l'avez regardé (violation de la vie privée). Cela se produit parce qu'ils insèrent ce qu'on appelle un « Web Bug » (Bibitte Web).

Pour mieux comprendre qu'est-ce qu'un Web Bug, il faut savoir qu'il existe deux types de courrier électronique. Le premier type est le courrier format texte, que le spammeur envoie en entier dans votre boîte de message. Le deuxième type est le courrier format page web (html), qui peut contenir des liens et des images. Dans le format html, les images peuvent être envoyées dans le email lui-même, ou le e-mail peut effectuer le téléchargement de l'image au moment de l'affichage du e-mail. Dans ce dernier cas, les images vont être téléchargées du site du spammeur, et non pas de votre fournisseur internet.

Les spammeurs ont eu ainsi l'idée de créer des images qui sont uniques parce qu'elles contiennent un identificateur numérique associé à votre e-mail. Par exemple, l'image associée à l'email [toi@hotmail.com](mailto:toi@hotmail.com) porterait le nom de « 387tym45cv5tmn8.jpg ». Ce nom d'image est unique. Lorsque que vous visualisez le message, votre logiciel de courrier va

télécharger cette image du site du spammeur, et le spammeur va savoir que vous avez lu son message puisque l'image a été téléchargée.

Une particularité de l'image est que cette image est souvent « invisible ». En fait, elle va être de la grandeur d'un point, ou pixel, et sa couleur va être la même que le fond de la fenêtre de email. Le terme Web Bug (bibitte web) est utilisé parce qu'une bibitte c'est petit (petit comme l'image d'un point)...

Comment éviter ce tour de passe-passe? Il est possible de télécharger les messages, puis de les regarder seulement après s'être déconnecté d'Internet. Par contre, le lecteur de courrier pourrait afficher automatiquement le premier email téléchargé, ce qui pourrait être un problème. Dans ce cas, vous devez désactiver la visualisation des messages de la manière suivante :

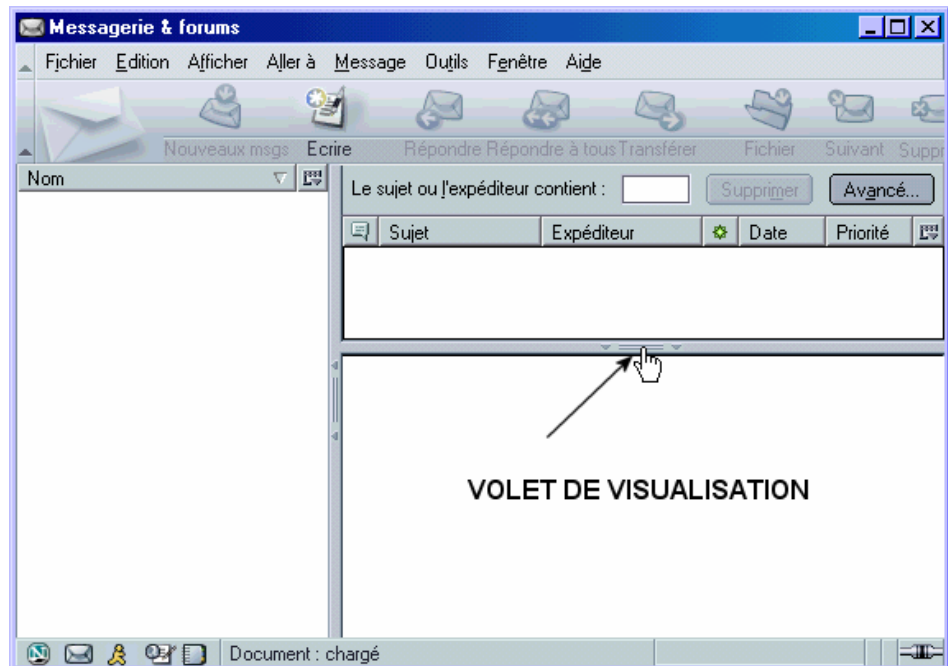
### Outlook Express

S'il y a déjà un bouton dans le haut de Outlook Express se nommant « Aperçu », vous n'avez pas besoin de faire les actions suivantes, sinon :

