

**CRI74 : Comment lutter contre les spams ?**

# Sommaire

<b><u>1. Introduction</u></b> .....	<b>1</b>
<b><u>2. Informations générales sur les spams</u></b> .....	<b>2</b>
<u>2.1. Qui envoie des spams ?</u> .....	2
<u>2.2. Pourquoi envoyer des spams ?</u> .....	2
<u>2.3. Comment ont-ils trouvé mon adresse e-mail ?</u> .....	2
<u>2.3.1. Votre fournisseur d'accès l'a cédée :</u> .....	2
<u>2.3.2. Vous l'avez communiquée sur un site web :</u> .....	2
<u>2.3.3. Vous l'avez publiée sur Internet :</u> .....	2
<u>2.4. Que faire pour ne plus recevoir autant de spams ?</u> .....	3
<b><u>3. Les URLs de référence, principalement en français, sur les SPAMS :</u></b> .....	<b>4</b>
<b><u>4. Les solutions logicielles</u></b> .....	<b>5</b>
<b><u>5. Spamihilator</u></b> .....	<b>6</b>
<u>5.1. Généralités sur ce logiciel</u> .....	6
<u>5.2. Principe de fonctionnement</u> .....	6
<u>5.3. Le filtrage des messages</u> .....	7
<u>5.3.1. Filtrage sur mots clés</u> .....	7
<u>5.3.2. Filtrage sur l'adresse email émettrice</u> .....	8
<u>5.3.3. Utilisation de la zone d'apprentissage</u> .....	8
<u>5.3.4. Filtrage à l'aide de plug-ins (ou "greffons")</u> .....	9
<u>5.4. Installation</u> .....	10
<u>5.5. Personnalisation de la configuration</u> .....	11

# 1. Introduction

Depuis le début de l'année 2003, le nombre de spams que nos utilisateurs reçoivent ne cesse d'augmenter. Les boîtes aux lettres font effectivement de plus en plus souvent l'objet d'une pollution par voie électronique par toutes sortes de mails publicitaires vantant les mérites de produits pharmaceutiques pour la plupart, mais aussi les cartouches d'encre pour imprimante à prix canon, certains invitant à fréquenter des sites pornographiques, et dernièrement, des logiciels anti-spams, un comble !

Certaines solutions pourraient être mises en place pour limiter ces spams au niveau des serveurs de messagerie du CRI74. Néanmoins, aucun système fiable et répondant aux aspects de légalité n'existe vraiment. Le problème est le même que pour un système anti-virus. Il faudrait que chaque usager puisse activer/désactiver ce système pour sa boîte email et qu'il soit pleinement conscient des risques encourus. Si, techniquement, des réponses pourraient être apportées pour limiter un peu la diffusion des spams, il n'est pas envisageable pour l'instant que le CRI74 décide d'imposer un tel système pour tous ses utilisateurs.

Néanmoins, pour limiter la gêne occasionnée, il existe des possibilités de filtrage à mettre en place sur l'ordinateur depuis lequel on a l'habitude de relever ses mails. Il faut aussi prendre des bonnes habitudes et avoir une connaissance du phénomène pour y trouver des parades.

Cette documentation a donc pour but de donner des informations utiles sur les spams et les moyens efficaces qui existent et que le CRI préconise pour lutter contre eux.

Les logiciels qui sont référencés ici ne couvrent pas toutes les solutions qui existent. Nous avons juste chercher parmi les solutions gratuites, efficaces et libres de préférence, celles qui pouvaient être envisagées dans un déploiement à grande échelle parmi nos utilisateurs.

[Retour au [sommaire](#)]

## 2. Informations générales sur les spams

Ce chapitre est une recopie exacte des informations présentées dans la première partie du CRI Pratique n°4 (voir <http://www.cri74.org/pratique/index.html>)

### 2.1. Qui envoie des spams ?

Les publicitaires et les services marketing des entreprises sont les premiers émetteurs de spams pour promouvoir produits, services, ou pour inciter les internautes à visiter leur site web. Les spams à caractère pornographique sont également de plus en plus nombreux.

### 2.2. Pourquoi envoyer des spams ?

Le spamming est employé massivement parce qu'il présente des avantages certains pour ses émetteurs : l'envoi de courrier électronique est bien moins onéreux que l'envoi de publicité papier, les adresses e-mail sont facilement trouvables, et le profil des internautes simple à esquisser.

