

05 62 68 39 92
jeuxminform@free.fr

Assembleur Informatique
Réparations, S.A.V.
Cyber Café



JEUX M'INFORM



Ouvert 6j/7
Lundi et Samedi: 14h-19h
Mardi au Vendredi: 9h-12h/14h-19h



Comment Nettoyer et Protéger son Ordinateur





Table des matières

1. Notions de base

- Page 3 1. À quoi ça sert de nettoyer son ordinateur?
- Page 3 2. Qu'est-ce qu'un virus?
- Page 4 3. Qu'est-ce qu'un spyware?
- Page 4 4. Comment ces menaces entrent-t-elles dans mon appareil?
- Page 5 5. Comment s'en débarrasser?

2. Utilisation des programmes de sécurité

- Page 6 1. Le dossier Sécurité
- Page 7 2. C Cleaner
- Page 8 3. AVG Anti Virus
- Page 9 4. AntiVir Anti Virus
- Page 10 5. SpyBot Search & Destroy
- Page 11 6. Spyware Blaster
- Page 12 7. Reg Cleaner
- Page 13 8. Défragmenteur de disque

3. Toujours des problèmes?

- Page 14 1. Le mode sans échec
- Page 15 2. Des outils gratuits en ligne
- Page 15 3. Le réparateur





1. Notions de base

1. À quoi ça sert de nettoyer son ordinateur?

Ne vous méprenez pas, nettoyer son ordinateur ne veut pas dire lui donner un bain tous les dimanches ou passer une éponge dessus afin de raviver les plastiques. Éventuellement lui faire la poussière est une bonne chose mais ce n'est pas non plus le sujet. En fait le nettoyage dont nous allons parler est un nettoyage dit *logiciel*.

À chaque fois que vous utilisez votre ordinateur, que ce soit pour aller sur internet, taper des lettres, visionner des photos, écouter de la musique, graver des CD ou toute autre utilisation que vous jugez comme « normale », votre appareil va créer à votre insu des *fichiers temporaires* et des *entrées de registre* qu'il oublie souvent de supprimer. À cela s'ajoute le risque de contamination par des *virus* ou des *espions (spywares)* arrivant d'internet, de clé USB, de CD ou de cartes mémoires.

À la longue, tous ces documents *parasites* vont le saturer, le rendre plus lent voire le déstabiliser. Du fait il sera moins réactif, aura plus de risques de se bloquer, de *planter* ce qui rendra son utilisation moins attractive voire impossible.

C'est pourquoi il est important de nettoyer votre ordinateur et ce, de manière régulière.

Toutes ces opérations ne sont pas forcément très aisées pour un utilisateur, c'est pourquoi nous avons installé tout un pack de logiciels gratuits (*freewares*) afin de vous simplifier cette tâche.

2. Qu'est-ce qu'un virus?

Il s'agit d'un programme malveillant développé par des personnes mal intentionnées (hacker, programmeur de génie en manque d'inspiration,... allez savoir) qui aura, selon le type de virus, différents effets du type destruction de données, envoi d'informations confidentielles ou corruption de données telles que photos, vidéos, mp3 ou films..

Pour donner quelques exemples, les virus les plus répandus sont les *troyens* autrement nommés *chevaux de troye* pour faire référence à la mythologie Grecque. Leur but étant d'ouvrir en grand *les portes* de votre ordinateur à la personne contrôlant ce virus, lui laissant libre accès à l'intégralité de vos informations personnelles.

En suivant viennent les *vers*, il s'agit là d'un programme qui se copie d'ordinateur en ordinateur. Ce type de réplique peut donc non seulement affecter un ordinateur, mais aussi dégrader les performances du réseau dans une entreprise.

Il est donc important de s'en prémunir et de régulièrement vérifier le *bon état de santé* de votre ordinateur.





33 boulevard Saint Jacques
32100 CONDOM

Assembleur Informatique
Réparations, S.A.V.
Cyber Café

05 62 68 39 92
jeuxminform@free.fr



3. Qu'est-ce qu'un spyware?

Il s'agit ici d'une toute autre stratégie que celle des virus. Un spyware est un logiciel espion qui va s'installer dans le système à l'insu de l'utilisateur quand ce dernier donnera son accord pour ajouter un programme quelconque tel barre d'outil, jeu ou toute autre application.

