



astaro
internet security

[Astaro Firewall](#)

Network Security Whitepaper

How to Combat Spam to Cost-effectively Minimize Productivity Losses

Version: 1.00

Release date: November 3, 2003

Author: Al Cooley, BSEE: WPI, MBA: University of Michigan,
Advanced Studies in Computer Engineering: Boston University



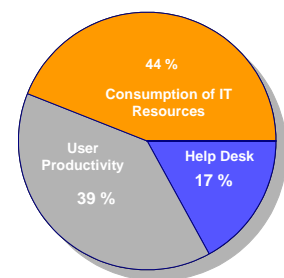
Table of Contents

The Spam Onslaught	3
Approaches to Spam Protection.....	4
Additional Evaluation Considerations	5
Astaro Security Linux	5
Astaro Security Linux's Spam Protection Capability	6
Conclusion.....	6
Appendix A: References.....	7
Further Reading	8

The Spam Onslaught

Email 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 email the favored means of soliciting customers for a wide variety of goods ranging from financial services to pornography to drugs. Unsolicited commercial email (spam) now makes up 46% of unfiltered email, having grown at an explosive rate of 56% in the last year! Forecasts indicate this rate of growth will continue next year.

For enterprises the deluge of spam is becoming increasingly costly. It consumes a huge amount of IT resources, including disk space, computing power, bandwidth and support personnel. Of equal concern are the business productivity losses stemming from spam, including the time spent by virtually every employee reading, deleting or responding to it. Ferris Research estimates that last year spam cost U.S. and European businesses \$8.9 billion and \$2.5 billion, respectively. From a financial perspective this places the spam threat in the same category as virus threats.



The Cost Elements of Spam

A growing number of states and countries are putting in place laws designed to curb spamming. However the global nature of the Internet, combined with the relatively small percentage of political entities addressing the issue make the projected timeframe for regulatory relief quite distant. Spam filtering software solutions offer the only immediate relief for enterprises.

Approaches to Spam Protection

Unfortunately spam comes in so many varieties, which are constantly altered to evade the effects of anti-spam algorithms, that no single technique can protect your organization. As a result, effective solutions employ multiple electronic filtering techniques that together minimize the amount of spam that escapes detection. These network filters are established on a system that sits at the point where the Internet enters the organization; ensuring spam is filtered before it is dispersed to computers 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 email addresses of known spammers. The databases are updated continually as spammers move their addresses to evade detection. Blacklist filters eliminate any email sent from spammers listed in these blacklist databases. Internally generated lists can also be used to complement third-party lists, if desired. The DMOZ open directory project is just one of the places you can go to find a guide to different lists (<http://dmoz.org/Computers/Internet/Abuse/Spam/Blacklists/>). Commercial blacklist database providers include the Mail Abuse Prevention System (<http://www.mailabuse.org/>).
- **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.

Incorporating all these techniques into a single spam protection solution has been proven to be very effective in minimizing the amount of spam that reaches users.

Additional Evaluation Considerations

Clearly accuracy is a major consideration in selecting a spam protection solution. However spam filtering is only one element of protecting your organization against the many threats of connecting to the Internet. In selecting a spam protection solution you should also consider:

1. **Security:** How does the spam protection solution integrate with other necessary perimeter solutions such as your firewall, web and virus filtering, as well as performance management tools for caching, load balancing and traffic shaping? Care must be taken in integrating solutions to prevent the creation of security gaps.
2. **Total Cost of Ownership:** How much will it cost over the life of the product to purchase, learn, install, configure, integrate, manage, update and reintegrate (as updates are issued) the product into your perimeter defenses? Remember the cost of the product is only a small portion of total lifecycle costs.
3. **Management burden:** How will this solution impact workforce planning? Will you require separate training, configuration, policy development and monitoring skills? Do you have the resources to provide these skills during all normal business hours? With lean staffs, many organizations find that adding a new application that needs support can be problematic.
4. **Automatic updates:** Does the product provide automatic software updates so you can maximize security and minimize labor dedicated to software updates?

Astaro Security Linux

Astaro Security Linux is a complete, integrated suite of network security software that protects against the major threats of connecting to the Internet. It is installed on standard PC hardware placed at the point where the Internet connects to an organization's network. Functions provided include:

- Spam protection
- Firewall
- Virus protection
- Content filtering
- Virtual Private Networking
- Wireless protection
- Performance management

By providing a single integrated security solution Astaro slashes the total cost of ownership, administrative labor and potential security gaps. There is no need to learn, install, integrate, manage and update multiple point solutions. A single secure Internet-based software update service keeps all elements of Astaro Security Linux up-to-date, maximizing security and minimizing costs.

Astaro Security Linux's Spam Protection Capability

Astaro Security Linux includes, at no extra cost, spam protection functionality that encompasses all of the techniques previously discussed (sender verification, known spammer blocking and heuristic identification). A simple point-and-click user interface, which is fully integrated with all the other functions of the product, allows administrators to invoke any combination of filtering techniques desired.

The administrator is given control over the handling of email 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 email 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. Similarly, local manual blacklist capability is supported to complementing external databases used. In both cases wildcards can be employed to block all users at a particular domain, or particular users sending from multiple domains.

Conclusion

Spam is one of the most visible Internet threats facing organizations today, requiring employees all the way from the CEO to interns to wade through a growing deluge of distracting email on a daily basis. Furthermore spam is expensive, with costs projected to continue to escalate at an astounding rate. To protect themselves, organizations should implement a spam protection solution that employs multiple filtering techniques and integrates seamlessly with other network security solutions.

Astaro provides an ideal spam protection solution that is highly accurate and extremely easy to manage. Being integrated into a comprehensive security solution it also provides greater security, lower total cost of ownership and simplified operation. A free 30-day evaluation version can be downloaded at www.astaro.com to verify operation in your environment. To facilitate the evaluation process, a free 90-minute web-based workshop is available which steps users through the process of configuring and using Astaro Security Linux.



Appendix A: References

1. Ferris Research, Spam Control, 2003
2. Business Week, 5/19/03, Hitting Spammers Where It Hurts



Further Reading

InfoWorld Magazine reviews Astaro Security Linux and reports "the most polished and easy to use Web-based management system we've seen to date." ([Read the whole article as PDF](#))

"A stylish-looking appliance that addresses the major internet-related security concerns of the small or medium business," says SC Magazine. ([Read the SC Magazine article as PDF](#))

Astaro named winner of the [product excellence award](#) at LinuxWorld.

A free 30-day fully-featured evaluation version of Astaro Security Linux can be downloaded at <http://astaro.com/php/download.php?lang=gb>