Mais pour le destinataire, le spam engendre une grande perte de temps (et d'argent) : les temps de téléchargement inutiles augmentent les temps de connexion lorsqu'il relève son courrier, et, surtout, le temps nécessaire pour trier tous ces messages, au risque de supprimer un message important...

### 2.3. Comment ont-ils trouvé mon adresse e-mail ?

Les spammeurs disposent de plusieurs moyens pour récupérer votre adresse :

#### 2.3.1. Votre fournisseur d'accès l'a cédée :

En revendant sa liste d'abonnés à un tiers, qui lui-même l'a revendue à un autre, etc., votre FAI a permis la diffusion de votre adresse en de nombreux exemplaires sur Internet. Attention, l'opération est légale si vous avez accepté que votre adresse soit diffusée (ou plutôt si vous n'avez pas pensé à décocher la petite case située, s'il y en a une, en bas du formulaire d'inscription, vous informant que votre adresse, sauf avis contraire de votre part, sera utilisée à des fins commerciales).

#### 2.3.2. Vous l'avez communiquée sur un site web :

En passant une commande sur un site de commerce électronique, en souscrivant à des services via un site web, en vous inscrivant sur une liste de diffusion par courrier électronique, vous avez forcément laissé une adresse e-mail. Là encore, si vous avez oublié de décocher la petite case qui figure en bas du formulaire, vous avez autorisé la diffusion de cette adresse.

#### 2.3.3. Vous l'avez publiée sur Internet :

En l'indiquant sur votre page personnelle, en la laissant sur des forums de discussion ou dans

une newsgroups, vous êtes susceptible d'intégrer un fichier d'adresses récupérées à l'aide de logiciels spécialisés : des « robots », comme ceux des moteurs de recherche, qui débusquent toutes les adresses e-mail à partir de sites web ou de forums de discussion, ou encore des générateurs automatiques d'adresses e-mail (dès lors que vous réservez un nom de domaine, vous pouvez vous attendre à recevoir des spams sur webmaster@..., contact@..., etc.).

## **2.4. Que faire pour ne plus recevoir autant de spams ?**

Créez-vous une seconde adresse de messagerie que vous n'utiliserez que pour passer des commandes en ligne ou que pour participer aux forums de discussion. Cette parade est plutôt symbolique puisqu'elle ne vous protégera pas plus des spams. Mais c'est à cette seconde adresse que vous les recevrez, épargnant ainsi votre adresse professionnelle ou votre adresse personnelle.

Utilisez un outil de lutte anti-spam, qui propose des options plus poussées que celles des logiciels de messagerie (voir chapitres correspondants dans cette documentation).

[Retour au [sommaire](#)]

### 3. Les URLs de référence, principalement en français, sur les SPAMS :

La liste ci-dessous regroupe quelques adresses qu'on considère être des références dans le domaine. Si vous connaissez d'autres sites extrêmement intéressants qui traitent du sujet, n'hésitez pas à nous en faire part afin qu'on les intègre à cette liste.

- ◆ 2 FAQs complémentaires, rédigées dans le cadre d'utilisation de newsgroups, mais dont des chapitres sont aussi consacrés/correspondants aux spams par courrier électronique "classique"
  - ◇ <http://www.usenet-fr.net/fur/usenet/abus/reagir-general.html>
  - ◇ <http://www.usenet-fr.net/fur/usenet/abus/reagir-conseils.html>
- ◆ Les "officielles"
  - ◇ [http://www.cnil.fr/thematic/internet/spam/spam\\_sommaire.htm](http://www.cnil.fr/thematic/internet/spam/spam_sommaire.htm)
  - ◇ <http://www.caspam.org/>
  - ◇ <http://www.euro.cauce.org/fr/index.html>
- ◆ Les "autres" :
  - ◇ <http://www.arobase.org/spam/index.htm>
  - ◇ <http://www.panicinside.be/spam/introduction.html>
  - ◇ <http://www.halte-spam.com/>

[Retour au [sommaire](#)]

