Niveau de difficulté

MOYEN

Cours Microfer Chartres

PROTEGER SON ORDINATEUR

Protéger son ordinateur : conseils et astuces - 06/10/2007

Carte blanche à : Jean-Pierre Louvet

Enseignant IUT

On se préoccupe trop souvent de la protection de son ordinateur lorsque c'est trop tard, en découvrant une infection. Or certains malwares sont très difficiles à éradiquer et nécessitent l'assistance de spécialistes. Il faut donc impérativement protéger l'ordinateur avant toute connexion à Internet. Non seulement les programmes malveillants peuvent perturber le fonctionnement de l'ordinateur, mais ils constituent un danger pour vous (par exemple programmes espions qui peuvent envoyer vers un pirate vos coordonnées bancaires, mots de passe…). En outre votre ordinateur peut constituer une source de nuisances pour les autres : sans que vous le sachiez il peut être contrôlé à distance pour envoyer du spam vers des milliers de victimes, ou participer à une attaque dirigée contre certains serveurs.

Ce mini-dossier n'a pas pour objectif d'entrer dans des considérations théoriques, ni de vous indiquer des techniques avancées de sécurité. Il vous propose un ensemble de méthodes simples, faciles à mettre en œuvre par un «utilisateur de base», et vous mettant à l'abri de pratiquement tous les risques de contamination.

Fidèles à une politique de neutralité par rapport à des offres commerciales, nous ne proposerons ici que des produits gratuits, même s'il existe des versions payantes (comportant des options supplémentaires) pour certains d'entre eux. Attention : certains produits peuvent êtres gratuits uniquement pour un usage privé. Vous possédez peut-être d'autres programmes gratuits ou payants remplissant certaines des fonctions assurées par ceux qui sont proposés ici. Il n'est pas question de discuter les mérites respectifs de tel ou tel produit, ni de prétendre que notre choix est le meilleur. Il a été guidé uniquement par un souci de simplicité.

Les stratégies listées ci-dessous sont classées par ordre de priorité, les plus importantes en tête.

Le pare-feu est la première protection indispensable de tout ordinateur relié à l'Internet. Son rôle est de bloquer les tentatives d'intrusion dans l'ordinateur par un pirate ou un virus. Il doit bloquer aussi toute tentative de connexion non autorisée à l'Internet par un programme résident sur l'ordinateur (par exemple un spyware : programme espion). Vous ne devez donc jamais vous connecter à Internet sans pare-feu.

La première fois que vous utilisez un produit se connectant à Internet (navigateur, programme de mail...) le pare-feu vous demandera si vous autorisez cette connexion. Vous pouvez répondre ponctuellement **Oui, ou demander que cette autorisation soit définitive. Les modalités peuvent être variables d'un pare-feu à l'autre.** Dans le but d'éviter certains risques, le pare-feu peut éventuellement demander aussi votre accord si un programme veut en lancer un autre, ou si un programme, sans aller sur l'Internet, veut exploiter l'adresse locale de votre ordinateur (127.0.0.1 ou localhost).
Par contre ne répondez pas Oui si l'avertissement du pare-feu ne correspond pas à un programme que vous êtes en train d'utiliser. De même, si le pare-feu vous avertit d'une tentative de connexion entrante, même sur un programme connu, en règle quasi générale vous devez répondre Non.
Vérifiez de temps en temps s'il n'y a pas une version récente de votre pare-feu, plus robuste face aux nouveaux types d'attaque.
Windows XP est équipé d'un pare-feu intégré qui est en service par défaut depuis le service pack 2 (attention, il ne sera pas actif si vous installez XP à partir d'un CD un peu ancien). Le gros défaut de ce produit est de ne pas filtrer les flux sortant. Il pourra donc juste servir de roue de secours pour une première connexion. Après installation d'un pare-feu efficace, arrêtez celui de Windows.

Zone Alarm est un pare-feu complet. C'est un des plus simple à utiliser et il en existe une version gratuite.

Sunbelt Personal Firewall est dans le même cas ; il a aussi une très bonne réputation. Si vous décidez de ne pas l'acheter, certaines fonctions évoluées deviendront inactives au bout d'un mois.
Comodo Firewall Pro est un pare-feu entièrement gratuit (il n'y a pas de version commerciale) qui paraît extrêmement puissant avec de nombreuses options ajoutées à la version 3 (novembre 2007). Il ne présente toutefois aucun problème de configuration pour ceux qui ne veulent pas s'écarter des réglages par défaut (il contient par exemple une liste des applications réputées sûres qui sont automatiquement reconnues).