- 1) Cliquez avec le bouton droit sur la barre d'outils de Outlook Express.
- 2) Dans le menu contextuel, cliquez sur « Personnaliser ».
- 3) Dans la fenêtre qui apparaît, faites défiler la liste de gauche jusqu'à ce que vous voyiez un petit icône intitulé « Aperçu ». Cliquez sur cet icône, puis cliquez sur le bouton « Ajouter » au milieu de la fenêtre.
- 4) Fermer la fenêtre en cliquant sur le bouton « Fermer ».

### Messagerie Netscape

Si le volet de visualisation est effectivement affiché (voir image ci-contre), cliquez à l'endroit indiqué par une flèche pour le cacher.



Notez que certains emails « corrects » pourraient ne pas voir leurs images affichées, mais c'est un mal pour un bien.

Il existe un autre truc pour ne pas télécharger les images pendant que vous visualisez les messages tout en restant connecté à l'Internet : Il s'agit de configurer votre firewall logiciel (si vous en avez un) pour ne laisser passer qu'un certain type d'informations. Votre lecteur de courrier va télécharger les messages de votre fournisseur Internet via une sorte de porte, appelée « Port ». Ces messages passent par le port # 110. Les images qui se téléchargent sur le site du spammeur passent par une autre porte, le port # 80, qui est le port par lequel passent toutes les pages Web. Il s'agit de configurer le firewall pour permettre à votre lecteur de courrier de communiquer seulement sur le port 110, et pas sur le port 80. Ainsi, vous pourrez lire le texte, mais les images à télécharger sur les sites distants ne le seront pas.

Presque tous les firewalls cités plus tôt permettent de spécifier les ports à utiliser sauf ZoneAlarm.

Les Web Bugs sont aussi présents dans les pages web. Un peu moins dangereux, ces Web Bugs des pages Web servent souvent à mesurer l'audience qui visite le site. Par exemple, le Web Bug va demander à votre navigateur qui il est (Netscape, IE, etc), quelle résolution d'écran est en fonction sur votre navigateur, quelle est votre version de Windows, à quelle heure vous vous êtes branché sur leur site, et bien sûr l'adresse IP de votre ordinateur.

Infos supplémentaires : <http://www.uzine.net/article1211.html>

Il existe un petit logiciel pour voir les Webbugs (mais pas les bloquer). Ce logiciel s'appelle Bugnosis, et est compatible seulement avec Internet Explorer 5 et plus récent. Vous pouvez le télécharger à l'adresse suivante :

<http://www.bugnosis.org>

Lorsque téléchargé, vous pouvez l'exécuter pour l'installer. Dans la première fenêtre qui apparaît, cliquez sur « **Finish** » pour extraire les fichiers d'installation. Par la suite, cliquez sur « **Oui** », sur « **Next** » puis encore sur « **Finish** ». L'ordinateur redémarrera.

Le fonctionnement de Bugnosis est simple : une section apparaîtra dans le bas de la fenêtre d'Internet Explorer pour vous signaler les Webbugs (ou si il n'y en a pas). Dans la fenêtre de navigation, les Webbugs seront représentés par un petit icône de 18 par 18 pixels représentant une « bibitte ». Dans la barre d'outils d'Internet Explorer, un bouton « **Bugnosis** » permettra d'afficher ou de cacher manuellement la section du bas de Bugnosis (si le bouton n'y est pas, cliquez avec le bouton droit sur la barre de boutons d'Internet Explorer, cliquez sur « **Personnaliser** » dans le menu contextuel, puis dans la fenêtre qui apparaît, faites défiler la liste de gauche pour voir l'icône « **Bugnosis** », cliquez dessus puis cliquez sur le bouton « **Ajouter** », puis enfin cliquer sur « **Fermer** ».