Le but de ces spywares est principalement de surveiller et de renvoyer à des tiers les habitudes de navigation des internautes, afin d'en créer une base de données commerciale ou de permettre l'envoi de publicité ciblée aux utilisateurs.

Parfois il arrive que les spyware s'apparentent à des virus de part leur *action potentiellement destructrice* sur le système.

Ils se présentent sous plusieurs formes allant du simple cookie envoyé par le site visité afin d'en autoriser l'accès, jusqu'aux programmes vous indiquant que votre appareil est infecté par des myriades de virus fictifs et ayant pour but de vous délester de quelques dizaines d'euro au profit de leur créateurs, en passant par des *barres d'outils* qui s'insèrent dans votre navigateur internet.

Quoiqu'il en soit, ces spywares ont souvent une action tout aussi pénalisante sur le bon fonctionnement de votre appareil.

4. Comment ces menaces entrent-elles dans mon appareil?

Pour la plupart, tous ces programmes néfastes s'immiscent dans l'ordinateur par le biais d'internet et profitant des failles de Windows. Soit apparaissant sous forme de fenêtres publicitaires, de messages d'alertes falsifiés, par le biais du téléchargement sur les réseaux P2P (Bit-Torrent, E Mule, Limewire ou autre Shareaza) ou tout simplement en naviguant sur la toile par une image *vérolée* que votre navigateur charge automatiquement en *cache*.

Souvent leurs développeurs profitent de la crédulité des utilisateurs qui cliquent sur le premier bouton venu afin de faire disparaître cette vilaine fenêtre qui leur cache la vue sur leur site favori.

Rien de tel que la vigilance. En cas de doute, prenez le temps de lire le message que vous avez devant les yeux, ayez un dictionnaire Français/Anglais s'il est écrit dans la langue de Shakespeare de manière à en décoder les grandes lignes. Ne cliquez pas sur les boutons *Oui* ou *Non*, préférez fermer le message douteux avec la croix . Et surtout, ne faites confiance qu'aux messages d'alerte renvoyés par les programmes de sécurité installés sur votre appareil.

Prenez garde aux clé USB, cartes mémoires ou CD venant de chez vos amis, ces supports peuvent aussi contenir un virus ou des données contaminées.

Grâce à ces règles simples, vous pourrez déjà vous prémunir contre bon nombre d'infections.





33 boulevard Saint Jacques
32100 CONDOM

Assembleur Informatique
Réparations, S.A.V.
Cyber Café

05 62 68 39 92
jeuxminform@free.fr



5. Comment s'en débarrasser?

Une fois qu'un virus est entré dans votre ordinateur et qu'il s'y sent bien, souvent il y invite ses *amis*. C'est pourquoi il est primordial d'installer un anti-virus efficace (tous ne le sont pas qu'il s'agisse de gratuits ou de payants), de le maintenir à jour avec les dernières définitions de virus disponibles et de lui faire faire une vérification approfondie du contenu de votre disque dur régulièrement (une fois par semaine par exemple). Certains de ces anti-virus n'aiment pas la compagnie de leurs congénères, d'autres les acceptent volontiers et du fait, protègent doublement votre système. Mais attention, n'en installez pas plus de deux au risque de voir les performances de votre appareil sensiblement réduites.

Complétez cette protection par un ou deux anti-spyware, puisque ces logiciels espions n'étant pas classés comme des virus, vos anti-virus y seront presque totalement indifférents. Là aussi, il y a des *bons* et des *moins bons* anti-spywares.

S'il s'agit d'un virus ou d'un espion récent, il est possible que votre anti-virus ou anti-espion ne le connaisse pas encore, donc patience. Attendez quelques jours, sans utiliser votre ordinateur (le moins possible tout du moins), qu'une mise à jour connaisse cette menace.

Nettoyez également les fichiers temporaires, le cache de votre navigateur et les cookies de ce dernier.

L'alternative à ce long et laborieux travail étant de ne pas utiliser Windows. Il existe des systèmes d'exploitation alternatifs étant beaucoup (mais alors beaucoup!) moins sujets aux attaques virales et d'espions. De part leur bonne conception, ils sont plus fiables, plus stables, plus rapides et tout aussi agréables à utiliser que les produits venant de chez Microsoft et gratuit de surcroît.