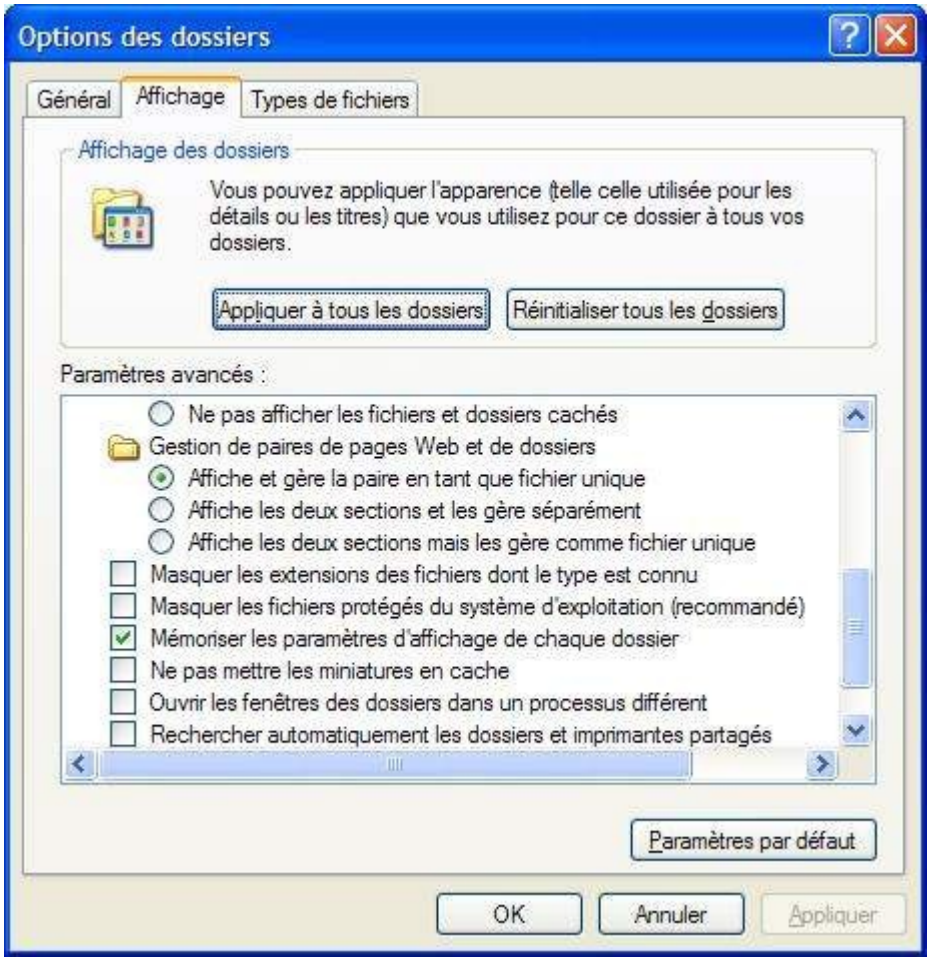
Malgré une arrivée très récente sur le créneau des pare-feux, Comodo fait globalement l'objet de commentaires flatteurs. La version 3 est uniquement en anglais au moment de la rédaction de ce paragraphe. La version 2.4 en français est toujours disponible chez l'éditeur.
Téléchargez ZoneAlarm
Téléchargez Sunbelt Personal Firewall

Télécharger Comodo Firewall Pro l

Le pare-feu des modem-routeurs et des Box
Un modem-routeur de même qu'une Box utilisée en mode routeur possède son propre pare-feu. La question de savoir s'il est alors utile d'installer en plus un pare-feu logiciel sur l'ordinateur est souvent posée. La réponse est claire : il faut également installer un pare-feu sur l'ordinateur. **En effet les pare-feux des routeurs ne bloquent que les intrusions, et non les sorties illicites.** Donc si vous avez un spyware sur

