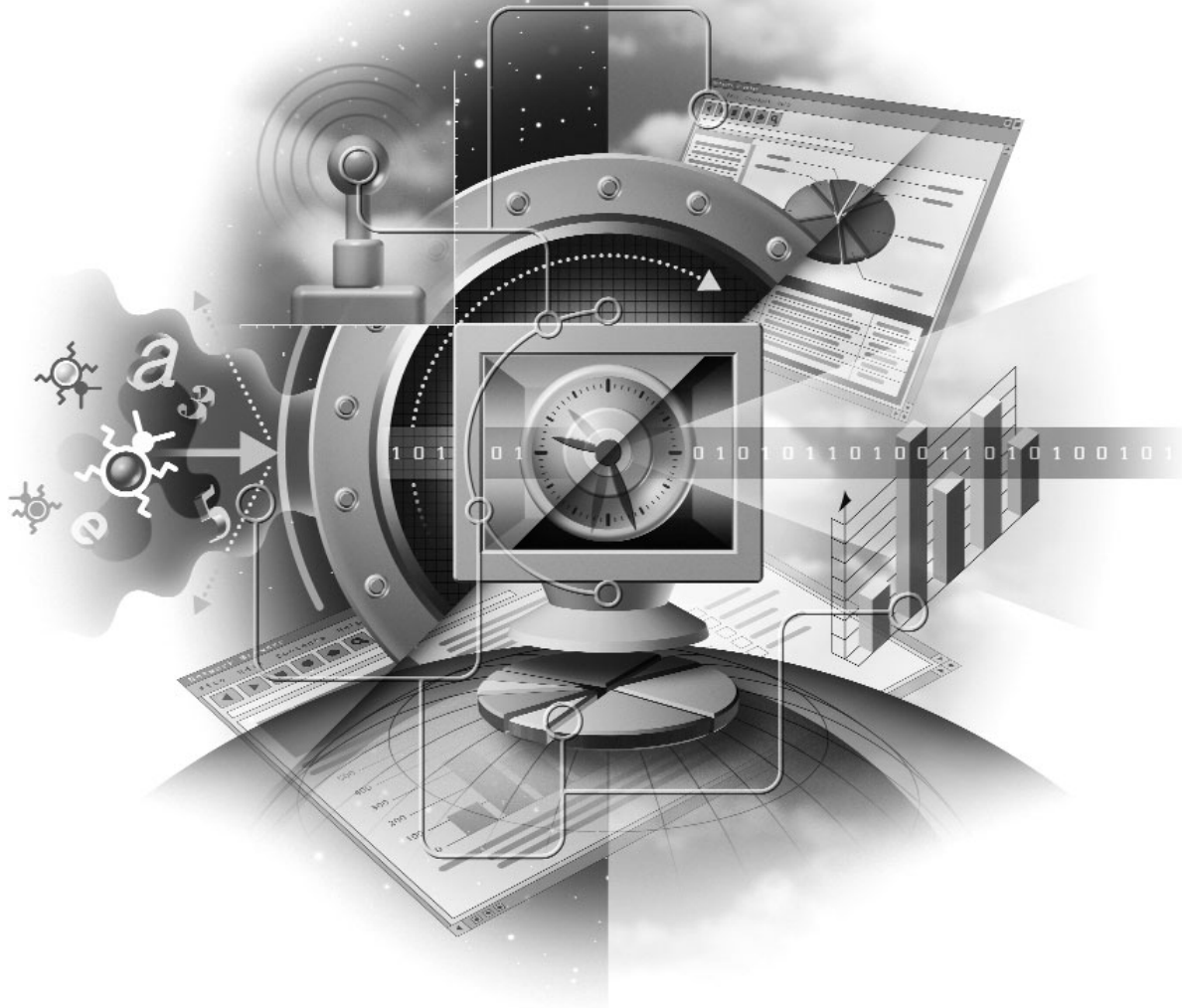


# Killing the Corporate Hydra: Spam E-Mail

McAfee Security Delivers Proactive Threat Protection with SpamKiller Technology



## Table of Contents

- I. Multiplying Faster than Heads on a Hydra: The Rise of Spam .....2**
  - Experts Agree: Spam Is a Serious and Growing Problem.....2
  - The Origin and Evolution of Spam .....2
  - McAfee SpamKiller: Proactive Threat Protection for the Enterprise .....3
  - Strong, Fast Return on Investment .....3
- II. Eradicating Spam with SpamAssassin Technology.....4**
  - Optimized for Corporate Use .....4
  - How SpamKiller Works .....4
  - Methods of Detection: The Power of Five .....5
- III. SpamKiller for Microsoft Exchange Small Business .....6**
- IV. Summary .....7**
  - About McAfee Security .....7
  - End Notes .....7