Il s'agit en fait de Linux. Plusieurs distributions sont disponibles, pour les plus connues, trouvez la **Ubuntu** et la **Mandriva**. Ce système existant dans l'ombre depuis plusieurs années a fait d'énormes progrès ces dernières années vis à vis de l'utilisation grand public. Il y a toutefois quelques inconvénients majeurs à son utilisation:

d'une part les programmes que tout le monde connaît et utilise sous Windows ne fonctionnent pas sous Linux (tout comme les virus en passant) au profit de programmes équivalents ou similaires,

d'autre part les apriori à surmonter, du fait que la majorité des utilisateurs se laissent bercer par les fabricants ne proposant pas, mais imposant Windows.

Et pour finir, les jeux vidéo ne fonctionnant pas encore très bien sous Linux.

Dernier conseil très important:

Rappelez-vous qu'un ordinateur est comme une brosse à dents : Il ne se prête pas!





2. Utilisation des programmes de sécurité

Les programmes dont nous allons aborder l'utilisation dans ce chapitre sont fiables, complémentaires et ce, dans leur version gratuite. Nous les testons et les recommandons depuis des années. Nous les paramétrons afin de les rendre plus efficaces.

Bien sûr pour accroître la protection de votre appareil, il est possible d'acheter leur version payante, ou bien de faire un don à leur développeurs afin de les encourager dans leur travail.

Merci à eux!

1. Le dossier Sécurité



Vous pouvez voir sur le bureau de votre ordinateur ce dossier en forme de cadenas, il contient tous les raccourcis utiles pour lancer tous les différents programmes qui vous simplifieront l'entretien régulier de votre ordinateur. Afin de l'ouvrir et d'accéder à la liste, il suffit de faire 2 clics gauche sur cette icône.

Pour exécuter les programmes, il faut également faire 2 clics gauche sur chacun d'entre eux. Faites-les les uns après les autres dans un premier temps. Une fois que vous vous serez familiarisé à leur usage, vous pourrez les lancer tous à la fois pour gagner du temps.





33 boulevard Saint Jacques
32100 CONDOM

05 62 68 39 92
jeuxminform@free.fr

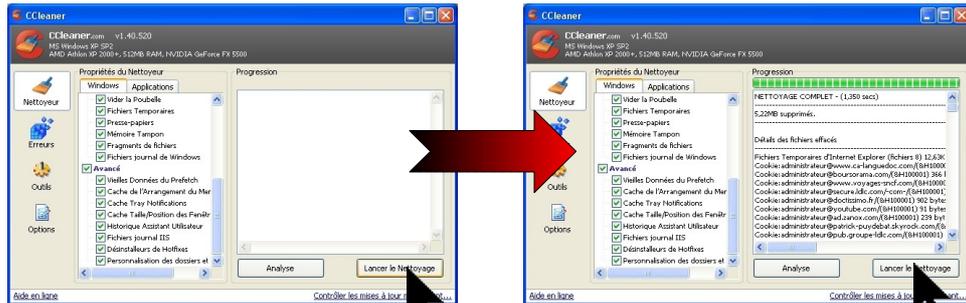
Assembleur Informatique
Réparations, S.A.V.
Cyber Café



2. C Cleaner

Ce programme permet de nettoyer votre ordinateur. En quelques clics, il va automatiquement vider les fichiers temporaires, le cache de votre navigateur, les cookies venant des sites internet et effectuer le nettoyage du registre système.