## 4. Les solutions logicielles

Les logiciels de messagerie "classiques" implémentent de plus en plus des solutions de filtrage élaborées pour limiter la pollution des boîtes aux lettres par les spams. Mozilla 1.4 par exemple propose l'installation d'un module anti-spam qui va filtrer les courriers indésirables au fur et à mesure que vous lui indiquez quels mails vous considérez comme des spams et lesquels doivent passer. On retrouve des systèmes similaires sur bon nombre de clients de messagerie depuis quelques temps. Les éditeurs de tels logiciels ont bien compris l'intérêt qu'ils avaient à proposer des outils répondant aux besoins des utilisateurs pour que ceux-ci s'orientent vers un logiciel de courrier plutôt qu'un autre. Afin de ne pas être dépendant d'un outil de messagerie et dans la mesure où ils ne proposent pas tous de tels systèmes, nous allons traiter ici de solutions indépendantes qui peuvent être utilisées quel que soit le logiciel de messagerie préféré par l'utilisateur.

Les logiciels gratuits, assez efficaces, en français qu'on peut conseiller pour lutter contre le spam "au niveau utilisateur" et qui font l'objet des chapitres suivants un peu plus dans le détail sont :

- ◆ MailWasher (pour Windows) – <http://www.mailwasher.net/> (et <http://www.framasoft.net/article388.html>) : outil gratuit en version limitée, disponible en français, qui s'installe sur l'ordinateur et qui permet de visionner les en-têtes des messages en attente sur le serveur, prévoir un tri en fonction de critères personnalisables et qui lance alors l'outil de messagerie pour ne récupérer que ceux qui doivent l'être (les autres étant supprimés sans être récupérés => risque de perte de mail)
- ◆ Spamihilator (pour Windows) – <http://www.spamihilator.com/> (et <http://www.framasoft.net/article1649.html>) : outil gratuit, multi-langue (dont le français), sous licence GPL, qui s'installe sur l'ordinateur et qui se place en intermédiaire entre le serveur de messagerie et l'outil de messagerie pour faire le tri lors de la relève des mails sur des critères personnalisables. Les messages sont alors tous relevés. Les messages supposés être des spams sont mis de côté et peuvent être réintégrés à l'outil de messagerie si on s'aperçoit qu'il s'agit d'un "vrai" mail.
- ◆ Spampal (pour Windows) – <http://spampal.corlobe.tk/> (et <http://www.framasoft.net/article1323.html>) qui fonctionne également en intermédiaire entre le client de messagerie et le serveur contacté mais qui a un fonctionnement basé sur l'utilisation de requêtes en direction de serveurs internationaux utilisés dans la lutte anti-spam. Pour l'instant, compte tenu de son fonctionnement "particulier", il va être testé également mais il ne sera pas retenu pour être recommandé à nos utilisateurs. Un chapitre expliquant tout de même son mode de fonctionnement permettra de se faire une opinion sur ce logiciel.

[Retour au [sommaire](#)]

# 5. Spamihilator

## 5.1. Généralités sur ce logiciel

Homepage du projet : <http://www.spamihilator.com>

Le développeur principal de ce logiciel est un allemand : [Michel Krämer](#)

Ce logiciel était un logiciel libre distribué sous licence GPL.

Depuis la version 0.9.7, l'auteur a décidé de le distribuer sous une licence particulière, sans donner toutes les sources du code car celui-ci a fait l'objet de "vol" à plusieurs reprises par d'autres éditeurs qui n'ont pas eu de scrupule à reprendre les sources en les modifiant légèrement et à revendre le tout, bafouant totalement les règles qui définissent la GPL. Donc, même si le logiciel n'est plus "opensource" (des portions de code devraient tout de même restées accessibles), son utilisation est tout à fait recommandable et je vous encourage personnellement à l'utiliser plutôt que n'importe quel outil commercial qui ne sera jamais plus efficace et qui risque d'avoir été basé sur le même "coeur".

Si le logiciel fonctionne déjà dans plus de 25 langues, la documentation "officielle" du logiciel n'existe actuellement qu'en anglais et en allemand (d'où cette documentation moins complète mais traitant des fonctionnalités principales du logiciel) et est accessible [en ligne](#) et une fois le logiciel installé dans le répertoire "help". Compte-tenu de l'intérêt que ce logiciel peut susciter pour les internautes du monde entier, une version française de la documentation officielle devrait voir le jour prochainement (mais le temps nécessaire au maintien d'une telle documentation n'est pas léger et il est nécessaire de pouvoir en assurer la pérennité).

