

# Les bonnes pratiques de sécurité

par Cédric Chatelain ([Pages perso](#))

Date de publication : 14/07/2004

Dernière mise à jour : 05/11/2006

Les menaces se multipliant ces derniers temps (virus, vers, spyware, intrusions), il est primordial de savoir quelles attitudes et actions adopter pour se prémunir et réagir aux problèmes de sécurité. A côté de ça un autre problème (le spam) augmente aussi de manière inquiétante...

Ce texte a été rédigé grâce aux remarques des différents internautes sur notre forum, et notamment les posts de ce sujet : <http://www.developpez.net/forums/viewtopic.php?p=1021600#1021600>. N'hésitez pas à venir y donner votre avis !

Merci

- 1 - Vérifiez vos informations
- 2 - les courriers non sollicités (le spam)
  - 2.1 - Ce qu'il faut savoir sur le spam
  - 2.2 - S'en protéger
- 3 - Se protéger contre les spywares
  - 3.1 - Ce qu'il faut savoir sur les spywares
  - 3.2 - Liens utiles pour enlever les spywares
- 4 - Se protéger contre les virus
  - 4.1 - L'attitude à adopter pour éviter les virus
  - 4.2 - Liens utiles pour lutter contre les virus
  - 4.3 - Les sites de base sur la sécurité et les virus
  - 4.4 - Les Chevaux de Troie
  - 4.5 - Adresses de laboratoires d'antivirus où envoyer éventuellement vos bêtes
- 5 - Se protéger des intrusions
  - 5.1 - Quel pare-feu ?
  - 5.2 - Testez votre sécurité
- 6 - Fermer les services inutiles
  - 6.1 - Sous Windows
  - 6.2 - Conseils pour les services sous Linux
- 7 - Les mots de passe

## Merci

Merci à **Marc Lussac**, **Florian**, **I.sage**, **iubito** et **Katyucha** pour les informations qui ont permis de rédiger cet article. Merci aussi à **Ricky81**, **HRS** et **Pascal Jankowski** pour les corrections effectuées.

## 1 - Vérifiez vos informations

Ne sombrez pas dans la paranoïa et vérifiez vos sources d'information, car quelques fois les remèdes que l'on vous conseille sont pires que les maux qu'ils sont censés soigner# Donc, si vous recevez un message alarmiste, vérifiez le. Un site permet cette vérification : <http://www.hoaxbuster.com/>.

## 2 - les courriers non sollicités (le spam)

### 2.1 - Ce qu'il faut savoir sur le spam

Tout ce que veulent les spammeurs, c'est recueillir un maximum d'adresses de courrier électronique valides.

Par conséquent:

- Ne répondez jamais à un spam (d'ailleurs la plupart du temps les adresses d'origine sont fausses).
- N'utilisez jamais les liens pour vous désinscrire, vous ne feriez que valider votre adresse, et la quantité de spam ne fera qu'augmenter
- Les pseudos-sites vous inscrivant sur des listes pour ne plus avoir de spam sont des escroqueries, vous recevrez encore plus de spam.

Un très bon site (en anglais) sur le spam:

 <http://www.spamhaus.org/>

### 2.2 - S'en protéger

- Ne faites **jamais** suivre des chaînes vous recevrez dans 99% des cas des virus sur votre adresse e-mail : pourquoi ? Le champ servant à masquer les destinataires est en effet peu utilisé, et les listes des destinataires restent dans le corps du message. Ainsi, la première machine infectée recevant cette chaîne dispose de plusieurs centaines d'adresses e-mail valides à infecter.. Faites pression sur vos contacts pour qu'ils ne vous envoient pas ces chaînes....
- Evitez de donner votre adresse de courrier électronique "n'importe où".
- Créez une boîte aux lettres "poubelle" que vous utiliserez si vous devez fournir une adresse de courrier électronique pour vous inscrire sur un site autre qu'un site de "confiance" (banque, enseigne connue,etc.).
- Utilisez un filtre anti-spam :

Le logiciel MailWasher est particulièrement adapté pour cette fonction. Le principe est qu'il va interroger vos courriers, et vous permettre, sans avoir besoin de les récupérer, de décider si vous voulez les détruire ou les récupérer par la suite. Ce filtrage en amont permet d'éviter les pièges des nouveaux courriers publicitaires, où le simple affichage d'une image permet à l'expéditeur de savoir que votre adresse est valide.