## I. Multiplying Faster than Heads on a Hydra: The Rise of Spam

In Greek mythology, the hydra was a nine-headed serpent that when one of its heads was cut off, two new heads would grow in its place. In the second of his twelve labors, Hercules handily figured out how to kill the monster, burning the neck after cutting off each of the hydra's heads.

Unfortunately, spam—loosely defined as unwanted, unsolicited e-mail—is not so easily eradicated. In December 2002, one anti-spam service measured more than five million unique spam attacks, almost three times as many as the year earlier.<sup>1</sup> The harvesting of e-mail addresses is equally relentless and swift. In a recent experiment, investigators for the US Federal Trade Commission recently posted freshly minted e-mail addresses in chat rooms and news groups to observe their fate. In one case, the first spam arrived within nine minutes of the e-mail address' inception.<sup>2</sup>

### Experts Agree: Spam Is a Serious and Growing Problem

Industry analysts and experts concur that the volume of spam is growing, although by different measures and approximations. The META Group estimates that medium-sized businesses are routinely receiving as many as 20,000 spam messages daily. The Aberdeen Group forecasts that the percentage of spam jamming corporate networks will climb from 25 percent in 2002 to 50 percent in 2003. Gartner Group similarly estimated that throughout 2002, spam accounted for as much as 25 percent of e-mail messages on the Internet, but only five percent of enterprises had successfully blocked about 90 percent of malicious spam.

Junk e-mail will cost U.S. corporations more than \$10 billion in 2003, according to a report released in January 2003 by Ferris Research, a consulting firm specializing in messaging and collaboration research. The report's authors believe the volume of spam had grown by 100 percent in the previous nine months. Other conclusions of the survey include:

- Spam cost U.S. corporations \$8.9 billion in 2002.
- Cost of spam in Europe was \$2.5 billion in 2002.
- Most spam is written in English.
- Anti-spam penetration will become similar to anti-virus penetration.

## The Origin and Evolution of Spam

Computer legend has it that spam originated in 1978, when a Digital Equipment Corporation salesperson typed several hundred e-mail addresses by hand—addresses of scientists and researchers using the Arpanet, the Internet's predecessor—and sent them an announcement of a product presentation. A recipient at Stanford University complained, "Where is the line to be drawn between this sort of thing (if it is to be allowed at all) and advertising?"<sup>3</sup>

Today, spam can be classified into three basic groups, all unwanted and unsolicited:

- **Malicious spam:** E-mail that includes adult content, violence, security threats or links to Web sites containing security threats, or scams such as the infamous "Nigerian letter" that has bilked unsuspecting recipients out of large sums of money.
- **Advertising spam:** E-mail from legitimate organizations trying to sell products (such as an online catalog) or services (such as mortgages).
- **Friendly spam:** E-mail jokes, chain letters, links to humorous Web sites sent by known friends or coworkers.

For small businesses and large organizations alike, the cost of spam is high, ultimately defying quantification. The high cost of spam can be dissected into three categories:

- **Lost productivity:** Spam costs dearly in lost productivity as users are distracted from their work to view and erase spam, or lured away to spam-linked sites—Gartner Group estimates the annual cost of lost productivity to U.S. organizations to be \$1 billion. In Ferris Research's model, loss of user productivity is the largest component, comprising 42¢ of every dollar lost as a result of spam. Finally, according to the Computer Security Institute Survey, 2002 financial losses attributed to inappropriate e-mail and Internet use soared to \$35 billion in 2002, with an average per company loss of \$536,000.
- **Inappropriate content:** E-mail deemed offensive is probably a Human Resources violation; the message could be pornographic, racist, sexist, or otherwise insulting, offending an individual or a group. Failure to shield users from inappropriate content has a huge litigious impact. A precedent was set in this area in 1996 by Chevron Corporation, where a \$2.2 million lawsuit was filed by female

employees who were offended by an e-mail joke titled "25 Reasons Why Beer is Better Than Women." As a result, at least 27 percent of Fortune 500 organizations have had to defend themselves against claims of sexual harassment stemming from inappropriate, i.e., pornographic, spam e-mail.<sup>4</sup>