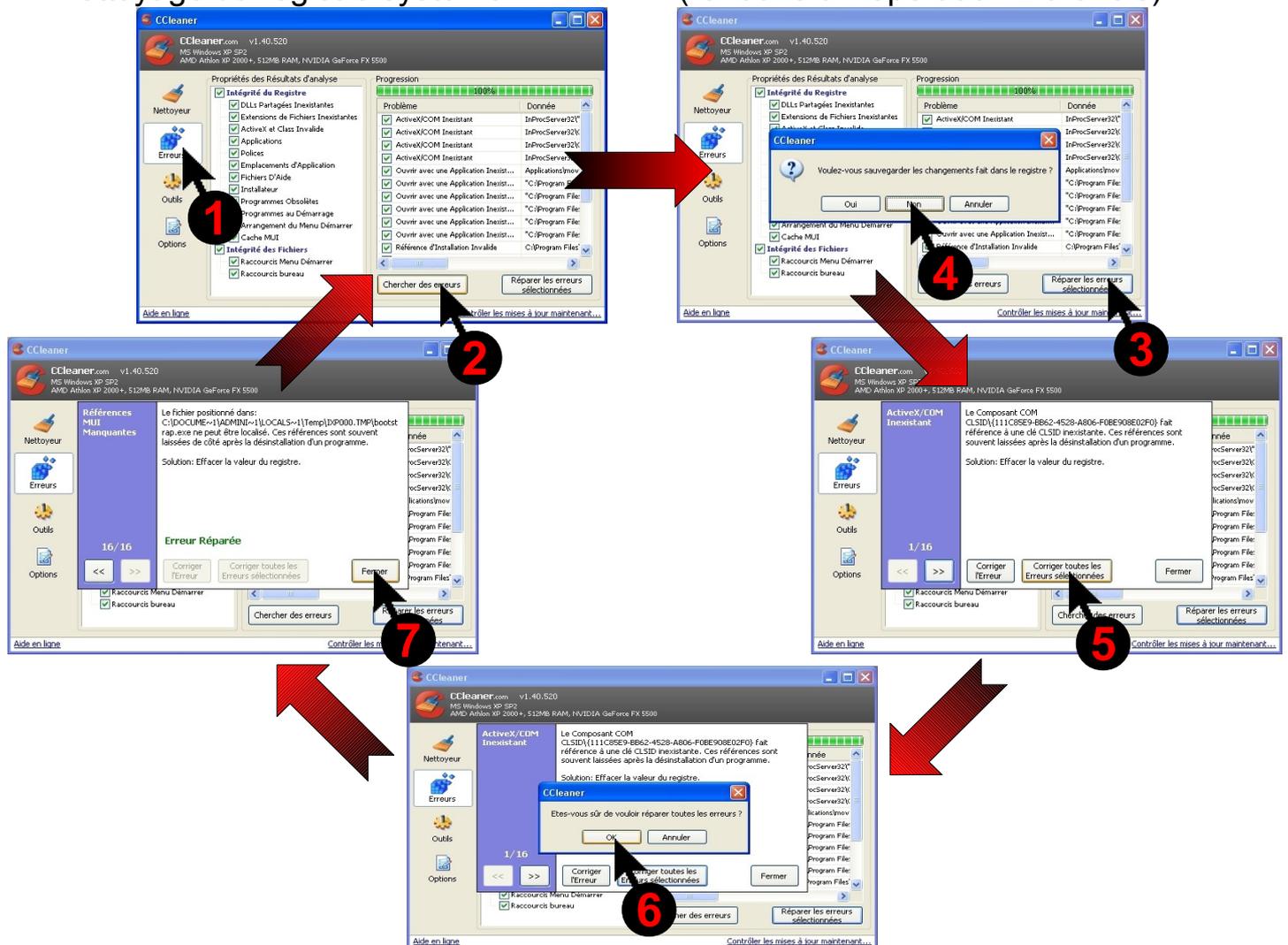
A. Nettoyage des fichiers temporaires:



(renouveler l'opération 2 à 3 fois)

B. Nettoyage du registre système:

(renouveler l'opération 2 à 3 fois)