Ce logiciel inclus un système de liste noire/liste d'amis, qui vous fera gagner du temps dans le filtrage de vos courriers.

Site de ce logiciel:  <http://www.mailwasher.net>

Ce logiciel inclut une fonction très utile: il peut envoyer un faux message d'erreur, afin de faire croire que votre adresse de courrier électronique est invalide. Utilisez systématiquement cette option afin de faire diminuer le nombre de courriers de type spam que vous recevrez.

Cliquez ensuite sur "Free download".

La configuration est simple, vous aurez besoin de vos codes de messagerie (ceux fournis lors de votre abonnement).

## 3 - Se protéger contre les spywares

### 3.1 - Ce qu'il faut savoir sur les spywares

Les spywares sont des espions qui récoltent des informations quand vous naviguez sur internet. Les spywares sont souvent présent dans les version gratuites de certains logiciels et récoltent des informations à but commercial.

Ils envoient donc, à votre insu, des données sur internet.

### 3.2 - Liens utiles pour enlever les spywares

Un bon anti-spyware que j'ai trouvé s'appelle spybot :  <http://www.safer-networking.org/en/index.html>

Il y a aussi AdAware de Lavasoft:  
 [http://www.lavasoft.com/download\\_and\\_buy/product\\_comparison\\_chart.php](http://www.lavasoft.com/download_and_buy/product_comparison_chart.php) gratuit et sans spyware

Et plein d'autres, là :  <http://assiste.free.fr/>

## 4 - Se protéger contre les virus

### 4.1 - L'attitude à adopter pour éviter les virus

- Si vous recevez par courrier électronique un message d'un inconnu, surtout si c'est dans une langue étrangère, avec une pièce jointe, ce message contient quasiment toujours un virus : supprimez le sans le lire. Cette simple précaution suffit à éliminer la plupart des virus.

- Installez un antivirus et mettez le à jour. Norton Antivirus inclut un an de mise à jour après l'installation.

- Installez les mises à jour de sécurité via Windows Update (Démarrer > Windows Update) pour les ordinateurs sous Windows, ou le système correspondant à votre OS. Ces virus s'en prennent aux machines connectées à Internet, sans que vous ayez eu à exécuter un logiciel infecté.

En cas de problème vous pouvez consulter le support Microsoft :

 <http://support.microsoft.com/default.aspx>

### 4.2 - Liens utiles pour lutter contre les virus

Antivirus gratuits en ligne :

 <http://webscanner.kaspersky.fr/>

 <https://fr.mcafee.com/root/mfs/default.asp>

 [http://www.pandasoftware.com/activescan/fr/activescan\\_principal.htm](http://www.pandasoftware.com/activescan/fr/activescan_principal.htm)

 [http://housecall.trendmicro.com/housecall/start\\_corp.asp](http://housecall.trendmicro.com/housecall/start_corp.asp)  <http://www.secuser.com/antivirus/> (même moteur)

 <http://security.symantec.com/fr/sscv6/>

F-Prot (sous DOS):


 <http://www.f-prot.com/f-prot/download/>

Avec utilitaires de mises à jour automatiques pour F-Prot:

 <ftp://ftp.F-Secure.com/anti-virus/updates/f-prot/fp-def.zip>

Page de mode d'emploi en français:  <http://claymania.com/f-prot-fr.html>

AntiVir (sous Windows)

 <http://www.free-av.com> Inconvénient: la MAJ remet à jour les définitions de virus ET le moteur d'inférence (dans 80% des cas), ce qui est assez long.(# 3Mo).