Using company resources to transmit e-mail content that do not reflect company policies—such as racist or sexist views—presents an additional legal quagmire. Traditionally, employers have been responsible and liable for the actions of their employees in the workplace. However, if an organization can demonstrate a "duty of care" to reduce unacceptable employee activity, then it could minimize its potential liability.

As of June 2001, IDC research indicated that 48 percent of employers that monitor employee e-mail say their intention is to protect against viruses and the loss of information; 21 percent monitor employee e-mail as a way to limit legal liability.

- **Wasted IT resources:** Finally, the huge and growing volume of spam e-mail consumes a significant amount of network resources, wasting bandwidth as well as considerable amounts of network storage. When an e-mail contains a delivery mechanism for malicious code—such as backdoors that trigger Trojan horses and viruses—spam becomes more than a nuisance; it is a security threat that can wreak havoc on an organization's entire IT infrastructure.

### **McAfee SpamKiller: Proactive Threat Protection for the Enterprise**

The SpamKiller™ product family from McAfee® Security provides industry-leading anti-spam solutions, helping companies of all sizes effectively handle their spam challenge. The McAfee SpamKiller product family incorporates leading-edge technology called McAfee SpamAssassin,™ acquired in 2003 by McAfee Security.

McAfee's SpamKiller product vision is consistent with its overall Proactive Threat Protection strategy, which

provides integrated protection at strategic points on the network including the gateway, desktop, and servers. Since recovery is often costly and difficult, Proactive Threat Protection is critical to have in place prior to an e-mail borne security attack. When threats do strike, Proactive Threat Protection helps IT security managers quickly close the Window of Vulnerability—the period of time when threats can do damage. Proactive Threat Protection is available in a wide range of McAfee Security products that, together and separately, help secure corporate data.

McAfee's vision for multi-tiered spam defense includes SpamKiller products for the gateway, the e-mail server (including Microsoft Exchange and Lotus Domino) and the desktop. While most anti-spam products reside as a stand-alone client or reside as a gateway with no knowledge of the client, McAfee SpamKiller offers both gateway and e-mail server filtering and administration, and end-user personalization. Tuned for performance, SpamKiller provides protection for desktops, e-mail servers, and Internet gateway, offering a 95 percent spam detection rate "out of the box."

### **Strong, Fast Return on Investment**

Spam eats into productivity and profitability in myriad ways—from the time spent reading spam e-mail to the bandwidth required to carry them, from storage costs to IT management requirements. In general, the more spam that can be eradicated before entering the company, the greater the cost-savings and productivity benefits.

McAfee Security has developed a comprehensive return on investment (ROI) tool that allows companies to pinpoint exactly the sobering costs that spam incurs. Comprising a dozen variables, McAfee's SpamKiller ROI Tool vividly illustrates the debilitating effect of spam on enterprises large and small, and provides solid proof points to support the value of implementing anti-spam solutions. The SpamKiller ROI Tool can be accessed at <http://www.mcafeesecurity.com/>.

## II. Eradicating Spam with SpamAssassin Technology

McAfee SpamKiller products are powered by SpamAssassin technology, renowned public domain software that has been commercialized by Deersoft. McAfee acquired Deersoft in early 2003. *The New York Times Magazine* says enthusiastically of SpamAssassin:

“One of the best tools for network administrators is an ever-evolving program called SpamAssassin, which uses a range of tests and a point system to identify spam. This is subtler than simple yes-no filtering. Messages get points for capitalized words like AMAZING and GUARANTEE and PROFITS. They get points for mentioning Viagra—especially “natural” or “herbal.” They get points for requesting a credit-card number, for including a toll-free number and for offering a full refund. They get points for odd-looking dates: much spam appears to have been sent in 1941; much appears to have been sent from the future. They get points for lively font colors and embedded scripts or links.

