



McAfee Anti-Spam: Protecting Your Organization from Spam, Phishing, and Other Unsolicited Messages

Table of Contents

Key Findings	3
Abstract	3
The Scourge of the Internet	3
Common Spam Techniques	3
McAfee Preemptively Blocks Spam	4
McAfee Stops Known Spam	5
Continuous Self-Tuning	6
How McAfee Verifies Detection Rates	6
McAfee Leads the Industry in Spam Protection	7
McAfee Provides Effective Spam Management	7
Choices, Choices	8
McAfee Is Your Proven Security Partner	8

McAfee Anti-Spam: Protecting Your Organization from Spam, Phishing, and Other Unsolicited Messages

Key Findings

1. Spamming is a lucrative, dynamic business. Offenders use increasingly sophisticated tactics to deliver spam and phish messages, which can result in fraud, identity theft, and the release of viruses, spyware, and adware inside your company.
2. McAfee® anti-spam products utilize a powerful combination of advanced techniques such as domain-name reputation and URI filtering, resulting in the industry's highest spam block rates.

Abstract

Stopping spam requires agility and advanced technologies. McAfee brings its proven security expertise, global visibility into spammers' tactics, and state-of-the-art techniques to keep your organization one step ahead of the deluge of unwanted email. McAfee anti-spam products use domain-name reputation, IP reputation filtering, advanced content filtering, and more to deliver the industry's highest effectiveness, able to stop a new spam campaign in less than three minutes. Read this white paper to discover the behind-the-scenes capabilities that McAfee uses to automatically protect your organization from spam, phish, and other unsolicited messages.

The Scourge of the Internet

Some 80 to 90 percent of all email is spam, according to McAfee Avert® Labs researchers. While most people wouldn't click on an email advertisement for pills, luxury watches, or online college degrees, only a tiny fraction of people need to respond to such messages to make spamming a highly profitable business. But it isn't only the transaction that makes money for the sender, for spam is often a conduit for fraud and identity theft. Some of these businesses take your money but never ship the promised goods. Other spam messages are loaded with viruses, spyware, adware, or bots, which can be used to steal or destroy your private information.

Shady businesses aren't the only ones unleashing torrents of spam. Legitimate businesses also use questionable bulk emailers for marketing, sometimes unwittingly through agencies. But whatever the intent, the end result is the same: a huge load bogging down your email infrastructure.

Employees waste time dealing with spam, whether they delete it, fine-tune their spam filters, or check their quarantine folders. The occasional important email that gets erroneously quarantined or deleted frustrates users and slows down business. Many spam messages are obscene or inappropriate in the workplace, which can offend employees and run your organization afoul of hostile workplace laws.

Spam consumes IT resources and costs you money. Spam overloads your email servers, consumes precious disk storage, and wastes network bandwidth. With an increasing number of industry and governmental regulations that govern the retention of electronic communications, your organization's policies may dictate that spam messages that reach your email servers have to be archived for years.

Common Spam Techniques

Spam attacks are more intense and agile than ever before, as spammers seek to evade detection by anti-spam defenses. A spam campaign may last only 30 minutes, whereas two years ago, spam attacks would last several days.

Botnets have become the preferred way to send spam, because spammers can easily send massive amounts of spam with a minimal investment. Criminals also use botnets to launch Denial of Service (DoS) attacks for extortion and run pay-for-click scams. A single botnet may control thousands or tens of thousands of PCs across the Internet, making it difficult to shut down these vast networks of compromised PCs.

Since spammers are in business to make money, they must provide contact information to make the sale. The spam message usually includes a telephone number, a link to a web site, or a postal address. Anti-spam products can use this contact information as a way to identify and block these messages.

However, spammers have plenty of tactics to get their messages past anti-spam products.

- **Obfuscate the URI**—One way to avoid detection is to obfuscate the Uniform Resource Identifier (URI) within the spam message

A spammer may make the URI look less like a URI, as in “www(dot)gotothissite(dot)com—please replace the (dot) with a dot.”

Simple URI obfuscation reduces the profitability of the spam campaign because a person can’t directly click on the link, so the spam is less effective at generating a sale.