votre ordinateur rien ne l'empêchera de communiquer des renseignements privés vers un site pirate. Certes il y a moyen de filtrer les sorties avec un pare-feu de routeur (voir la notice de votre appareil pour les détails) mais cela pose des problèmes difficilement surmontables pour les protocoles qui assignent dynamiquement des ports variables, comme le FTP. **C'est donc à déconseiller, sauf pour un utilisateur très averti. De plus, même avec un filtrage en sortie rien n'empêche un spyware de communiquer par un port autorisé.**
Les pare-feux logiciels constituent donc un complément indispensable car ils filtrent les sorties en reconnaissant les programmes que vous avez autorisés à communiquer avec l'extérieur. **Toutefois certains malwares sont capables de les désactiver, ce qui leur est impossible de faire pour les pare-feux des routeurs.** Comme les deux types de pare-feux agissent à des niveaux très différents leur coopération constitue un rempart très efficace.
Les mises à jour du système d'exploitation sont destinées à corriger des bugs et des failles de sécurité. Votre système doit donc impérativement être à jour. En particulier le Service Pack 2 doit être installé car il comble des failles graves et, sauf exception rarissime, il n'y a pas de bonnes raisons pour l'écarter. Pour Windows les mises à jour sont publiées le deuxième mardi (heure US) de chaque mois.

Des mises à jour plus urgentes peuvent être publiées en dehors de ces dates. Avec Windows XP réglez la fonction de mise à jour automatique de façon à ce qu'elle soit active (clic droit sur le **Poste de travail, Propriétés**, onglet de **Mises à jour automatiques**).



Par défaut Windows XP est configuré pour cacher les extensions des fichiers connus par les programmes que vous utilisez. **Il faut impérativement supprimer ce réglage** (menu **Outils**, **Options des dossiers** ; dans la liste des paramètres avancés, désélectionnez **Masquer les extensions des fichiers dont le type est connu**). Ceci est nécessaire pour repérer les fichiers ayant une double extension : ce sont tous des vers ou virus.

Dans les versions de Windows à base NT (2000, XP) il est possible de limiter les droits octroyés aux différents utilisateurs. Le problème est que par défaut la session est habituellement ouverte en mode administrateur (c'est le mode qui peut tout faire) ce qui fait qu'un malware s'introduisant dans l'ordinateur héritera lui aussi des droits de l'administrateur. **Une règle de base de la sécurité est de ne jamais ouvrir de session en mode administrateur, sauf pendant le bref temps nécessaire pour effectuer certaines opérations (installer un programme, gérer le système...).** De plus l'accès au compte administrateur doit être protégé par un mot de passe robuste (7 à 8 caractères en mélangeant plusieurs types de caractères : majuscules, minuscules, chiffres et signes de ponctuation).

Attention : XP pouvant être utilisé en mode multisession, il ne faut pas laisser le compte administrateur ouvert en arrière plan ; il faut réellement le fermer dès qu'on n'en a plus besoin.

Microsoft fournit une solution intermédiaire pour utiliser certains programmes depuis le compte administrateur : le programme **DropMyRights (à télécharger).** Le principe est de lancer tout programme accédant à l'Internet (navigateur, programme de courrier...) par l'intermédiaire de **DropMyRights**. Ce dernier limite fortement les droits attachés au programme qu'il lance et réduit les risques d'installation de malwares.

Exemple pour lancer Internet Explorer faites un clic droit sur son icône, sélectionnez **Propriétés**, l'onglet **Raccourci** et mettez dans le champ **Cible** le contenu des deux lignes suivantes, sur une seule ligne et séparé par un espace :

"C:Program FilesDropMyRightsDropMyRights.exe"
"C:Program FilesInternet Exploreriexplore.exe"

à la place de :