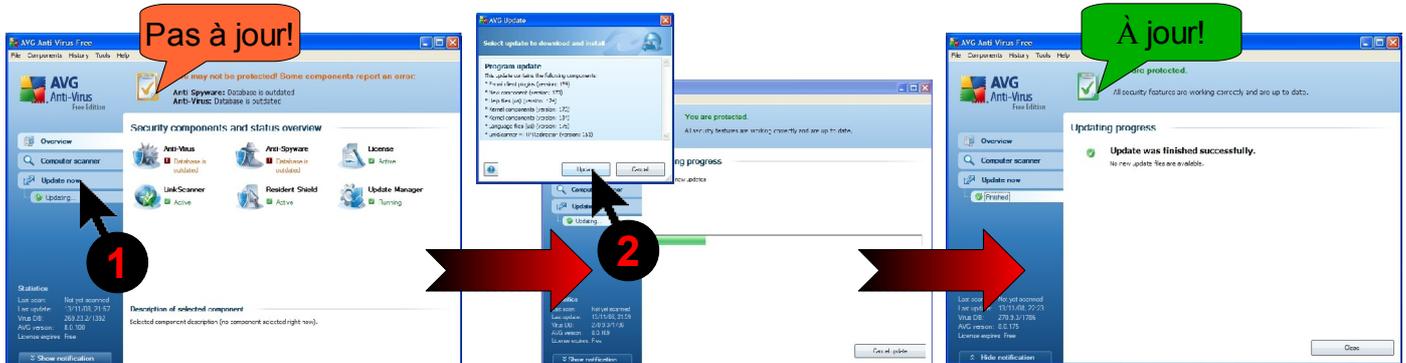
3. AVG Anti Virus

Le 1er des deux antivirus installés, en Anglais, mais paramétré par nos soins pour exécuter ses mises à jour à 1h00 et la vérification du système à 3h00 à condition de laisser l'ordinateur allumé et connecté à internet. Sinon, voici la marche à suivre pour l'exécuter manuellement.

En cas de détection préférez les choix: Delete , Heal , Quarantine ou Virus Vault.

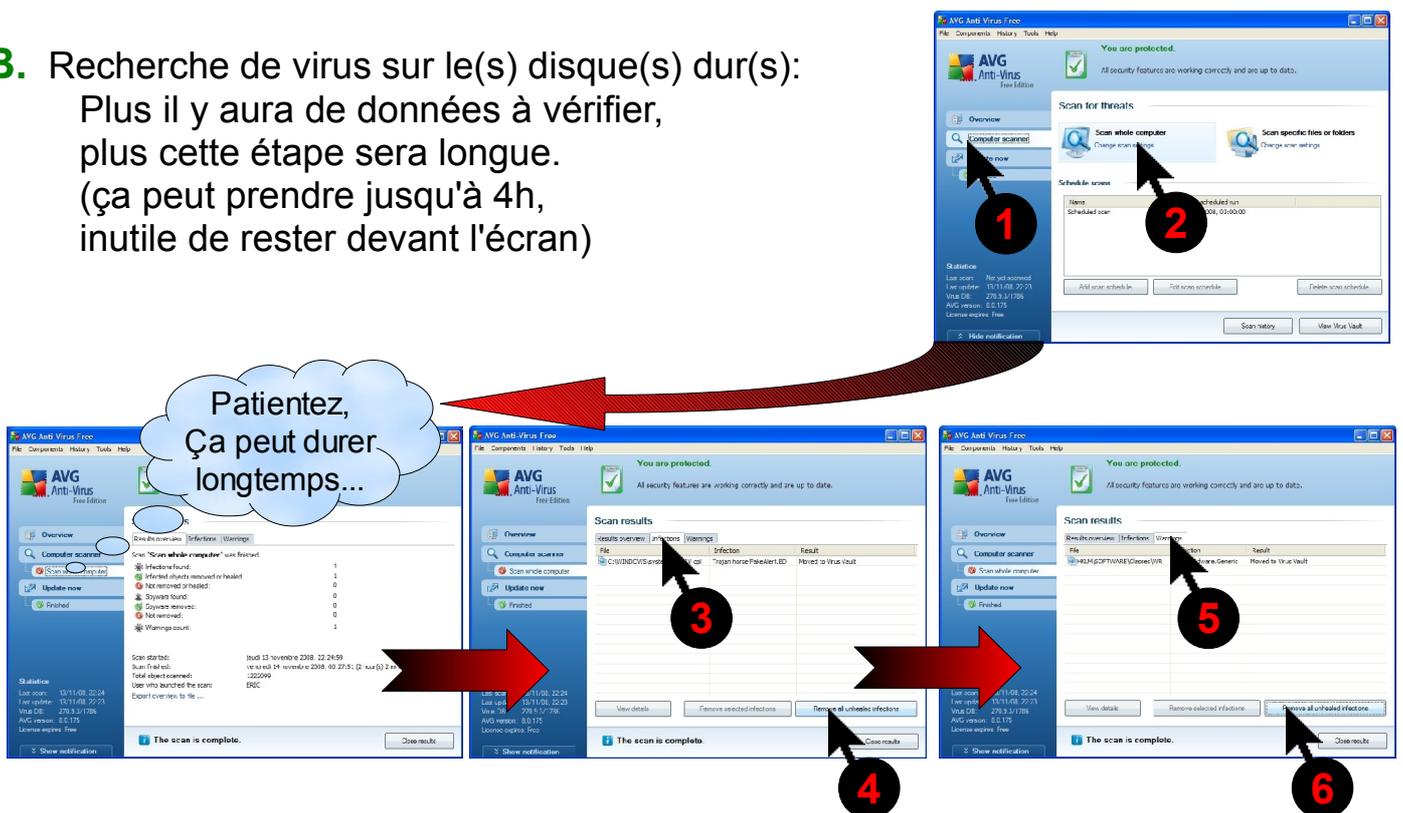
A. Mise à jour du programme:

Répéter l'opération tant que des mises à jour sont disponibles, redémarrez l'ordinateur si besoin.



