

Protect IT and personnel resources from productivity sapping e-mail solicitations

[Astaro Firewall](#)

E-mail has become one of the most frequent means of communicating with customers, suppliers and employees. However pervasive usage, combined with the fact that it is essentially a free form of communication for the sender, has made e-mail the favored means of soliciting customers for a wide variety of goods ranging from pornography to drugs.

Unsolicited commercial e-mail (spam) is extremely costly for businesses. Spam now makes up 46% of unfiltered e-mail, having grown at an explosive rate of 61% in the last year. It consumes a huge amount of IT resources, including disk space, computing power, bandwidth and personnel. Of greater concern are the business productivity losses stemming from spam, including the time spent by virtually every employee to read, delete or respond to it. Ferris Research estimates that last year spam cost U.S. and European businesses \$8.9 billion and \$2.5 billion, respectively.

Approaches to Spam Protection

Unfortunately spam comes in so many varieties, which are constantly altered in attempts to evade the effects of anti-spam techniques, that no single solution can protect your organization. As a result, most organizations deploy multiple electronic filtering techniques that together minimize the amount of spam that escapes. These filters are setup on a system that sits at the point where the Internet enters the organization; ensuring spam is filtered before it is dispersed to systems and employees across the organization. Techniques that have been found to be effective include:

- **Sender verification:** This approach uses the Internet DNS directory to check whether the sending mail server is legitimate. Sender verification can also be taken a step further by contacting the sending mail server to verify authenticity of the particular sending address.
- **Known spammer blocking:** There are many databases on the Internet that contain e-mail addresses of known spammers. The databases are updated continually as spammers move their addresses to evade detection. Blacklist filters eliminate any e-mail sent from spammers listed in these blacklist databases. Internally generated lists can also be used to complement third-party lists, if desired.
- **Heuristic identification:** The majority of spam messages share certain characteristics. Heuristic filtering rates messages on their similarities to these characteristics, allowing spam from new or unknown spammers to be identified. Administrators are provided controls to set the sensitivity of the filter, which then dictates whether or not a particular message is categorized as spam.

Astaro Security Linux's Spam Protection Capability

Astaro Security Linux is a complete, integrated suite of security software that is installed on standard PC hardware, and placed at the point where the Internet connects to your organization's network. Astaro Security Linux includes, at no extra cost, spam protection functionality that encompasses all of the techniques listed above. A simple point-and-click user interface allows administrators to invoke any combination of techniques desired.

The administrator is also given control over the handling of e-mail that is identified as spam. It can be:

- Automatically deleted,
- Quarantined for review by the administrator,
- Returned to the sender with an explanation of why it was returned, or
- Forwarded to the sender with a special header that can be used by the receiving mail system to deal with the offending message as desired.

Should a legitimate e-mail address accidentally be identified as a spammer, for example if it were erroneously included in a third-party blacklist database, the administrator can easily override the spam filters. This is done by creating a whitelist, which is a list of known, good addresses.

Astaro Security Linux includes powerful, easy-to-use capabilities for dealing with the rapidly growing problem of spam, while also protecting against the many other threats of connecting to the Internet.