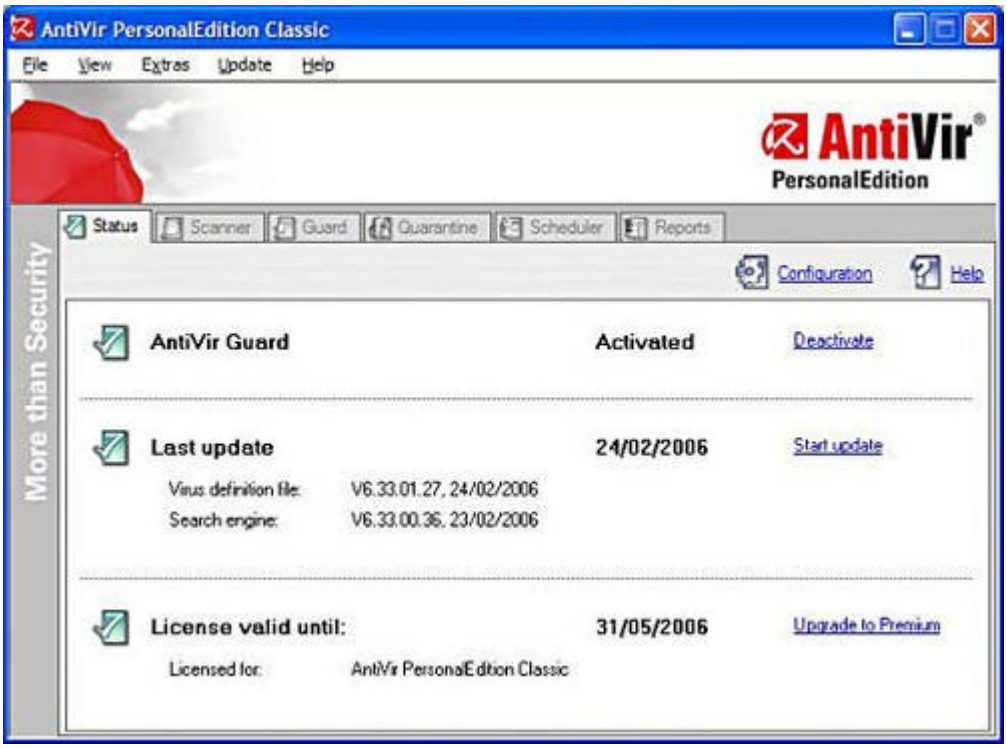
"C:Program FilesInternet Exploreriexplore.exe"

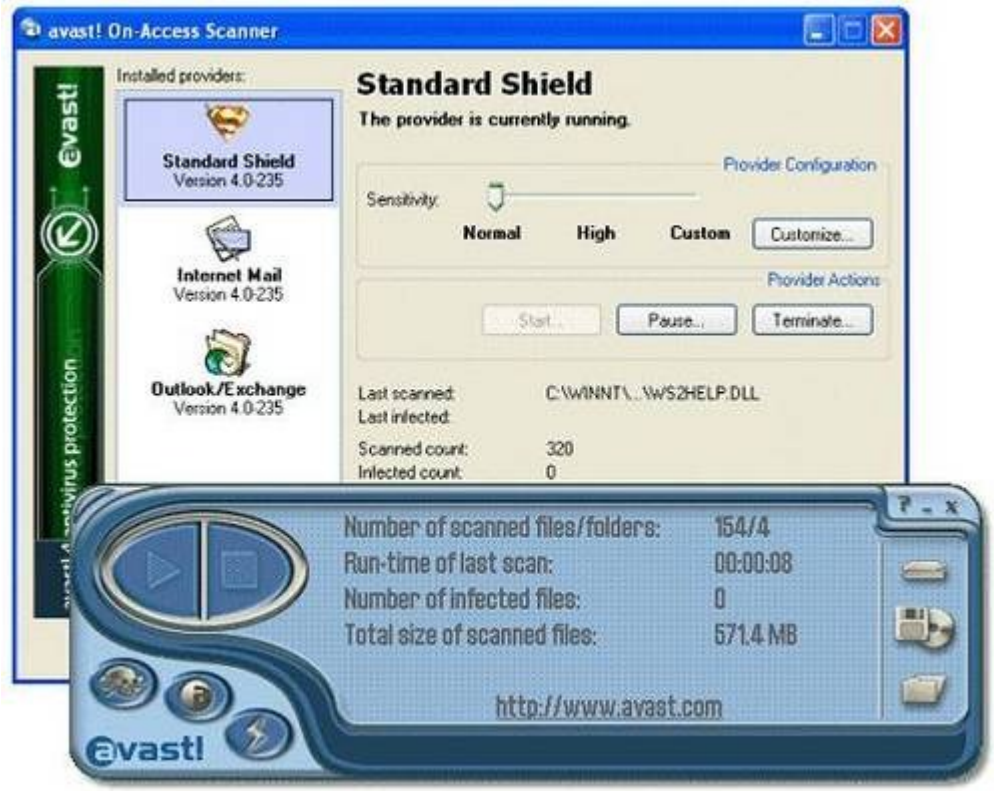
Remarques :