Another approach to URI obfuscation is to use HTML to camouflage links and keywords. Phish messages commonly contain obfuscated links, as the attacker tries to trick you into clicking on a fraudulent web page. For example, a link that appears to go to *www.mybank.com* may contain HTML code that actually takes your browser to *www.phishsite.com*.

- **Change the URI**—One of the most prevalent methods spammers use is to constantly change the URI within the spam message itself. It’s easier to change a URI in an email than to change a phone number or physical mailing address

To change the URI in a spam message, the spammer may buy hundreds of domain names. A single new domain name may cost up to \$15, so this technique can be quite costly. The useful life of a new spam domain may be a few minutes or a few days, depending on how quickly the security companies can identify and react to it. This puts spammers under pressure to send out huge volumes of spam very quickly when using this technique.

- **Image-based spam**—Spammers also use images to hide the URIs. Spammers, particularly for stock pumping and luxury watches, increasingly try to sneak past anti-spam filters by sending their come-ons as GIF or JPEG images instead of text

With image spam, each email is slightly different. For instance, the image may be slightly blurred or sharpened or the colors slightly altered. These subtle modifications, which are hardly perceptible to the human eye, can evade detection by less-advanced content filters.

- **Obfuscate the content**—Spammers misspell words and use numbers instead of letters to try to evade content filters

The idea is to obfuscate enough content to evade a content filter that looks for specific “spammy” or offensive words, but still have you understand the message. This technique has limited effectiveness. If the spam message spells too many words wrong, you simply can’t understand it. Plus, advanced content filters can recognize the obfuscated text, and block these spam messages.

These email subjects contain simple obfuscation:

“Better refyinanclng available”

This subject line contains a misspelling of the word “refinancing” to attempt to avoid keyword filters.

“St0kkMarrkett Picks Watch watch”

This example replaces letters with numbers and contains repeat characters again to attempt to avoid keyword matching.

“Do away with all you are indebted for with out mailing another cent”

This example attempts to use “non-spammy” words while still indicating what the spammer is selling.

- **Add ordinary text to the message**—Spammers add long passages of unrelated information to lessen the overall probability that the content filter will identify the email as spam or offensive. Or they may insert words randomly selected from the dictionary to skew the content filter’s statistical measures for spam
- **Use floating text**—Another technique is to use floating text in the HTML code to obfuscate spam words

McAfee Preemptively Blocks Spam

McAfee anti-spam products provide strong protection against spam and phish messages. McAfee’s research and development team uses industry leading techniques to stay one step ahead of the spammers. McAfee uses multiple proactive and reactive detection methods simultaneously, which makes it difficult for spammers to evade detection and results in the industry’s highest detection rates. Proactive methods, such as domain-name reputation technology, heuristics, and integrity analysis, detect and block spam, phish, and other malicious messages to provide zero-day detection of new spam.

- **Domain-name reputation**—Spammers attempt to slip past anti-spam filters by frequently changing URIs, but it’s much more difficult for spammers to change the underlying servers that host the domains themselves. McAfee’s advanced domain-name reputation technology identifies when spammers change their domain names or domain servers

With domain-name reputation, McAfee does not need to receive a sample of the spam to block the messages. McAfee can block the URI before spammers use it, providing zero-day detection of new spam.

McAfee’s advanced domain-name reputation technology locates spam sites based on Internet registration information and multiple types of IP and domain reputation systems. McAfee proactively identifies potentially bad URIs and places them on a watch list. Once a spammer uses the domain, McAfee immediately identifies it as a bad URI and discards the email coming from that domain.

McAfee uses domain-name reputation technology to preemptively stop spam as follows:

1. A spammer registers a new domain.
2. McAfee confirms the domain as a spam site within minutes of registration.
3. McAfee sends an update to its anti-spam products deployed at customers' sites, telling the anti-spam products to block spam containing a URI pointing to this new domain.
4. The spammer starts using the URI in spam and McAfee anti-spam products automatically block the spam.

McAfee's domain-name reputation technology is highly effective against all types of spam campaigns, even very short campaigns with frequently changing URIs or obfuscated content. This technique also works to block phishing and messages containing links to malicious payloads like spyware. McAfee's domain-name reputation technology is so effective that this technique alone can block up to 40 percent of all spam before it is sent.