AVG 7

 [http://www.grisoft.com/us/us\\_dwnl\\_free.php](http://www.grisoft.com/us/us_dwnl_free.php) [AVG 7 est maintenant gratuit]

Avast 32

 <http://www.avast.com/> (plutôt complexe, mais un mode d'utilisation "simple" est disponible)

#### 4.3 - Les sites de base sur la sécurité et les virus

 <http://www.lacave.net/~jokeuse/usenet/faq-fcsv.html>

 <http://www.claymania.com/safe-hex-fr.html>

 <http://www.claymania.com/nav-map-fr.html>

 <http://sebsauvage.net/safehex.html>

 <http://assiste.free.fr/>

Quelques comparatifs sur les antivirus :

 [http://www.messagerie-antivirus.com/comparatif\\_antivirus.shtm](http://www.messagerie-antivirus.com/comparatif_antivirus.shtm)

 <http://eservice.free.fr/comparatif-antivirus.html>

 <http://www.claymania.com/tests-trojan-fr.html>

#### 4.4 - Les Chevaux de Troie


Parmi les modes de propagation de virus, le cheval de Troie est très répandu. Il consiste à placer le programme infecté à l'intérieur d'un autre programme ou d'un document exécutable.

L'exécution de celui-ci, ou son ouverture, entraîne l'activation du virus, qui infecte le système et se propage à d'autres ordinateurs.

Voici quelques liens utiles :

The cleaner  <http://www.moosoft.com/>

Pest patrol  <http://www.regnow.com/softsell/nph-softsell.cgi?item=5957-1> (payant)

Tauscan  <http://esales.element5.com/product.html?productid=133013&languageid=1&affiliateid=71907>  
(démonstration gratuite)

(Liste non exhaustive)

#### 4.5 - Adresses de laboratoires d'antivirus où envoyer éventuellement vos bêtes

BitDefender: [virus\\_submission@bitdefender.com](mailto:virus_submission@bitdefender.com)

CAI (IPE), Vet: [ipevirus@vet.com.au](mailto:ipevirus@vet.com.au)

Eset (NOD32): [samples@nod32.com](mailto:samples@nod32.com)

Frisk (F-Prot):  [http://www.f-prot.com/virusinfo/submission\\_form.html](http://www.f-prot.com/virusinfo/submission_form.html)

F-Secure: [samples@f-secure.com](mailto:samples@f-secure.com)

H+BEDV (AntiVir): [virus@antivir.de](mailto:virus@antivir.de)

Kaspersky (AVP): [submit-virus@avp.ch](mailto:submit-virus@avp.ch)

NAI (McAfee): [virus\\_research@nai.com](mailto:virus_research@nai.com)

Norman: [analysis@norman.no](mailto:analysis@norman.no)

Panda Software [virus@pandasoftware.com](mailto:virus@pandasoftware.com)

RAV:  <http://www.ravantivirus.com/support/submit-file.php>

Sophos: [support@sophos.com](mailto:support@sophos.com)

Symantec (Norton): [avsubmit@symantec.com](mailto:avsubmit@symantec.com)

Trend Micro: [virus\\_doctor@trendmicro.com](mailto:virus_doctor@trendmicro.com)

Quelques statistiques (surprenantes!) sur l'efficacité des programmes anti-troyens et anti-backdoors:

 <http://www.claymania.com/tests-trojan-fr.html>

## 5 - Se protéger des intrusions

### 5.1 - Quel pare-feu ?

une liste de très bons pare-feux (utilitaires évidemment in-dis-pen-sa-bles en cas de connexion DSL/câble) :

- Outpost Agnitum [version "lite" gratuite]  <http://www.agnitum.com/products/outpost/>
- Kerio Personal Firewall [gratuit]  <http://www.sunbelt-software.com/Kerio.cfm> Pour Moi le meilleur...
- Look'n Stop [une version d'évaluation]  <http://www.looknstop.com/Fr/index2.htm>
- Zone Alarm [version "légère" gratuite, et amplement suffisante pour un usage classique]  <http://www.zonelabs.com> La version "pro" consomme une quantité importante de ressources CPU.