B. Recherche de virus sur le(s) disque(s) dur(s):

Plus il y aura de données à vérifier, plus cette étape sera longue. (ça peut prendre jusqu'à 4h, inutile de rester devant l'écran)



Patiencez, Ça peut durer longtemps...

4. AntiVir Anti Virus

Le 2eme antivirus installé, en Anglais également, mais paramétré par nos soins pour exécuter ses mises à jour à 1h00 et la vérification du système à 3h00 à condition de laisser l'ordinateur allumé et connecté à internet. Sinon, voici la marche à suivre pour l'exécuter manuellement.

En cas de détection préférez les choix: Delete , Heal , Quarantine ou Virus Vault.

A. Mise à jour du programme:

Répéter l'opération tant que la mise à jour renvoie une erreur, elles peuvent parfois être longues à aboutir.

B. Recherche de virus sur le(s) disque(s) dur(s):

Dans le doute, il vaut mieux aller voir le rapport d'analyse, en recherchant "detection", de manière à s'assurer qu'à chaque virus trouvé il y ai indiqué: "The file was deleted". Ce qui signifie que le virus a été effacé.

5. SpyBot Search & Destroy

L'anti-Spyware, en Français celui-ci, paramétré par nos soins pour exécuter ses mises à jour à chaque lancement du programme à condition que l'ordinateur soit connecté à internet à ce moment là et à effectuer une vaccination du système à chaque mise à jour pour éviter au possible le retour des espions.

A. Si vous n'êtes pas connecté à internet, voici les messages que vous pourriez avoir:

Ne soyez pas surpris, ils demande simplement une connexion à internet, à sa façon. Fermez le programme, connectez-vous et relancez-le.

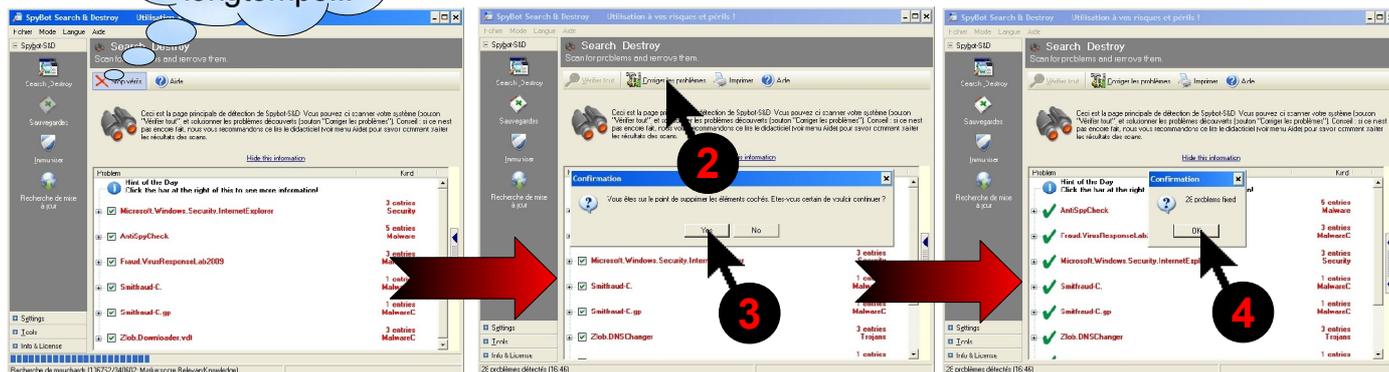


B. Recherche de spywares sur le(s) disque(s) dur(s):

Ce nettoyage est à faire sur chacun des comptes utilisateur créés!
Parfois, il arrive que Spybot demande à se lancer au prochain démarrage, c'est tout simplement pour mieux enlever les spywares récalcitrants.