- **Heuristics**—A second proactive technique is the use of heuristics. Heuristics are rules of thumb that rate a message's likelihood to contain spam. These rules measure particular conditions that indicate that an email is spam. The heuristics assign a spam score to each email. For example, the presence of a spam-tool name in the email header or the use of uppercase letters in the subject line or body of the message may be indicators that the email is spam

For high accuracy, McAfee applies a confidence factor that measures how much the pattern in the condition indicates spam. Some patterns are highly associated with spam, such as a URI with the word "remove" and a subject line that contains a unique identifier. Both legitimate email and spam contain certain patterns, such as color-coded HTML, so the confidence factor would be lower for this condition. When a message's spam score exceeds a threshold, McAfee automatically categorizes the email as spam.

McAfee's heuristics techniques can make fine distinctions. For example, heuristics can take into account the location of a pattern, such as in the email header versus the body, rather than just looking for a particular pattern of characters anywhere in the message.

Different combinations of rules can detect a wide variety of spam. For instance, McAfee products can detect one spam message because it uses colored text while it detects another message because it has an invalid date header and a suspicious phrase like, "As seen on national TV!" At the same time, IT administrators can adjust the sensitivity of spam detection, if required, to ensure that the anti-spam product doesn't quarantine or block legitimate email as spam.

McAfee works quickly to develop new heuristic rules whenever McAfee identifies a new type of spam. McAfee updates its rule sets and streams them out to customers frequently—up to multiple times a minute—to ensure customers have up-to-date protection.

- **Integrity analysis**—A third proactive technique is the use of integrity analysis. Integrity analysis is a type of heuristics that examines an email's structural characteristics to determine if it is spam

An email's header, layout, and overall organization provide clues as to whether it is spam or a phishing attempt. For example, a header may have an invalid time zone, a date far earlier than the time the message was sent, or the structure of the header information may be in the wrong order. The message body may contain a single line of text in upper case with many whitespace characters, a short paragraph of text, and the words "click here" followed by a web link. Or the email may have a series of image files formatted in a particular way. An email that claims to come from a bank but has a header that shows it was sent from a botnet indicates that it is a phishing attempt.

McAfee Stops Known Spam

McAfee's proactive technologies effectively identify and block a large percentage of zero-day spam, but some spam can evade proactive techniques. For this reason, McAfee also uses reactive technologies to identify spam shortly after a campaign has begun. McAfee's reactive techniques include IP reputation filtering, URI monitoring, and DNS block lists to stop spam.

- **IP reputation filtering**—IP reputation filtering is a highly dynamic method to eliminate spam quickly and efficiently. McAfee IP reputation filtering is based on the Postini Threat Identification Network (PTIN), a real-time information service that identifies malicious computers that recently launched email attacks, such as viruses, phishing, spam, and directory harvests. The PTIN monitors 500 million IP connections per day, which allows McAfee anti-spam products to react very quickly and very accurately to new spam campaigns

The PTIN identifies computers that have sent unwanted email in the past few hours. When McAfee's IP reputation filter sees a message from a computer that has an IP address with a bad reputation, it immediately rejects the message. The list of IP addresses sending unwanted email is updated constantly, so it's always current. Unlike sender reputation systems, senders cannot self-certify their "good" reputation with an IP reputation filter, so they can't bypass McAfee's defenses.

- **Harvest URIs**—McAfee actively harvests spam, phishing, and messages containing inappropriate content from around the world, then passes those messages through a sophisticated artificial intelligence process that gleans URIs, URLs, and other characteristics of the message that “fingerprint” the message as spam. McAfee then quickly writes rules that are automatically distributed to customers’ anti-spam products to automatically block those spam messages

McAfee works closely with customers and the SpamAssassin user community to monitor and immediately blacklist spam URIs contained in the emails anywhere in the world. McAfee processes millions of these transactions a day and so has broad visibility into the changing dynamics of spam campaigns. A significant portion of these transactions are spammers who send their spam victims new URIs to click on. Using advanced URI filtering techniques, McAfee can detect and stop spam and phishing attacks as soon as they start.