## 5.2. Principe de fonctionnement

Plate-forme de fonctionnement : Microsoft Windows (testé notamment sur Win98SE mais doit fonctionner sur à peu près toutes les versions 32bits. Compte-tenu du fonctionnement en "proxy", il faut néanmoins avoir les autorisations nécessaires sous Windows XP Pro par exemple.)

Spamihilator est ce qu'on appelle un "proxy pop" car c'est un logiciel qui fonctionne en intermédiaire entre le client de messagerie et le serveur POP contacté (ne fonctionne pas avec IMAP/IMAPs pour l'instant). Lorsqu'on l'installe, il modifie les paramètres de l'outil de messagerie pour que celui-ci le contacte plutôt que le serveur de messagerie. Il transmet alors la requête de relève du courrier au serveur et fait le tri sur les messages rappatriés avant de les renvoyer vers l'application de messagerie utilisée.

Particularité : les serveurs POP du CRI74 supportent les POPs (voir [documentation concernant la configuration de l'outil de messagerie](#)). Spamihilator ne fonctionnera pas avec ce protocole sécurisé. Seul le protocole POP est supporté (pour l'instant).

Spamihilator n'agit bien entendu que sur la réception des messages et ne modifie en rien le processus d'envoi du courrier (sauf dans le rare cas où votre serveur SMTP nécessiterait une authentification pour l'envoi des messages. Ce n'est pas le cas au CRI.).

Spamihilator reconnaît automatiquement un grand nombre d'outils de messagerie les plus courants afin de modifier leur configuration et de la rétablir en cas de désinstallation du logiciel. Potentiellement, il peut être utilisé avec n'importe quel autre client POP qui ne serait pas reconnu. Dans un tel cas, une modification manuelle de la configuration de l'outil de messagerie serait nécessaire.

*Très important : étant donné que le logiciel va modifier les paramètres de l'outil de messagerie, il est nécessaire de disposer du mot de passe nécessaire pour relever les mails avec le compte configuré car il pourra être demandé après installation de Spamihilator.*

L'accès aux options du logiciels (qui sera résumé dans les futurs chapitres de cette documentation par "Paramètres") se fait en cliquant avec le bouton droit sur l'icône présente dans la barre des tâches et dans le menu qui apparaît, en choisissant "Paramètres" (ou "Settings" tant qu'on est en version anglaise).

## 5.3. Le filtrage des messages

Le filtrage des messages est basé sur plusieurs critères.

L'ordre de passage du mail dans les différents filtres est en partie configurable. Aussi, vous avez la possibilité de définir si, lorsqu'une règle de filtrage est reconnue, le mail doit être classé immédiatement spam/non spam ou s'il doit suivre son chemin au travers des autres règles de filtrage. Pour plus de simplicité, on considérera que l'utilisateur choisit que le mail sera catalogué dès qu'il sera reconnu dans une des chaînes de filtrage.

Pour prendre un exemple concret, si le filtrage sur l'attachement est défini avant le filtrage sur les mots interdits, un mail arrivant avec un type de fichier à bloquer sera placé en corbeille sans vérifier s'il contient ou non des mots clés banis.

Important : En tout état de cause, le filtrage sur l'adresse de l'émetteur est effectué en premier. Aussi, si un ami vous envoie un fichier avec une extension qui devrait être rejetée, le mail vous parviendra tout de même dans l'outil de messagerie.

### 5.3.1. Filtrage sur mots clés

Spamihilator va analyser les mails récupérés et y faire une reconnaissance syntaxique sur les mots présents dans le sujet et le corps du message. Toute chaîne de caractères est comparée à une liste de mots clés auxquels est affecté un pourcentage de probabilité de spam. Spamihilator va alors ajouter ces probabilités et si la somme dépasse le seuil défini par l'utilisateur, le message va être récupéré et stocké dans une corbeille interne à Spamihilator. Le message n'apparaîtra donc pas dans l'outil de messagerie.