- vous ne pouvez pas utiliser Windows Update avec ce mode de fonctionnement d'Internet Explorer ; il faut le lancer de façon classique en mode administrateur ;
- la protection par DropMyRight ne fonctionne que si vous appelez le programme à partir du raccourci modifié ; ceci signifie par exemple que si vous lancez le navigateur en cliquant sur un lien contenu dans un mail, le navigateur utilisera les droits de la session en cours et non les droits limités ;
- il est impossible de limiter les droits des utilisateurs dans Windows 98 ou Millenium.

Téléchargez DropMyRight

Il s'agit également d'une protection indispensable.
Il existe d'excellents antivirus gratuits : on peut citer par exemple Antivir, Avast ou AVG. Vous devez impérativement régler l'antivirus pour qu'il aille chercher **quotidiennement** sur le site de l'éditeur la présence de mises à jour. Divers spécialistes de la lutte contre les infections affichent actuellement une préférence pour Antivir en raison d'une excellente rapidité de mise à jour lors de l'apparition de nouveaux malwares.



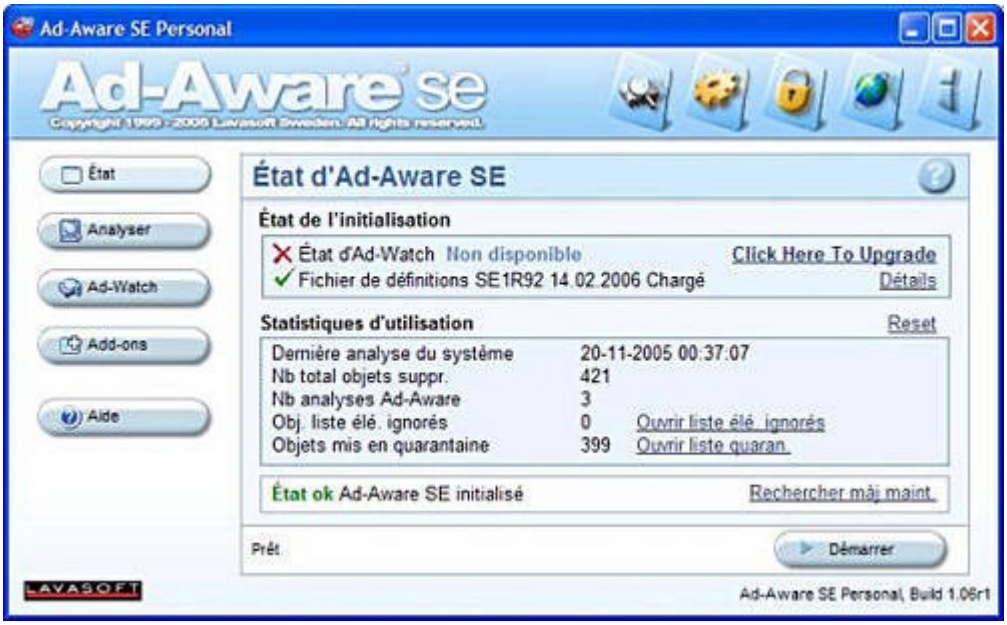


Attention : Avast contient un pare-feu léger (« Network Shield » - non testé).
S'il entre en conflit avec le pare-feu que vous avez installé, désactivez celui d'Avast. On a aussi signalé un problème de conflit entre Avast et Zone Alarm. Si vous choisissez cet antivirus, utilisez plutôt Kerio comme pare-feu.

Un antivirus comporte une partie résidant en mémoire qui surveille en temps réel les événements impliquant la présence ou l'activité d'un virus ou ver, et un programme plus classique utilisé pour scanner l'ordinateur. En effet, malgré la présence du programme résident vous devez faire un scan hebdomadaire de votre disque dur avec l'antivirus. S'il détecte un parasite lors de ce scan il vous en avertira mais ne pourra généralement pas vous en débarrasser. **Il faut alors relancer Windows en mode sans échec puis refaire le scan.** Si vous avez Windows Millenium ou XP il faut en outre désactiver au préalable la restauration du système, puis la remettre après la désinfection (clic droit sur Poste de travail, Propriétés, onglet restauration du système).