Patience,
Ça peut durer
longtemps...



6. Spyware Blaster

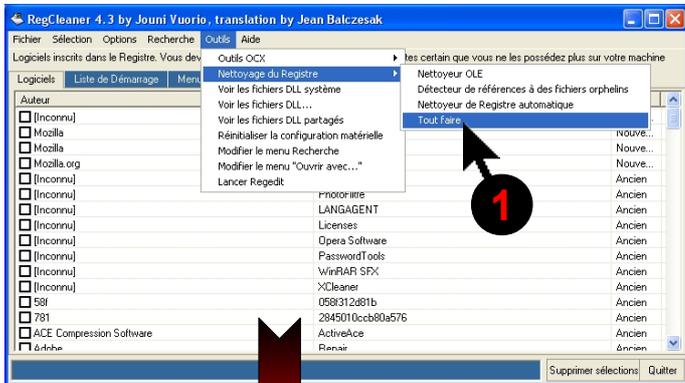
Ce petit programme en Anglais sert simplement à immuniser le système contre les spyware en complément de Spybot. Il est très simple à utiliser et très rapide.



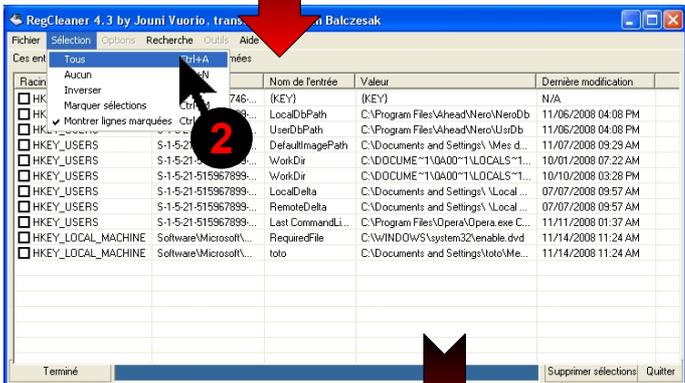
7. Reg Cleaner

C'est un vieil outil qui a longtemps fait ses preuves, qui est toujours utile mais qui maintenant à quelques difficultés à fonctionner correctement sur les nouveaux appareils (Windows Vista ou processeurs double cœur). Malheureusement, son concepteur n'a pas donné de suite, peut-être par manque de temps ou de moyens. Si quand vous essayez de le lancer rien ne se passe, n'insistez pas et passez à la suite.

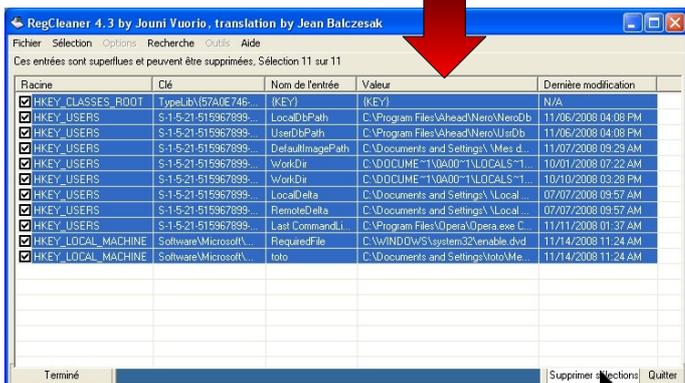
Si l'ouvre correctement, voici la marche à suivre:



Menu Outils,
Nettoyage de disque,
Tout faire.



Menu Sélection,
Tous.



Supprimer sélections.

8. Défragmenteur de disque

Lorsque vous ajoutez ou supprimez des informations sur le disque dur, tout cela ne s'agence pas très bien, comme un puzzle auquel il manque des pièces, il fragmente les informations stockées en plusieurs petits morceaux.

De ce fait il doit travailler, *gratter* beaucoup plus afin que vous puissiez vous en servir.

La défragmentation permet de réorganiser tous ces petits morceaux de manière à ce que le disque dur ait à moins travailler pour retrouver vos informations.

Il est utile de lancer ce programme à chaque fois qu'on ajoute ou enlève des données au disque dur. Lancé régulièrement, ça prendra moins de temps à s'effectuer.

Il se peut que la 1ere défragmentation soit incomplète, d'où l'intérêt d'en faire 4 ou 5 à la suite.