In a delightful SpamAssassin irony, a message gets extra points for declaring that it is not spam. After all, such statements are invariably lies.”<sup>5</sup>

### Optimized for Corporate Use

The SpamAssassin engine, on which the SpamKiller product line is based, is indeed open-source code. As *The New York Times Magazine* alluded, the program is “ever-evolving” because it is publicly available on the Internet and can be modified by anyone who wishes to do so. The open source version of SpamAssassin is much more suitable for hobbyists; it runs only on the UNIX operating system, does not contain any code to integrate with popular e-mail servers such as Microsoft Exchange or Microsoft Outlook, nor does it offer the option of professional technical support.

When Network Associates® acquired Deersoft and the SpamAssassin trademark, Deersoft’s top spam-filtering design engineers joined Network Associates to lead McAfee’s anti-spam research and perfect the SpamAssassin engine for use in the enterprise. Deersoft and McAfee have subsequently made numerous performance enhancements to the SpamAssassin engine that are not available in the open source version,

optimizing the McAfee solution for corporate use. The SpamKiller products, which are designated as being “powered by McAfee SpamAssassin,” have the benefit of McAfee’s strict quality procedures and customer focus, as well as future technology improvements that will be available only in the McAfee SpamKiller products.

### How SpamKiller Works

As described in the excerpt above, the SpamKiller extensive rule-based scoring system determines whether a particular e-mail message is spam. Hundreds of rules are run against every e-mail; each rule is associated with a score, positive or negative. Rules with negative scores indicate attributes of legitimate e-mail, while rules with positive scores indicate attributes of unsolicited spam e-mail.

A genetic algorithm optimizes the scoring, using an archive of millions of spam and non-spam messages to determine the scores for the individual rules. When added together, these individual scores give each e-mail an “overall spam rating.” SpamKiller is extremely accurate “out of the box,” catching more than 95 percent of all spam e-mail with zero user customization, while giving a very low false positive rate of less than 0.05 percent.

In addition to its low false positive rates, the SpamAssassin technology is designed to not delete or bounce suspected spam, so if a false positive e-mail is detected, negative business impact is minimized. When a potential false-positive e-mail is detected it is either quarantined in a special folder, or tagged to visibly identify it as likely to be spam. It is not advisable to automatically delete potential spam e-mail, since legitimate communications can be erroneously discarded.

In general, as soon as the SpamAssassin engine identifies spam e-mail, it marks the message as spam by changing the message header, subject line, or both. Based on finding the necessary keyword in the subject line or message headers, Microsoft Exchange or Microsoft Outlook will then re-direct the e-mail. McAfee SpamKiller products give administrators several choices. The e-mail can be either moved to a junk mail folder in the individual’s Microsoft Outlook application on the desktop, or moved to a system-wide junk mail folder on the Exchange server. The latter is dependent on whether McAfee SpamKiller for Exchange is installed on the server, and its junk mail folder set up.

## Methods of Detection: The Power of Five

Utilizing its underlying rule-set process, McAfee SpamKiller simultaneously checks each e-mail message that is received by using five different methods of detection:

- **Integrity analysis:** SpamKiller examines the header, layout, and organization of each e-mail message to identify the common characteristics of spam. An advanced pattern-matching engine simultaneously applies thousands of algorithms during a single pass. The results determine a probability rating and the e-mail is then classified spam or not.
- **Heuristic Detection:** Within its score-based framework, the SpamKiller engine employs a number of heuristic methods of detection to identify e-mail as probable spam. Heuristic detection uses a series of internal tests to determine the likelihood that a message might be spam and each test carries a point value to reduce false positives. These methods can include: header analysis, body analysis, and the presence of structural tricks employed by spammers to disguise the content of the message. The SpamAssassin engine handles the mechanics of this, so fewer rules need to be created.
- **Content Filtering:** The content filtering functionality within SpamKiller can be used to help identify key words or phrases that appear in an e-mail to indicate the message is spam. The administrator or user (depending on whether server or client-based software is being used) can add words or phrases to a database such as "XXX," "free," "cheap mortgages," etc. This functionality complements, and is in addition to, the rule set supplied with SpamKiller products.
- **Blacklists and Whitelists:** SpamKiller supports blacklists (commercial lists of domains known to send spam) and whitelists (organization-specific lists of

domains, from which e-mail is always accepted; even if a whitelisted domain is on a blacklist). It offers the additional versatility of two layers of whitelists and blacklists. The administrator sets the standards at the server level to determine spam e-mail for everyone in the organization using the global whitelist and blacklist settings, while individuals are able to supplement the rule set at the desktop by defining their own whitelist or blacklist entries.