Tous les fichiers importés dans votre ordinateur et toutes les pièces jointes doivent être scannés avant leur ouverture.
Attention à un piège : si le scan détecte un virus dans la boîte des mails que vous avez reçus, comme tous les mails sont stockés dans un fichier unique, l'antivirus est susceptible de détruire entièrement votre boîte (et pas uniquement le message) s'il est réglé de façon trop intrusive.
On ne doit pas installer deux antivirus simultanément : ceci engendre habituellement des conflits.
Téléchargez Antivir Personal Edition Classic
Téléchargez Avast
Téléchargez AVG Free

Ces programmes suppriment les programmes espions et peuvent éventuellement avoir des rôles plus étendus. Deux programme gratuits peuvent être recommandés : **Adaware SE et Spybot Search and Destroy**. Ces deux programmes utilisent des techniques d'exploration différentes et peuvent donc être complémentaires. Comme les antivirus ils utilisent une base de données qui doit être mise à jour régulièrement. Un scan hebdomadaire de l'ordinateur est recommandé.



Il existe deux options de surveillance en temps réel dans **Spybot** (il faut le lancer en mode avancé et sélec-

tionner **Outils, Résident**) : le bloqueur de téléchargements nuisible pour Internet Explorer, et Tea Timer qui alerte en cas de modification de la base de registre. Ce dernier est très utile, mais un novice peut rester perplexe devant certains affichages : le fait de savoir s'il faut oui ou non autoriser une modification signalée, peut ne pas paraître évident.
L'antispyware de Microsoft (version bêta gratuite pour le moment) a également bonne réputation. Il comporte une mise à jour automatique et assure une protection en temps réel en cas d'intrusion.

On peut avoir plusieurs antispywares sans problème sur l'ordinateur.
Télécharchez Ad-Aware 2007 Free
Pack pour l'affichage en français
Téléchargez Spybot Search and Destroy
Téléchargez l'antispyware de Microsoft

La vaccination est une opération qui consiste (pour l'essentiel) à modifier la base de registre de façon à bloquer l'installation (ou s'ils sont déjà présents sur l'ordinateur, l'activation) de nombreux malwares, spécialement ceux qui utilisent la technique ActiveX.

Spybot possède une fonction de vaccination.

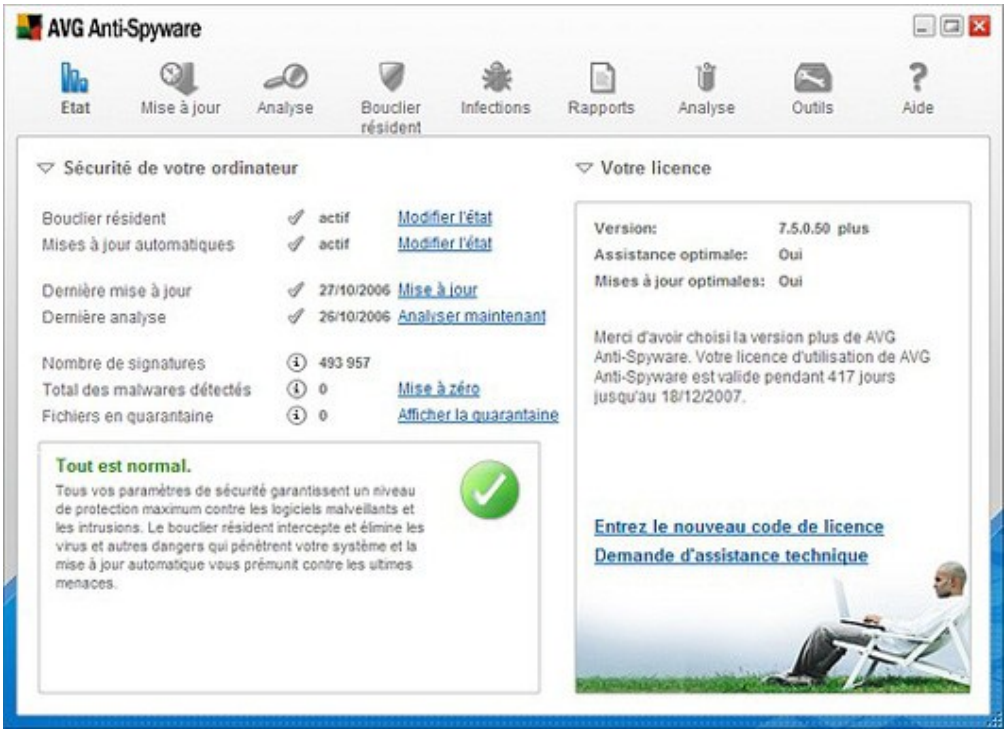
SpywareBlaster est uniquement dédié à cet usage et protège également contre les quelques rares mal-wares qui s'attaquent à Firefox.