3. Toujours des problèmes?

1. Le mode sans échec

Parfois, certains virus ou spywares récalcitrants refusent catégoriquement de se supprimer parce que chargés en mémoire, Windows refuse que l'on y touche. Dans ce cas, il existe une solution qui fonctionnera presque à coup sûr, c'est le *mode sans échec*.

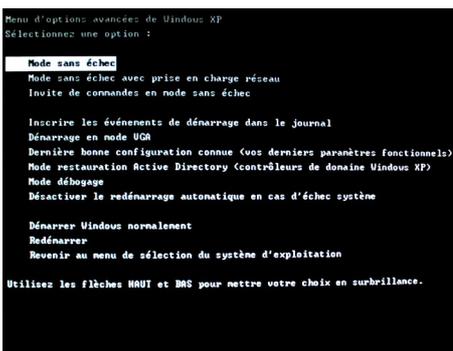
Dans ce mode particulier de fonctionnement, Windows démarre avec le strict minimum pour son fonctionnement et donc sans tous les effets visuels, programmes et virus qui seraient susceptibles de se lancer au chargement du système.

De ce fait, les programmes de sécurité, bien que plus longs à s'effectuer, seront plus efficaces.

Voici comment démarrer votre ordinateur dans ce mode d'urgence:



Dès l'allumage de l'ordinateur, quand le tout premier écran apparaît, appuyez plusieurs fois sur la touche "F8" en haut de votre clavier pendant au moins 30 secondes.



Si la manipulation a correctement été effectuée, vous allez tomber sur l'écran suivant.

Choisissez à l'aide des flèches directionnelles du clavier le "Mode sans échec"



Windows va démarrer d'une manière peu commune, et vous allez enfin tomber sur ce message, cliquez sur "Oui" Ensuite vous retrouverez votre bureau basique et pourrez lancer tous les programmes de sécurité. Une fois terminé, il reste à redémarrer.



33 boulevard Saint Jacques
32100 CONDOM

Assembleur Informatique
Réparations, S.A.V.
Cyber Café

05 62 68 39 92
jeuxminform@free.fr



2. Des outils gratuits en ligne

Le risque zéro n'existe pas. Tous les programmes que nous venons d'aborder ne sont pas infallibles et protègent votre ordinateur à environ 70%. Il y a donc un risque pour que des programmes malveillants passent tout de même à travers ces protections. Bien sûr on pourrait installer encore plus d'anti-virus et d'anti-espions, mais ça serai au détriment des performances de votre appareil.

L'alternative étant de n'utiliser ces programmes additionnels qu'en cas de réel besoin.

Pour cela il existe chez les grands fabricants d'anti-virus des *scan en ligne*. C'est simplement une partie de l'anti-virus, habituellement proposé à la vente, qui est mis à disposition gratuitement et pourra scanner vos fichiers à travers internet.

Pour ce faire, il faut généralement aller sur le site web du fabricant d'anti-virus voulu et en cherchant un peu, vous tomberez très certainement sur le choix d'un *scan en ligne*.

Certains sites recensent et proposent les liens directs à ce genre d'outils, comme par exemple zebulon.fr ou bien encore secuser.com.

À chaque fois il vous faudra accepter et installer un *contrôle ActiveX* qui est en fait la partie de l'antivirus destinée à votre ordinateur. Vous pouvez accepter d'installer ces modules sans craintes lorsqu'ils proviennent du fabricant voulu.

Une fois l'installation du contrôle Active X effectué et le téléchargement des mises à jour fait, il faudra être patient, le temps que l'analyse soit terminée et que le rapport arrive.

Le scan terminé, il vous reste à rechercher et supprimer les menaces trouvées manuellement.

3. Le réparateur

Si malgré tout cela il persiste des problèmes ou que vous ne vous sentez pas capable d'effectuer toutes ces fastidieuses opérations, n'oubliez pas qu'il existe des professionnels à votre écoute dont c'est le métier.

Il est souvent préférable de les consulter plutôt que de faire confiance au *copain qui connaît*, ce dernier risquant d'aggraver le problème.

Puisque *connaître* n'est pas *savoir*, faites confiance aux techniciens dont c'est le métier.

*En espérant que la lecture de ces quelques pages à été instructive,
je vous remercie d'y avoir prêté attention.
N'hésitez pas à nous consulter pour tout renseignements ou suggestions.*