This functionality is especially important because what one user or company might classify as spam, another may want to receive. For example, an associate in a law firm working on a case concerning Viagra can create her own whitelist to let through e-mails from specific clients or domains.

- **Self-Tuning:** The SpamKiller engine is able to learn the characteristics of typical e-mail users receive, interpreting that information to adjust the spam score given to incoming e-mail messages—a process also known as "auto-white listing." The self-tuning functionality works out the statistical distribution of the overall spam rating for e-mail sent by each individual sender, and uses this to adjust the overall spam rating for new messages sent by a known sender.

For example, a user may have a vendor who regularly sends (non-spam) e-mail. The vendor may forward a virus alert that might ordinarily be given a high overall spam rating due to its formatting. Here, the SpamKiller product will use historic data provided by the SpamAssassin engine to lower the message's overall spam rating so it doesn't get classified as spam.

Together, these capabilities make McAfee SpamKiller a top choice for both small businesses and larger enterprises struggling to eradicate spam.

### III. SpamKiller for Microsoft Exchange Small Business

McAfee SpamKiller for Microsoft Exchange Small Business is the first of the SpamKiller family to be released. Additional products will become available, offering SpamKiller protection at the gateway, server, and desktop, in the second half of 2003.

This solution is ideal for small businesses that require enterprise-caliber spam protection. Designed for ease of deployment and low-maintenance administration, SpamKiller for Microsoft Exchange incorporates the SpamAssassin rules-based scanning and five methods of detection. In addition, its special features include:

- **The ability to auto-create an end user “Junk Mail” folder:** System administrators have the option of sending e-mail identified by SpamKiller as spam to either a junk mail folder in Microsoft Outlook, or a system junk mail folder. The first time a spam-rated e-mail is sent to an end user’s inbox, a “junk mail” folder can be automatically created. Thereafter, all e-mail rated as spam goes to the junk mail folder rather than to the inbox. This feature makes for a very streamlined installation; the Exchange Administrator is not required to write any rules. It also immediately gets spam out of the end user’s inbox, and moves the responsibility for reviewing junk mail from the system administrator to the end user.
- **Auto-sync to Outlook Contacts:** The system will automatically synchronize to an end user’s Exchange Contacts folder to create a default personal whitelist. Additions or deletions to Contacts will be synchronized to the personal whitelist, avoiding the potential for legitimate e-mails to be falsely identified as spam. The end user, if given permissions, can then use a Web interface to view and edit the whitelist and blacklist. Auto-sync with Outlook Contacts quickly and easily lowers the false positive rate without the involvement of the end-user or the system administrator having to get involved.
- **Tiered routing of spam e-mails:** The system administrator can set up tiered routing of e-mails, so e-mails scoring under a certain threshold (default is five) are sent to the system junk mail folder. For example, e-mails with scores of less than five will go to the inbox, those between five and fifteen will go to the junk mail folder in the inbox, and e-mails with scores larger than fifteen will go to a system junk mail folder. A tiered routing approach sends questionable e-mail can go to the end user for review. E-mail that is definitely spam will stay on the server to be archived and/or deleted. As a result, system administrators have more flexibility without having to write any rules.
- **Default settings:** SpamKiller for Exchange Small Business ships with best practice settings. This includes hundreds of rules and an associated scoring system, allowing for 95 percent accuracy “out of the box.” The system can be up and running in one hour; administrators needn’t write rules, create dictionaries, or define routing parameters. Some systems take several weeks just to set up the rules and the scoring parameters.
- **Modify the header:** The system administrator can modify the header for e-mail scored as spam; for example appending a prefix to the subject line with text such as “\*\*\*\*SPAM\*\*\*\*.” Alternatively the header of the e-mail message can be appended with its SpamKiller numeric score. Appending a prefix to the subject line makes it easy for end users to identify e-mail scored as spam, and for the system administrator to avoid writing custom rules.
- **Easy rules editing:** The user interface for SpamKiller for Microsoft Exchange Small Business makes it easy and convenient for the system administrator to view, edit, and create rules at the code level to fine-tune the product for specific needs.
- **Show which rules have been triggered per e-mail:** The administrator can activate an option that creates a report showing which rules that have been triggered on an e-mail as well as the overall spam score. This report is attached to the e-mail and is accessed via Microsoft Outlook. The administrator can use this report see why e-mails are being flagged as spam, or not being flagged. The administrator can then decide if individual rules need to be modified or if a new rule should to be created.
- **New rules added by open-source contributors:** SpamAssassin ships with hundreds of optimized rules and techniques contributed by members of the global open-source community. New rules are first submitted by the open-source community and are then tested and optimized by McAfee, to be brought into McAfee’s SpamKiller product family. The result is an excellent product enhanced by the constant addition of cutting-edge anti-spam techniques, creating a highly effective, low-maintenance implementation.