Comparatif Firewall :  <http://www.firewall-net.com/fr/home/comparatif.php>

### 5.2 - Testez votre sécurité

 <https://grc.com/x/ne.dll?bh0bkyd2>

 <http://www.grc.com/files/dcombob.exe> utilitaire pour protéger un port

 <http://check.sdv.fr:3658/cgi/scan?>

 <http://security.symantec.com/fr/sscv6/>

## 6 - Fermer les services inutiles

Il est important de ne pas lancer de services inutiles. Les ressources libérées en mémoire et en CPU peuvent alors servir aux applications de sécurité (firewall et antivirus) et évitent aux failles de sécurité de devenir critiques. De plus, certains services, de par leur fonctionnement peuvent directement poser des problèmes de sécurité. D'autres, au contraire, sont indispensables au bon fonctionnement de votre PC.

### 6.1 - Sous Windows

| Service                                  | Description (la description est dans le panneau de configuration)   | Conseil   |
|--|---|---|
| <b>Accès à distance au Registre</b>      | Permet aux utilisateurs à distance de modifier les paramètres du Registre sur cet ordinateur.   | Ce service <b>doit être "désactivé"</b> , les raisons de sécurité sont évidentes.   |
| <b>Acquisition d'image Windows (WIA)</b> | Fournit des services d'acquisition d'images pour les scanners et les appareils photo.   | Ce service peut être mis sur "manuel" sans perturber le bon fonctionnement, passez le en "automatique uniquement si vous constatez un problème lors de l'utilisation de votre scanner ou de votre appareil photo numérique. |
| <b>Affichage des messages</b>            | Envoie et reçoit les messages des services d'alertes entre les clients et les serveurs. Ce service n'est pas lié à Windows Messenger. Si ce service est arrêté, les messages d'alertes ne seront pas transmis. Si ce service est désactivé, les services qui en dépendent ne pourront pas démarrer.     | Ce service <b>doit être "désactivé"</b> . Il constitue le moyen privilégié de vous faire parvenir de la publicité ou de vous attirer sur un site "piège".   |
| <b>Aide et support</b>                   | Permet à l'application Aide et support de fonctionner sur cet ordinateur. Si ce service est arrêté, la fonctionnalité Aide et support ne sera pas disponible. S'il est désactivé, tous les services dépendant explicitement de ce service ne pourront pas démarrer.                                     | Ce service peut être "désactivé" si vous pouvez vous passer de l'aide Windows, sinon vous pouvez le laisser en "manuel".  |
| <b>Application système COM+</b>          | Gère la configuration et le suivi des composants de base COM+ (Component Object Model) . Si le service est arrêté, la plupart des composants de base COM+ ne fonctionneront pas correctement. Si ce service est désactivé, les services qui en dépendent de manière explicite ne pourront pas démarrer. | Vous pouvez laisser ce service en "automatique" pour conserver un bon fonctionnement plus "simple". Pour renforcer la sécurité vous pouvez le passer en "manuel".   |
| <b>Assistance TCP/IP NetBIOS</b>         | Permet la prise en charge pour NetBIOS sur un service TCP/IP  | Si vous êtes en réseau, laissez-le en "automatique". Dans le  |