Il faut mettre à jour périodiquement les bases de données de ces programmes et revacciner ensuite. La conjonction de ces deux programmes permet de bloquer plusieurs milliers de programmes illicites.
Téléchargez SpywareBlaster

Le blocage ou la limitation de l'accès à certains sites réputés dangereux (car contenant des pages ou des programmes piégés) peut se faire de deux manières : **Spybot** peut ajouter au fichier **hosts** normalement présent sur tous les ordinateurs une liste de sites dangereux (aucun navigateur ne pourra alors les

atteindre). **IE-SPYAD** (également gratuit) rajoute une liste de sites dangereux dans la liste des sites sensibles d'**Internet Explorer** (et uniquement lui). SpywareBlaster possède une option comparable. Le navigateur accède à ces sites avec le niveau de sécurité maximum possible. **Attention :** il peut y avoir des conflits mineurs entre les règles introduites par IESpad et celles de Spybot et SpywareBlaster. Il est donc recommandé de réutiliser les fonctions de protections de ces deux programmes après avoir installé celles de IE-SPYAD
Téléchargez IE-SPYAD

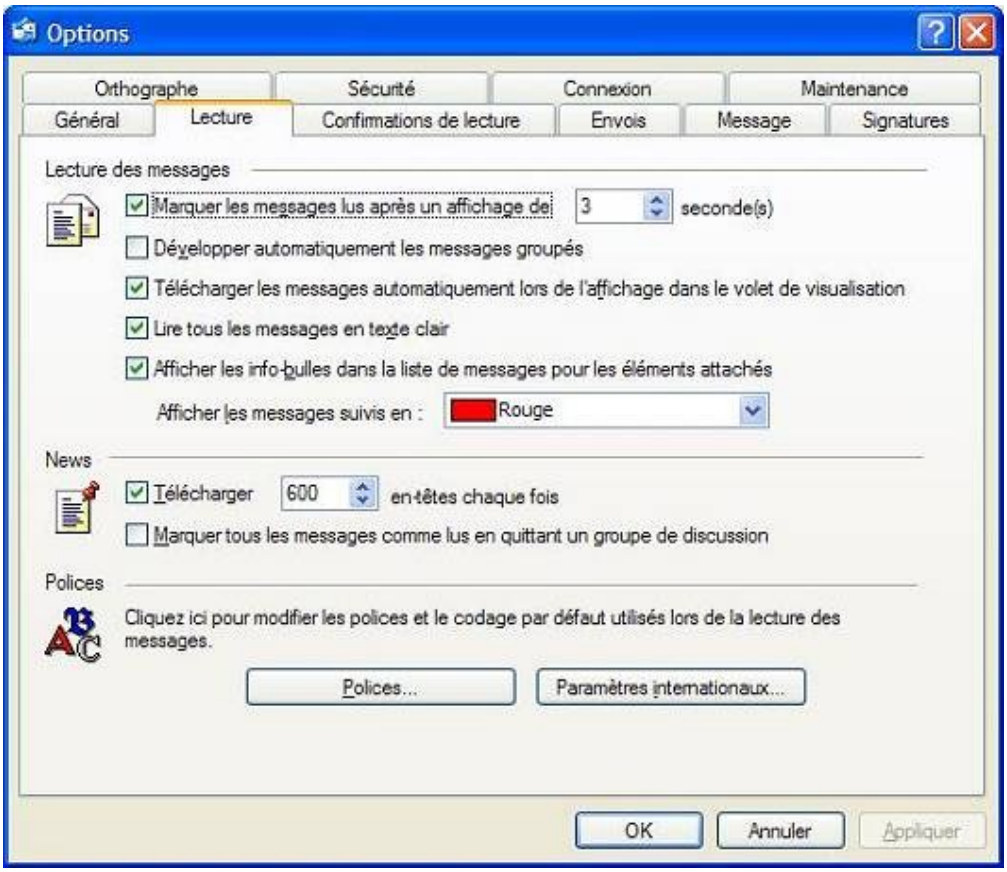
AVG Anti-Spyware (anciennement Ewido) est un programme qui est consacré aux spywares, hijackers, vers, dialers, chevaux de Troie et keyloggers. Il semble avoir une très bonne réputation d'efficacité. La version téléchargée a toutes les fonctionnalités pendant deux semaines.
Au bout de ce délai la surveillance en temps réel et la mise à jour automatique sont désactivées si vous n'avez pas acheté le programme, mais il est toujours possible de faire les mises à jour manuellement et de se servir du programme pour scanner l'ordinateur.