McAfee uses multiple methods to determine whether a URI is legitimate or not, including heuristics to look for spikes in requests for a domain, examining the domain registration information, scanning the content of the web site and matching it with content from known spammer web sites, and cross-referencing hosting DNS servers and DNS block lists. These techniques make new spam or phishing attacks look obvious and different from legitimate email.

- **DNS block lists**—McAfee anti-spam products also use DNS block lists to identify known spammers. McAfee additionally uses its own internally maintained DNS block lists of spammer IP addresses, as well as DNS block lists that are publicly available on the Internet

McAfee has global visibility into spammers’ tactics because we work closely with Internet service providers, businesses, and consumers around the world to identify new forms of spam. McAfee uses both proactive and reactive techniques, coupled with whitelisting of senders and human content review when required, to create a system that can stop most spam. McAfee’s advanced techniques eliminate reliance on having to receive the spam to detect it, and can stop new spam campaigns in less than three minutes.

Continuous Self-Tuning

McAfee anti-spam products also perform continuous self-tuning using Bayesian filtering, whitelists, and blacklists to stop more spam.

McAfee uses Bayesian filtering to tune the spam score of messages. Bayesian filtering is more precise than content filtering. Content filtering relies on a person to compile a list of commonly used words or phrases in spam or inappropriate messages. Bayesian filtering is a mathematical method for assessing the probability that a certain word, phrase, or symbol would occur in a spam message. Bayesian filtering can produce more accurate results as the number of examples of spam and legitimate email grows.

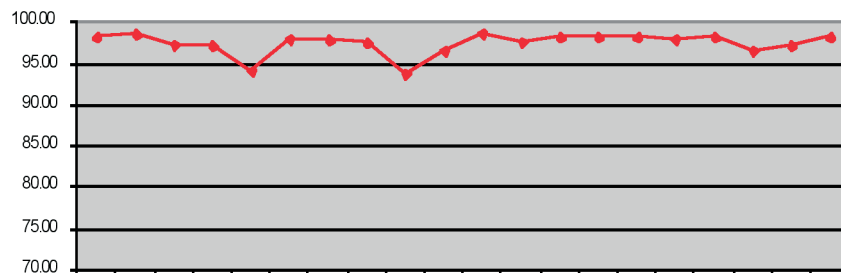
Consider the word “free.” The word “free” may appear 200 times in a sample of 10,000 legitimate emails, but the same word might appear 1,000 times in a sample of 10,000 spam messages. Thus, Bayesian filtering techniques will assign a higher spam score to a message containing the word “free.” By continually fine-tuning the spam probabilities of words occurring in messages, McAfee can stay a step ahead of spammers’ changing tactics.

McAfee also makes use of whitelists and blacklists to continuously hone its spam detection. McAfee considers email as legitimate if a user sends the email or if the recipient is on the user’s whitelist. McAfee may identify messages as spam because a user has blacklisted the sender or if users delete certain messages without opening them.

How McAfee Verifies Detection Rates

McAfee conducts extensive internal monitoring to verify that its detection rates are consistently high. McAfee maintains feeds of “control” spam separately from spam feeds used by McAfee’s anti-spam engineering team. McAfee uses this control spam, other independent spam feeds and customer-reported detection rates to verify that McAfee anti-spam products are always performing at a high level of effectiveness.

Control Feed Detection Rates



McAfee streaming updates provide continuous filtering updates every day of the year, which improves the detection rate even higher. McAfee anti-spam products have a highly agile engine that engineers tune daily to detect and block the newest spam techniques. McAfee updates its anti-spam rules around the clock. McAfee can stream very small rule updates to customers as frequently as multiple times a minute, so their protection is always current.

McAfee Leads the Industry in Spam Protection

McAfee participates in a broad range of independent industry tests and certifications for anti-spam products. McAfee earned the Checkmark PREMIUM Anti-Spam Certification for accurately detecting more than 97 percent of spam in independent testing performed by West Coast Labs. The research firm Gartner places the average effectiveness of a best-of-breed anti-spam system at 95 percent, which McAfee products exceed.



The Checkmark PREMIUM certification is just the latest in a series of awards won by McAfee.