|  |   |  |
|--|---|--|
|  | (NetBT) et la résolution des noms NetBIOS.  | cas contraire, vous pouvez le désactiver.  |
| <b>Audio Windows</b>   | Gère les périphériques audio pour les programmes basés sur Windows. Si ce service est arrêté, les périphériques et les effets audio ne fonctionneront pas correctement. Si ce service est désactivé, les services en dépendant explicitement ne démarreront pas.                    | Si vous utilisez votre carte son, laissez le en "automatique". Dns le cas contraire vous pouvez le désactiver.   |
| <b>Avertissement</b>   | Informe les utilisateurs et les ordinateurs sélectionnés des alertes administratives. Si ce service est arrêté, les programmes qui utilisent les alertes administratives ne les recevront pas. Si ce service est désactivé, les services qui en dépendent ne pourront pas démarrer. | Vous pouvez désactiver ce service sans risquer de problèmes particuliers.  |
| <b>Client DHCP</b>   | Gère la configuration réseau en inscrivant et en mettant à jour les adresses IP et les noms DNS.  | Si vous êtes en réseau avec des IP fixes, ou que vous n'êtes pas dans un réseau, vous pouvez le désactiver. Il n'y aura pas de disfonctionnement.  |
| <b>Client DNS</b>  | Résout et met en cache les noms DNS pour cet ordinateur. Si ce service est arrêté, l'ordinateur ne pourra pas résoudre les noms DNS et trouver les contrôleurs de domaine Active Directory. Si ce service est désactivé, les services qui en dépendent ne pourront pas démarrer.    | Vous pouvez le désactiver. Il n'y aura pas de disfonctionnement.   |
| <b>Compatibilité avec le Changement rapide d'utilisateur</b> | Fournit un système de gestion à des applications qui nécessitent de l'Assistance dans un environnement d'utilisateurs multiples.  | Si vous êtes le seul utilisateur, ou que vous changez rarement d'utilisateur sur votre PC, vous pouvez le désactiver.  |
| <b>Configuration automatique sans fil</b>                    | Permet le démarrage des processus sous d'autres informations d'identification. Si ce service est arrêté, ce type d'ouverture de session sera indisponible. Si ce service est désactivé, tout service en dépendant explicitement ne démarrera pas.                                   | Si vous n'utilisez pas de réseau sans fil, vous pouvez le désactiver.  |
| <b>Connexion secondaire</b>                                  | Permet le démarrage des processus sous d'autres informations d'identification. Si ce service est arrêté, ce type d'ouverture de session sera indisponible. Si ce service  | Ce service peut poser des problèmes de sécurité et le mettre en manuel ne suffit pas. <b>Il faut le désactiver.</b> <i>Attention toutefois aux applications qui ont une option "lancer avec un compte restreint"</i> |

|   |  |   |
|---|--|---|
|   | est désactivé, tout service en dépendant explicitement ne démarrera pas.   | <i>et qui en auront besoin si cette dernière est activée.</i>   |
| <b>DSDM DDE réseau</b>                    | Gère l'échange dynamique de données partagées de réseau. Si ce service est arrêté, l'échange dynamique de données partagées de réseau ne sera plus disponible. Si ce service est désactivé, tout service en dépendant explicitement ne démarrera pas.  | Vous pouvez le désactiver si vous n'utilisez pas de réseau.   |
| <b>Explorateur d'ordinateur</b>           | Tient à jour une liste des ordinateurs présents sur le réseau et fournit cette liste aux ordinateurs désignés comme navigateurs. Si ce service est arrêté, la liste ne sera pas mise ou tenue à jour. Si ce service est désactivé, les services qui en dépendent ne pourront pas démarrer.   | Vous pouvez le désactiver si vous n'utilisez pas de réseau.   |
| <b>Gestionnaire de l'Album</b>            | Active le Gestionnaire de l'Album afin de stocker les informations et les partager avec des ordinateurs à distance. Si le service est arrêté, le Gestionnaire de l'Album ne pourra pas partager les informations avec des ordinateurs à distance. Si ce service est désactivé, tout service en dépendant explicitement ne démarrera pas. | Ce service peut être désactivé si il n'y a pas de partage avec une machine distante.  |
| <b>Horloge Windows</b>                    | Conserve la synchronisation de la date et de l'heure sur tous les clients et serveurs sur le réseau. Si ce service est arrêté, la synchronisation de la date et de l'heure sera indisponible. Si ce service est désactivé, tout service en dépendant explicitement ne démarrera pas.   | Si vous pouvez vous passer de la mise à l'heure depuis le internet, désactivez ce service.  |
| <b>Journal des événements</b>             | Active les messages d'événements émis par les programmes fonctionnant sous Windows et les composants devant être affichés dans l'observateur d'événements. Ce service ne peut être arrêté.   | Si vous ne consultez pas le journal des événements, vous pouvez le passer en "manuel". La modification prend effet après le redémarrage de Windows. |
| <b>Journaux et alertes de performance</b> | Collecte les données de performances des ordinateurs locaux ou distants basés sur des paramètres planifiés préconfigurés, puis écrit les données dans un journal ou déclenche une alerte. Si ce service est arrêté, les informations de performances ne seront pas collectées. Si ce   | Il est préférable de désactiver ce service. Aucune perturbation ne devrait en résulter.   |