## IV. Summary

For enterprises looking for powerful, yet low-maintenance way to defeat the “spam hydra,” McAfee SpamKiller solutions, powered by SpamAssassin, are an ideal choice. SpamAssassin is unique in that it is the only anti-spam engine available today that provides integrated five-level protection for spam detection; most other anti-spam solutions provide only a subset of the SpamAssassin protection, which comprises:

- Integrity Analysis
- Heuristic Detection
- Content Filtering
- Blacklists and Whitelists
- Self-Tuning

As a result, while other systems have spam-catch rates of 40 to 70 percent, SpamKiller products were designed to provide excellent detection rates with very low false positive rates straight “out of the box.” These detection rates can be even further improved with rapid self-tuning. For example, the SpamAssassin detection rate starts at 95 percent “out of the box” (i.e., with zero user personalization) and then can quickly rise as the system is personalized to the company and individual users. Likewise, its low “out of the box” false positive rate is less than one in 2,000 messages (0.05 percent); SpamKiller products additionally incorporate self-tuning systems that are designed to lower this number further. After approximately one week of operation, the false positive rate is very close to zero.

The McAfee SpamKiller product family is ideal for today’s IT resource-strapped small businesses and enterprises, offering an Internet-independent solution with a tiered product architecture. SpamKiller products

also integrate into the McAfee ePolicy Orchestrator™, for easy, automatic rule updating and reporting, and play an integral role in McAfee’s Proactive Threat Protection strategy, designed to close the Window of Vulnerability.

For more information about how McAfee SpamKiller products can lower IT costs and raise productivity, please use the SpamKiller ROI Tool at <http://www.mcafeesecurity.com/>.

### About McAfee Security

McAfee Security is a product line of Network Associates, Inc. that protects businesses from security breaches, virus attacks and blended threats. McAfee

Security provides comprehensive network protection through industry leading anti-virus, encryption, desktop firewall, intrusion detection, vulnerability assessment and managed security technologies. All McAfee Security products and services are backed by the world-leading anti-virus research organization, AVERT™ (Anti-Virus Emergency Response Team), the team responsible for providing cures for major outbreaks like LoveLetter, CodeRed and Nimda. For more information, McAfee Security can be reached at 888-VIRUS-NO, and on the Internet at <http://www.mcafeesecurity.com>.

### END NOTES

- <sup>1</sup> “Tangled Up in Spam,” James Gleick, The New York Times Magazine, February 9, 2003.
- <sup>2</sup> Ibid.
- <sup>3</sup> Op. cit.
- <sup>4</sup> Source: “The e-Policy Handbook,” Nancy Flynn.
- <sup>5</sup> Tangled Up in Spam,” James Gleick, The New York Times Magazine, February 9, 2003.

All Network Associates® products are backed by our PrimeSupport® program and Network Associates Laboratories. Tailored to fit your company’s needs, PrimeSupport service offers essential product knowledge and rapid, reliable technical solutions to keep you up and running. Network Associates Laboratories, a world leader in information systems and security, is your guarantee of the ongoing development and refinement of all our technologies.