- McAfee Secure Messaging Gateway appliance was rated number one by West Coast Labs in anti-spam testing against CipherTrust's IronMail appliance
- McAfee Secure Internet Gateway was awarded Network Testing Lab's top rating for overall gateway protection. It stopped 90 percent of spyware, 95 percent of spam, and 100 percent of viruses attempting to penetrate the network through web and email
- McAfee Secure Web Gateway was awarded Network World's Clear Choice Award for the best enterprise anti-spyware product out of sixteen tested

"The Secure Messaging Gateway box performed well, delivering 100 percent of the genuine mail correctly and correctly classifying 97 percent of the spam mail in a straight out-of-the-box configuration... West Coast Labs is pleased to award the McAfee Secure Messaging Gateway the PREMIUM-level Anti-Spam Checkmark."

—West Coast Labs, February 2006

McAfee Provides Effective Spam Management

McAfee's anti-spam products are easy to install, update, and maintain, which ensures efficient operations. Administrators can configure security policies to meet the needs of different groups within an organization. Administrators and users can control their whitelists and blacklists to adjust the sensitivity of their anti-spam product to the type of email the company receives. For some organizations, any email incorrectly classified as spam is unacceptable, while others are more accepting if their anti-spam product quarantines a few legitimate messages.

A good anti-spam solution should do more than just block spam. It should provide users and administrators with a rich set of spam management tools. McAfee anti-spam appliances provide two options for storage of spam. First, the spam can be stored on the appliance itself, using the appliance's built-in hard disks. Second, the spam can be stored on a Windows® server somewhere on the network that is running McAfee's free McAfee Quarantine Manager software.

McAfee Quarantine Manager is especially advantageous for large organizations that utilize multiple McAfee anti-spam appliances, since it's easier to manage a single spam quarantine than to manage multiple quarantines. Also, the McAfee Quarantine Manager represents just one place that users or administrators need to go to search for inappropriately blocked messages, release those messages, and configure blacklists and whitelists. Users can access McAfee Quarantine Manager from a web browser.

Regardless of where spam is stored, McAfee anti-spam appliances can be configured to send users a daily digest of the messages that have been blocked during the previous 24 hours. The digest lists the header of each message and states whether it was blocked because it was spam, phishing, or for some other reason such as inappropriate content or forbidden file attachments. Users can click a drop-down box next to each message to release it from the quarantine and/or to add the sender of the message to the user's personal whitelist.

McAfee also provides a Microsoft Outlook plug-in that can be used to send samples of missed spam back to the appliance or to McAfee's labs for purposes of learning and fine-tuning. The McAfee appliance has the ability to learn the peculiar characteristics of your organization's messages. Once the appliance has been provided with samples of mail, it uses Bayesian technologies to better judge future messages.

Choices, Choices

McAfee's anti-spam technologies are available in multiple forms, including a fully managed service, a range of appliances, and several different software solutions.

McAfee Secure Messaging Service™ is a hosted email security solution. Businesses that place a high value on ease of implementation should consider McAfee Secure Messaging Service. It requires no additional hardware, software, or IT staff. Your emails are redirected through McAfee's servers where they are quickly scanned before entering or leaving your network, with less than a one-second delay in transit. Messages containing viruses or spam are quarantined on McAfee's servers and never enter your network. The service also provides excellent protection against directory harvest attacks and DoS attacks.

McAfee appliances can be installed at the edge of your network to block spam before it can load down your email servers. McAfee appliances come pre-loaded with a hardened operating system and McAfee anti-spam and

anti-virus capabilities. McAfee appliances have the added capability of being able to protect your organization from breaches of government privacy regulations and from unauthorized transmission of confidential information. Automatic filters can detect whether email messages contain private or confidential information and can block or encrypt these messages prior to transmission.

Some organizations prefer to focus their anti-spam defenses at their mail server. These organizations should consider the software-based McAfee SpamKiller® products.

McAfee Is Your Proven Security Partner

McAfee helps you meet the challenge of spam, phish, and other unwanted content. By choosing McAfee's comprehensive email and web security solutions to protect your network and workforce from spam, phishing, and other threats, you will ensure the productivity of your employees, preserve your precious IT resources, and save your organization money.