Téléchargez AVG Anti-Spyware

Internet Explorer et Outlook Express sont les programmes les plus visés par les créateurs de malwares. En outre ils incorporent la technologie ActiveX qui les rend potentiellement vulnérables. **Vous améliorerez grandement votre sécurité en utilisant comme navigateur Firefox ou Opera, et Thunderbird comme programme de courrier.**
Vous garderez **Internet Explorer** uniquement pour aller sur **Windows** Update ou pour lire quelques pages qui ont été codées (hélas) uniquement pour ce navigateur. Et n'oubliez pas que **dans Internet Explorer** il existe, **Outils, Options Internet**, un volet Sécurité qui permet de régler celle-ci à un niveau plus ou moins élevé. Réglez-la au niveau le plus élevé possible compatible avec les sites que vous avez l'habitude de consulter, si vous persistez à utiliser ce navigateur.

Si, pour des raisons qui vous regardent, vous souhaitez continuer à utiliser **Outlook Express**, **dans Outils, Options, Lecture** cochez la ligne **Lire tous les messages en [texte clair](#).** Certes l'affichage sera moins beau, mais vous serez à l'abri de surprises.



Remarque : il est possible de durcir encore la sécurité de Firefox en contrôlant l'utilisation du [javascript](#) ; ceci n'est pas exposé ici car les réglages peuvent désorienter l'utilisateur de base.

[Téléchargez Firefox](#)

[Téléchargez Thunderbird](#)

Téléchargez Opera

Un adage de la sécurité informatique est que la faille principale du système se trouve entre le clavier et la chaise. **Ceci signifie que vous éviterez à peu près tous les ennuis en adoptant un comportement raisonnable.**
La plupart des vers ou virus arrivent par mail : utilisez donc toujours la dernière version de votre programme de mail, corrigée des failles connues. N'ouvrez jamais les pièces jointes et ne cliquez jamais sur un lien d'un message dont vous ne connaissez pas l'expéditeur. Même si vous connaissez l'expéditeur, assurez-vous bien que l'envoi de cette pièce jointe est plausible : votre correspondant a pu se faire infecter à son insu, ou bien ce peut être une usurpation d'identité (le plus classique actuellement).
D'autres programmes nocifs peuvent arriver par messagerie instantanée ou se trouver sous des noms très attractifs, mais fallacieux, dans des ordinateurs offrant des fichiers en P2P. **N'oubliez pas, comme cela a été dit plus haut, que tout nouveau fichier arrivant sur votre ordinateur doit être scanné par votre antivirus, même si c'est un document Word, une archive .zip, ou une image.**
Certains malwares peuvent contaminer l'ordinateur simplement par l'ouverture d'une page ou d'une image piégées. Même si vous avez appliqué les mesures de sécurité ci-dessus, évitez les sites qui vous semblent plutôt « border line » par exemple par leur contenu photographique ou par la mise à disposition en téléchargement de programmes qui ne devraient se trouver que dans le circuit commercial.
Le dernier conseil concerne plutôt votre propre protection : évitez le phishing. Votre banque, compagnie d'assurance, service de paiement en ligne… ne vous contacteront jamais par mail pour vous demander vos mots de passe, vos coordonnées de carte bancaires, même si ces message vous paraissent bien imités et vous offrent de cliquer sur un lien qui semble être de celui de la banque, par exemple. Ce sont en réalité des sites imités pour vous mettre en confiance et pour vous soutirer des informations qui serviront à exploiter vos comptes à votre insu.
N'hésitez pas à venir poser toutes vos questions sur notre forum informatique