3 General principles

A powerful anti-spam shield.
State of the art technology.
Made in Switzerland.

What you should know about spam

An astonishing 95% of all messages traveling through the Internet are unwanted by their recipients. Spam is the number one enemy of your e-mail system.

Spam doesn't just pollute your mailbox. It costs time and money. It takes an average of ten minutes a day to manually clean up a mailbox in the absence of spam filters. This adds up to more than one week of working time per year. Moreover, the thousands of unwanted mail messages that are stored by your company or your ISP also represent a wasteful burden.

MailCleaner is an efficient and indispensable tool that makes sure your e-mail system does what it is supposed to do.

Filtered messages

MailCleaner filters three types of unwanted messages:

- **Viruses.** MailCleaner simply deletes viruses without sending any alerts to the recipient.
- **Dangerous content.** Your e-mail administrator must filter dangerous content as a preventive measure. Examples of such content include attachments with executable scripts (.exe) or links to suspicious web sites. MailCleaner removes potentially harmful content and delivers the remainder of the message to your mailbox along with a note explaining how to ask your administrator to send you the complete message.
- **Spam.** Spam does not constitute any technical threat but is simply unwanted, unsolicited e-mail. It can be seen as the electronic version of printed advertisements that fill up your postal mailbox. As you will see in the following sections, MailCleaner offers you three different modes for handling incoming spam.

Principles behind filtering

MailCleaner operates in a transparent fashion, without slowing down or stopping up the stream of incoming messages. The filtering relies on over thirty quality control criteria. Some criteria concern the potentially illicit aspects of a message, while others focus on issues of trust and confidence of the sending server.

MailCleaner verifications belong to different categories: statistical (for example, repeated occurrences of specific terms or concepts), explicit (the sending server may be blacklisted or the message may have a specific format) or dynamic (the signatures and the volume of received mails are analyzed).

A relevance score is calculated mathematically at each step of the analysis. The sum of these scores determines whether the message is classified as legitimate or as spam.

Internet domains and addresses under protection

MailCleaner analyzes all incoming mail for all Internet domains that are under its protection. This basic setting is configured when MailCleaner is installed by your e-mail administrator or your ISP. You do not need to configure anything.

All of the e-mail addresses belonging to the *protected domains*, including redirections, aliases and distribution lists, are handled by MailCleaner.

For example, MailCleaner will filter *john@company.com* and *john@enterprise.com* if the two domains *company.com* and *enterprise.com* have been put under its protection.

★ ***Customization***

Configuring an address group – P. 32

Principles behind adjustments

A protection appliance such as MailCleaner is capable of filtering out nearly all spam. However, some inaccuracies may occur and specific exceptions may have to be made. Three scenarios are possible :

- A spam has managed to pass undetected through MailCleaner and has been delivered to your mailbox.
- A message that should have reached you was classified by MailCleaner as spam.
- An unsolicited message (commercial information, newsletter, etc.) has attracted your attention and you would like, as a personal exception, to receive future messages from the sender of this message.

MailCleaner offers you simple solutions to manage all of these situations. You will find all the necessary information in Appendix A of this manual.

Principles behind spam processing

As a precaution, it is not possible to modify MailCleaner features that handle viruses and dangerous content. In contrast, spam can be handled by three different modes:

- In **quarantine mode,** all spam is kept in an isolated zone outside of your mailbox.
- In **flag mode,** spam is delivered to the mailbox but is identified by adding a keyword to the message subject.
- In **delete mode,** all spam is irreversibly deleted.

Quarantine mode

By default, MailCleaner operates in *quarantine mode.*

All spam is placed in a quarantine zone located outside of your computer, thus keeping your mailbox as clean as possible.

In this mode you may consult a list of the spam that has been blocked and release the messages of your choice. MailCleaner will send you periodical reports that list all the e-mails that have been intercepted.

Flag mode

In *flag mode,* all incoming mail is delivered to your mailbox. However, MailCleaner helps you identify spam by adding a keyword of your choice in front of the subject of the message (for example, SPAM --). Flagging makes it easy to select all spam using your e-mail software: You may simply sort your messages alphabetically, run a search or even implement an automated rule based on a keyword.

The subject of a flagged message may be as follows:

SPAM -- Blue pills very low price

Delete mode

In *delete mode,* spam is immediately and irreversibly deleted.

You should choose this mode if you prefer expediency and if you accept the fact that MailCleaner may, on rare occasion, incorrectly evaluate an incoming message as spam and erase what is in fact a legitimate message.

★ ***Customization***

Configuring spam processing modes – P. 27