Pour configurer les options de Bugnosis, vous devez faire afficher la section du bas de bugnosis. Cliquer avec le bouton droit dans cette section et cliquer dans le menu contextuel sur « **Options** ». Dans les options, vous pouvez décocher la case « **Popup Bugnosis window when a Web bug is found** » pour empêcher la section du bas d'apparaître tout le temps; les web bugs eux-mêmes resteront visibles dans la page web.

## COMMENT BLOQUER LES WEB BUGS?

Il existe un logiciel permettant d'effacer les Web Bugs des pages que vous téléchargez (mais ça ne les efface pas du propriétaire de la page...). Ce logiciel va en quelque sorte « détourner » les informations que vous téléchargez. C'est comme si un autre ordinateur était placé entre le vôtre et la connexion Internet, et que cet autre ordinateur modifiait les pages avant de vous les envoyer. De plus, toutes les applications voulant utiliser le Web se brancheront sur le logiciel, qui lui transfèrera la demande à l'Internet.

Le logiciel s'appelle WebWasher. En plus de retirer les Web Bugs, il va retirer les fenêtres popup, les bannières de publicité et d'autres choses permettant de retracer l'utilisateur. Par exemple, un site ne pourra pas savoir quel navigateur vous possédez, mais ce cas particulier pourrait changer un peu l'apparence des pages Web.

Pour télécharger le logiciel WebWasher, allez à l'adresse suivante :

<http://www.webwasher.com>

Important, il faut désactiver le filtrage standard de WebWasher pour que Windows Update fonctionne (si vous l'utilisez). Pour cela, cliquez une fois sur l'icône W dans la barre d'icône à droite de la barre des tâches, ce qui va mettre un X par-dessus.

Il m'est pour le moment impossible de vous assurer qu'aucun problème ne se passera avec ce logiciel. Pour la simple navigation, tout est OK, mais pour les services plus rares, il n'y a aucune garantie, je n'ai pas pu essayer ce logiciel avec assez de choses pour en être sûr.

## **CHAPITRE 7 – LE « PARENTAL CONTROL »**

### SECTION 1 – QU'EST-CE QUE LE PARENTAL CONTROL ?

Le « parental control » ou le contrôle parental vous permet de protéger vos enfants des sites dont le contenu est inapproprié. Vous pouvez personnaliser ce service à votre guise en bloquant ou en autorisant l'accès aux sites Web de votre choix. De plus, le service Contrôle parental vous permet de déterminer quand vos enfants ont le droit ou non de naviguer sur Internet, car vous pouvez choisir à quel moment du jour ou de la semaine ils peuvent y accéder.

### SECTION 2 – POURQUOI LE CONTRÔLE PARENTAL ?

Pour les parents, l'accès facile au Web soulève une question simple : comment protéger efficacement les enfants, qui peuvent rencontrer des sites ou des contenus inacceptables à caractère pédophile, pornographique, violent ou encore raciste ? La meilleure parade reste encore l'apprentissage de l'outil, en évitant de laisser seuls les enfants devant l'écran. Mais une solution complémentaire existe également, avec l'équipement de l'ordinateur familial d'un logiciel de filtrage.

Il y a aussi un autre risque à surveiller pour les plus jeunes. Il se cache derrière des sites qui leur sont directement destinés. Sous le couvert de jeux avec des lots ou des cadeaux à gagner, des sites commerciaux indécents questionnent les plus jeunes sur les caractéristiques de leur famille, leur âge, leur numéro de téléphone, la profession des parents... Ce recueil d'informations personnelles sert ensuite à bâtir des bases de données à l'insu des consommateurs. Une pratique inacceptable qui nécessite, de la part des parents, la plus grande vigilance, et une éducation des enfants.

Conseil pour éviter le plus possible cette menace sur la vie privée :

- Installez l'ordinateur dans une pièce ouverte
- Informez vos enfants sur les dangers de divulguer des informations personnelles (sur les sites et dans les forums de discussions)
- Limitez le temps de connexion
- N'hésitez pas à faire valoir vos droits à l'information auprès des sites où vous avez accepté que votre enfant s'inscrive.
- Accompagnez de temps en temps votre enfant lors de ses surfs.