Prenons un exemple concret et simple :

- ◆ l'utilisateur a défini un seuil de probabilité de spam à 100%
- ◆ le mot "sex" a une probabilité de 50%
- ◆ la chaîne de caractères "your money" : 60%
- ◆ lors de la réception du mail, Spamihilator détecte ces 2 expressions
- ◆ la somme des probabilités est faite :  $50+60=110\%$

- ◆ le seuil est dépassé, le mail est catalogué comme étant un spam et il est placé dans la corbeille de Spamihilator

### 5.3.2. Filtrage sur l'adresse email émettrice

Spamihilator permet de gérer 2 listes d'adresses email qui seront systématiquement comparées avec l'expéditeur du message qui est relevé. Si l'adresse est reconnue "amie" ou "proscrite", le message sera conservé ou placé dans la corbeille :

- ◆ une liste "noire" : pour définir les adresses émettrices que vous estimez être des spammers en puissance. Cette liste peut être éditée au coup par coup ou par l'importation d'une liste au format texte où les différentes valeurs sont séparées par un caractère spécial. Si vous configurerez Spamihilator de la sorte, les adresses que vous indiquerez ici seront proscrites et n'importe quel mail arrivant avec cette origine sera systématiquement placé dans la corbeille de Spamihilator.
- ◆ une liste "blanche" : pour définir les personnes dont on est sûr qu'il ne s'agit pas de spammers et dont les mails pourraient se retrouver "banis" s'ils contenaient les mots clés suspects. Il est possible de gérer un à un ces contacts, mais aussi d'importer ces informations depuis un carnet d'adresses de messagerie ou un fichier texte avec des séparateurs. Tout message en provenance d'adresses déclarées "amies" sera accepté et ne subira pas les autres types de filtrage.

### 5.3.3. Utilisation de la zone d'apprentissage

Le principe est simple, ce qui est fait derrière l'est moins...

Tous les messages récupérés restent pendant une durée limitée dans ce qui est appelée une "zone d'apprentissage". De temps en temps, l'utilisateur peut aller consulter les messages qui y sont présents (ceux qui ont été filtrés et ceux qui sont passés dans l'outil de messagerie) et préciser pour chaque s'il estime que c'est un spam ou un mail "normal". L'utilisateur déclenche alors un processus de parcours des messages et Spamihilator va analyser tous les mots présents et l'associer à un caractère "spam" ou "non spam". Un savant calcul de probabilité (basé sur des règles définies par le mathématicien anglais Thomas Bayes, XVIII<sup>e</sup> siècle) est fait sur chaque mot et cette probabilité sera appliquée par la suite sur les nouveaux messages qui seront réceptionnés. Ainsi, les mots, expressions les plus courantes dans les spams seront automatiquement reconnues sans avoir à les spécifier dans les mots clés. De même pour les messages "amis" (considérés comme n'étant pas des spams). Un message sera d'autant plus reconnu comme ami lorsqu'il contient beaucoup de similitudes avec les messages reçus précédemment des mêmes personnes ou types de personnes.

La visite régulière de cette zone d'apprentissage pour l'utilisateur va permettre d'avoir un filtrage de plus en plus efficace sans avoir à rajouter de mots clés au fur et à mesure que les spammers trouvent des astuces pour contourner ce filtrage "basique". S'il est aisé de modifier l'écriture de "viagra" (pour prendre un exemple ultra courant) en "VIAGRA", "\viagra", "VIAGRA", ... pour que les filtres sur le mot lui-même soient inefficaces, étant donné que les méthodes de commercialisation et les descriptifs du produit seront toujours dans le même genre, ils seront donc reconnus par le filtrage par apprentissage.

### 5.3.4. Filtrage à l'aide de plug-ins (ou "greffons")

Accès à ces plug-ins pour les installer sur le site de Spamihilator rubrique "Plugins/Add-Ons".

Il existe d'ores et déjà plusieurs plug-ins qui peuvent être installés en complément de Spamihilator et qui rendent son fonctionnement encore plus efficace. D'autres plug-ins pourront être disponibles en supplément au fur et à mesure des développements réalisés par l'auteur du logiciel ou les personnes qui y contribuent (si vous avez des connaissances en développement et que vous souhaitez soumettre un plug-in pour filtrer les messages sur des critères autres, vous pouvez proposer votre aide au développeur. Certains de ces plug-ins (les plus populaires) sont installés par défaut avec Spamihilator.

Vous avez la possibilité d'activer ou non les plugins installés sur le poste utilisé avec Spamihilator. Vous trouverez l'option correspondante dans les "Paramètres", rubrique "Propriétés du filtre".

Vous pouvez désactiver uniquement un des plusings installés. Vous pouvez aussi, pour certains, les configurer en fonction de votre envie (vrai pour le plug-in sur les attachements par exemple où la liste des extensions à banir est modifiable par l'utilisateur).