|  |  |   |
|--|--|---|
|  | service est désactivé, tout service en dépendant explicitement ne démarrera pas.                 |   |
| <b>Partage de Bureau à distance NetMeeting</b> | Permet aux personnes autorisées d'accéder à votre Bureau Windows en utilisant NetMeeting.        | Il faut <b>désactiver ce service</b> pour des raisons évidentes de sécurité.                              |
| <b>Routage et accès distant</b>                | Offre aux entreprises des services de routage dans les environnements de réseau local ou étendu. | Comme tout ce qui permet des accès distants, pour des raisons de sécurité, <b>il faut le désactiver</b> . |

## 6.2 - Conseils pour les services sous Linux

Mon expérience Linux est assez restreinte, mais nous allons essayer de faire le tour des services linux potentiellement dangereux pour votre PC.

| Service        | Description   | Conseil   |
|----------------|---|---|
| fingerd        | Ce service fournit des informations sur les utilisateurs déclarés dans votre système. | Il est préférable, au minimum, de le rendre inaccessible depuis internet et, au mieux, de le désactiver.  |
| ftpd           | C'est un serveur FTP.   | Il a connu de nombreux bugs. Il est préférable d'utiliser un autre serveur FTP ou de se contenter du user "anonymous", mais en aucun cas d'utiliser les users du système. |
| httpd (Apache) | C'est le serveur Web.   | Utilisez-le seulement si vous avez besoin d'un serveur Web. Assurez-vous que votre version de PHP est à jour, et désactivez le PHP si vous ne l'utilisez pas.             |
| telnetd        | Permet la prise de contrôle à distance du poste                                       | Il est fortement recommandé de désactiver ce service.   |

Vous trouverez des éléments intéressants pour sécuriser linux dans l'article de Nicolas Vallée : [Mise en place d'une passerelle "sécurisée" pour le partage d'une connexion internet](#)

Si vous avez d'autres suggestions, n'hésitez pas à me les faire parvenir par MP ou par mail (il y a un lien vers mon profil forum en haut de cet article).

## 7 - Les mots de passe

Les mots de passe, que ce soit sur votre PC ou sur une application internet (webmail, forum, etc...) sont une cible d'attaques. Les attaques se font principalement sous 2 formes :

- dictionnaire des mots de passe les plus fréquents
- brutforce

Le mot de passe ne doit donc, ni être un mot commun, ni être facile à trouver. De plus il doit avoir une longueur suffisante (6 caractères me semble être le minimum passable) et être composé de minuscules, majuscules, chiffres et caractères spéciaux (si ces derniers sont acceptés) tels @\*ù\$#{[]}()-\_ ou de ponctuations ,;: afin de compliquer au maximum une attaque brutforce (attaque dans laquelle toutes les combinaisons possibles sont testées en mot de passe). Un mot de passe généré aléatoirement est ce qu'il y a de mieux. De tels générateurs existent, en extensions firefox ou en widgets opéra par exemple.

Afin que votre mot de passe reste une protection efficace de vos données personnelles, vous devriez suivre les recommandations suivantes :

- Un mot de passe est personnel : ne le confiez jamais à un tiers, ne l'écrivez pas sur un post it collé sur l'écran...etc
- Evitez tant que possible d'avoir le même mot de passe sur 2 (ou plus) applications différentes.
- un mot de passe doit être changé régulièrement

Si vous devez mettre en place une politique de mot de passe au sein d'une application ou d'un système, il arrive souvent d'avoir des utilisateurs très récalcitrants. C'est alors à vous de faire preuve à la fois de diplomatie mais aussi de sévérité pour que soit respectée cette politique.

Il existe des programmes tel que John The Ripper sous Unix qui permettent de faire une attaque de force brute sur vos fichiers de mot de passe. C'est très intéressant de montrer aux utilisateurs non informaticiens, comment un mot de passe faible est si facilement trouvable.