### SECTION 3 – COMMENT FONCTIONNENT LES LOGICIELS DE FILTRAGE ?

Pour simplifier, nous distinguons, d'une part, le filtrage des sites sur lesquels les parents ne souhaitent pas que leurs enfants naviguent. Et, d'autre part, le filtrage des applications qui permettent de communiquer facilement : chats et messagerie électronique. La fonction d'un filtre consiste à s'intercaler entre le navigateur ou un autre logiciel, et Internet. Les types de filtrage sont:

- La liste noire

L'éditeur du logiciel établit une liste d'adresses de sites par catégorie : sexe, violence, etc. Lorsque le logiciel est activé, pour chaque site visité, il compare l'adresse à celles qu'il a stockées comme étant à éviter. Il empêche ainsi automatiquement qu'un site non désiré s'affiche sur l'écran. Cette liste de sites est mise à jour continuellement. Les éditeurs de ces logiciels dressent leurs listes noires de plusieurs façons (elles peuvent être utilisées simultanément). Les mieux équipés font appel à des surfeurs spécialisés qui traquent les sites, catégorie par catégorie. Certains font appel à des robots pour repérer les sites douteux, ces derniers étant ensuite évalués par l'éditeur. D'autres, enfin, font appel aux utilisateurs qui font remonter les adresses indécrites qu'ils ont croisées. Ensuite, l'utilisateur doit télécharger régulièrement la fameuse liste noire actualisée par l'éditeur. Ceci s'effectue soit manuellement à l'initiative de l'internaute soit automatiquement au cours des connexions Internet. Signalons l'apparition de logiciels faisant appel à l'intelligence artificielle et qui pensent de télécharger des listes noires.

- La liste blanche

À l'inverse de la liste noire qui est alimentée par l'éditeur, la liste blanche est dressée souvent par l'internaute. Cette option autorise une navigation restreinte aux adresses de la liste. Un contrôle absolu qui limite toute découverte du monde de l'Internet...

- Les mots clés

Certains mots-clés sont détectés soit dans les adresses (URL), soit dans les pages elles-mêmes. Certains logiciels filtrent même ces mots-clés dans les moteurs de recherche, les mails, les news groups... Mais sur certains logiciels, il est impossible de visualiser la liste des mots concernés. Il est aussi difficile de savoir à quel niveau le mot-clé est filtré (dans l'adresse, dans la page...). Le blocage est parfois contestable et souvent le mot détecté peut être remplacé par un blanc. Enfin, le blocage sur un mot, "sein" par exemple, empêche l'accès à de multiples sites d'information médicale!

- Le contrôle des discussions

Des logiciels contrôlent les échanges des news groups, des chats, des forums ou les pourriels électroniques. Certains ont un pare-feu (ou firewall) qui bloque complètement une application choisie par l'internaute.

#### SECTION 4 – COMMENT BIEN UTILISER SON LOGICIEL DE FILTRAGE?

- Téléchargez régulièrement les mises à jour des « listes noires »
- Paramétrez le niveau de filtrage pour chacun des utilisateurs
- Choisissez liste noire ou liste blanche
- Limitez la durée de navigation
- Changez régulièrement votre mot de passe
- Évitez la liste personnalisée d'adresses à proscrire (manipulation lourde et fastidieuse)

SECTION 5 – SITES SUGGÉRÉS POUR LE TÉLÉCHARGEMENT GRATUIT D'UN PROGRAMME DE « CONTROL PARENTAL »

[http://telecharger.01net.com/windows/Internet/cont\\_parentale/](http://telecharger.01net.com/windows/Internet/cont_parentale/)

<http://www.01net.com/article/181835.html>

<http://www.fdepot.com/parentalctrl.asp>

[http://www.cyberpatrol.com/parental\\_control\\_software.aspx](http://www.cyberpatrol.com/parental_control_software.aspx)

<http://www.contentpurity.com/>

Ps : Aucun logiciel de contrôle parental n'est efficace à 100 %. Ils ne peuvent pas se substituer au rôle éducatif des parents en ce qui concerne l'usage d'Internet. Leur fonction se limite à une première barrière.