A l'heure actuelle, les plugins les plus utiles sont :

- ◆ *"Image filter"* (filtrage des images extérieures) : lorsque, dans un mail, cela fait appel à une image référencée sur un site web (au lieu que l'image fasse partie du message lui-même), le message est placé en corbeille. Ce genre de procédé est extrêmement utilisé par les spams à caractère pornographique où des images stockées sur des serveurs web sont chargées lorsque vous relevez vos messages. En général, personne n'écrit d'email en y référant des images à charger à la réception lors d'une correspondance "classique". Ce filtrage sur les images est actuellement installé par défaut avec Spamihilator.
- ◆ *"Attachment filter"* (filtrage des fichiers attachés en fonction de leur extension) : vous savez que beaucoup de virus sont rapidement identifiables sur les extensions des fichiers attachés qu'ils utilisent pour se propager. Les fichiers .pif, .bat, .scr, ... sont à proscrire de la messagerie électronique. Ce plug-in permet de définir la liste des fichiers attachés qu'on ne veut en aucune manière voir arriver dans l'outil de messagerie. Ce plug-in est installé par défaut avec la version 0.9.7 de Spamihilator
- ◆ *"Newsletter Plugin"* (pour autoriser des messages de type "newsletter" ("bulletins" en français) ou "mailing list" (listes de diffusion) à être reconnus comme valides, et par conséquent acceptés). Beaucoup d'email d'informations qui peuvent arriver avec des fréquences assez élevées peuvent être reconnus grâce à un mot clé particulier dans le sujet du mail (entre crochet en général). Aussi, pour ce genre de message, c'est en général toujours la même adresse destination qui est utilisée. L'activation de ce plug-in (installé par défaut avec Spamihilator 0.9.7) et la définition de ces newsletters dans les propriétés de Spamihilator permettront d'éviter à de tels mails d'être filtrés sur les autres critères si le plug-in correspondant est placé en premier dans l'ordre de priorité des filtres de Spamihilator.
- ◆ *"AlphabetSoup filter"* (filtrage sur les chaînes de caractères "soupes") : certains spams, pour ne pas être filtrés par les outils anti-spam, utilisent des chaînes de caractères à rallonge pour diffuser leur message (ex : pas d'espace ni de ponctuation

dans une phrase complète). Ce plugin permet de faire le tri dans les mails qui contiendraient de telles suites de caractères sans sens réel.

- ◆ Vous pouvez tester les autres afin de constater de leur efficacité...

## 5.4. Installation

*Rappel : Spamihilator va modifier la configuration de votre outil de messagerie. Afin d'éviter tout problème, il est conseillé de sauvegarder votre configuration actuelle en cas de problème afin de pouvoir revenir en arrière. De plus, si vous avez activé la mémorisation de votre mot de passe pour la relève de vos mails, cette mémorisation pourra être perdue et le mot de passe redemandé dans la plupart des applications de messagerie. Il est donc impératif d'avoir accès à ce mot de passe (feuille de compte imprimée à la création ou lors d'une modification de mot de passe par exemple).*

Info : Lors de la rédaction de cette documentation, Spamihilator est disponible en version 0.9.7 et le fichier d'installation fait 568 kO (temps de récupération à travers une connexion par modem d'environ 2 minutes).

Après avoir récupéré le fichier exécutable d'installation (un exemplaire est disponible [sur notre serveur FTP](#) et vous le trouverez aussi sur [le site officiel de Spamihilator](#)), il faut lancer l'exécutable dont la première phase est en anglais (ou en allemand pour ceux qui préfèrent). L'espace requis est de 1.6 MO pour la version avec documentation. Il est demandé le répertoire destination, laissez celui par défaut ou précisez le répertoire de votre choix...

On entre alors dans une phase d'installation en français (si votre Windows est installé en français...) où la licence du logiciel apparaît (en anglais). Vous êtes invité à la lire et à accepter si vous êtes d'accord. Cette licence ne traite quasiment que de la distribution du logiciel. Aucune particularité n'est spécifiée au niveau de son utilisation. Vous pouvez installer et utiliser ce logiciel sans crainte (contrairement à d'autres logiciels où les conditions d'utilisation sous beaucoup moins attrayantes...).

Etant donné que c'est la première fois que Spamihilator est lancé, un assistant de (re)configuration des outils de messagerie et de Spamihilator est lancé. Il est précisé les clients de messagerie supportés (Microsoft Outlook 2000/XP/Express, Opera, Eudora, Pegasus Mail, Phoenix Mail (maintenant renommé Thunderbird), Netscape 7/Mozilla 1)). Spamihilator va être capable de modifier les paramètres de configuration de ces logiciels et de rétablir la configuration initiale si vous souhaitez un jour ou l'autre désinstaller Spamihilator (si les spams s'arrêtent un jour...). De même, il est possible de configurer plusieurs clients de messagerie sur la même machine pour utiliser Spamihilator. Il suffit de relancer autant de fois l'assistant de configuration qu'on a de comptes de messagerie à relever (cet assistant peut être relancer à travers le menu "Démarrer/Programmes/Spamihilator/Setup-Wizard").

Spamihilator a été installé sur une machine où étaient installés les clients de messagerie suivants (à chaque fois en version française) : Outlook Express 6.0, Outlook 2000, Opéra 7.11, Eudora 5.2.1, Pegasus Mail 4.02, Mozilla Thunderbird 0.2, Mozilla Courrier 1.4, The Bat 1.62

Mozilla Courrier, Outlook, Pegasus Mail, Eudora, Opera et Outlook Express sont apparus dans la liste des clients repérés ! Pour les logiciels reconnus, aucune action "manuelle" n'est nécessaire. Il suffit de sélectionner l'application utilisée, le ou les profil(s) souhaité(s) (si

plusieurs comptes de messagerie sont configurés dans le client de messagerie) et Spamihilator va modifier les paramètres en conséquence. L'opération devra être renouvelée si plusieurs outils de messagerie sont utilisés.

Spamihilator propose tout de même un choix "Autre" si votre client de messagerie n'apparaît pas dans la liste retournée. Il est alors demandé le serveur POP, le nom du compte et l'éventuel port spécifié (laisser 110 par défaut) et les paramètres à spécifier "manuellement" sont alors affichés.

Spamihilator étant un "proxy POP", il va être en écoute sur la machine (il se comporte en tant que serveur) et sera contacté directement par le logiciel de messagerie. Le nom du serveur POP devient alors "localhost" (qui correspond au nom symbolique de la machine elle-même quelle que soit sa configuration). Le nom du compte (habituellement codé sur 8 caractères dans le fonctionnement du CRI) est transformé lui aussi et reprend l'ensemble des informations utiles à Spamihilator pour contacter le serveur auprès duquel les mails vont être récupérés.

En résumé, si la configuration "initiale" du client de messagerie est :

- ◆ serveur pop : pop.domaine.tld
- ◆ port d'écoute : 110
- ◆ nom du compte : username

pour que Spamihilator soit utilisé, les paramètres seront transformés en :

- ◆ serveur pop : localhost
- ◆ port d'écoute : 110
- ◆ nom du compte : pop.domaine.tld&username&110

Si Spamihilator a reconnu votre logiciel de messagerie et l'a configuré, vous pourrez constater en allant dans les options de celui-ci que les valeurs ont été changées comme mentionné ci-dessus.

Une fois que l'assistant est terminé, Spamihilator démarre (on le voit dans la barre des tâches sous la forme d'une enveloppe "jaunâtre" qui va parfois changer d'apparence, en cas de présence de courrier dans la corbeille par exemple). C'est l'indicateur que le proxy POP est lancé et prêt à être sollicité par les clients de messagerie configurés pour.

Si on veut que Spamihilator démarre automatiquement au lancement de Windows, il faut aller dans les "Paramètres" (on retournera ici plus tard pour personnaliser sa configuration de filtrage), aller dans "Paramètres généraux" et cocher la case "Lancer Spamihilator au démarrage de Windows" si elle ne l'est pas.

## 5.5. Personnalisation de la configuration

Par défaut, Spamihilator s'installe avec une liste prédéfinie de mots clés qui indiquent une probabilité que le mail soit un spam. Cette liste peut être visionnée, modifiée, complétée. Son accès se fait par un clic droit sur l'icône dans la barre des tâches puis en sélectionnant "Paramètres/Propriétés du filtre/Mots interdits". Le pourcentage de probabilité affecté à chaque mot devra être réfléchi en fonction de la configuration choisie sur le seuil de

tolérance.

A suivre...

[Retour au [sommaire](#)]

---

Document généré avec les cri-doctools