

Postini™ White Paper

Three New Ways to Stop Spam—Preemptively

Executive Summary

Spammers are constantly inventing dangerous new ways to circumvent your email security system and invade your network. First-generation spam protection can't keep pace, forcing your inhouse IT staff to scramble to react to the latest clever trick. Welcome to Postini. We have pioneered three new ways to successfully stop your spam problem, today and in the future. In fact, Postini's Preemptive Email Technology (preEMPT™) will be the *only* email security solution you will ever need. Sound too good to be true? It's time to learn why the current email security methods employed by desktop software and gateway applications and appliances can't effectively stop spam and why Postini can.

First-Generation Spam Methods Stop Short

Traditional anti-spam products employ one of two filtering methods to block spam. Content-based filtering considers the question "*What does it say?*". These filters compare incoming messages against a list of words or set of rules to determine whether email is spam or legitimate mail. Identity-based filtering considers the question "*Who is it from?*" They examine the domain, IP or sender address of incoming messages. The most common anti-spam solutions on the market today use one or both of these filtering techniques.

Key word lists are content-based filters. Key word lists were the earliest anti-spam methods developed. However they soon turned out to be too simplistic and vague to be effective. For example, the word "breast" could relate to an X-rated mail or to cancer research. As a result, key word lists tend to have very high rates of false positives—blocking legitimate mail as well as spam. This leads

to constant fine-tuning of the lists by the administrator. Another serious drawback is that spammers can easily develop ways around the lists, creating spam that appears to look legitimate by avoiding commonly used "trigger" words, including inserting spaces between the letters of a word.

Rule-based systems were the next step in anti-spam technology. These content-based filters use a set of programming rules to evaluate incoming messages. The program accords points to various results and adds up the score. If the messages clear a threshold they are considered spam. While rule-based systems are flexible, they can be complex and time-consuming to manage. Spammers can also outwit this method with techniques that make their messages look like legitimate communications, including obfuscating trigger words, just as with key word lists above.

White lists use identity-based filters. They essentially consist of a list of approved email addresses; incoming email is compared against the list of legitimate sender names before it is allowed to pass through to the network mail servers. White lists require a lot of ongoing management; they constantly need updating as new sender addresses are added or existing ones change.

White lists also preclude the ability to receive legitimate email from unknown contacts, a common event for companies in the course of their business. A more serious flaw is that every domain entry creates a small opening for spammers to sneak through. Spammers routinely spoof the "From" address in their messages. Because email that appears to come from a white list gets a "free pass", if a spammer happens to use an approved address, the filters will allow it through.

Black lists, or real-time black hole lists (RBLs) are another type of identity filtering method. These lists consist of domains or email addresses, or range of IP addresses that have been identified as sources of spam. Most businesses subscribe to multiple blacklists, maintained by different communities of Internet service providers (ISPs) and backbone providers, to increase effectiveness. Unfortunately, domain and email addresses are easily forged or spoofed by spammers, leading to high rates of false positives.

Blocking by IP address doesn't work effectively either because spammers move around: they find an open relay on the Internet and use it until the computer gets blacklisted, then move on to another location. The spammer gets what they need, and the owner of the open relay gets stuck with a system that can't send legitimate email anywhere.

To add to the misery, a new type of virus such as *Mydoom* and *SoBig* infects legitimate computers on unprotected, continuous (always on) cable or DSL connections and turns them into spam-sending "zombies." The owners are unaware their computers are wreaking havoc until they find their IP addresses on a blacklist. Like an identity theft victim struggling with the aftermath of a damaged credit rating, a virus victim, once on a blacklist, finds it very hard to get off the blacklist.

Bayesian filters are a type of content-based filter that uses statistical probability analysis to adapt and learn from user responses. This technique works well for single users who will take the time to train the filtering program to identify what is spam and what is not spam. It does not work as effectively for groups, however, because of the wide disparity of what is considered "not spam"

between individuals. What is spam is fairly universal, but what is considered non-spam is very individualistic.

Unfortunately, spammers have also figured out how to "poison" these filters by loading email messages with completely innocuous words. The subject line on the spam message may contain random unobjectionable words, so the filters let the message through. When the user opens up the message and realizes it's really spam, he or she will unthinkingly label the offending message as spam, confusing the filters by adding otherwise legitimate words to its rule list.

Shortcomings of First-Generation Spam Filters

There are two major flaws with all the methods used by first-generation anti-spam solutions:

1. They are too static.
2. They operate behind the company firewall.

These older filtering systems operate reactively so they cannot successfully stay ahead of spammers' diabolical creativity. They also allow spam traffic onto the network to swamp your LAN and WAN bandwidth, server transaction capacity and message storage. As a consequence, your IT staff spends a great deal of time upgrading software, installing patches and new filters, and tracking and increasing server capacity. What you need is a proactive defense that will always keep you ahead of the game.

Three New Ways to Preemptively Stop Spam

In the war on spam, experience counts, and Postini is the world's largest managed email security service provider and the fourth largest email processor in the

U.S., following AOL, MSN/Hotmail and Yahoo. Postini invented the managed service email security delivery model five years ago and holds the patent on associated technologies.

From the knowledge and expertise gained from processing over 175 million messages a day, Postini has developed a unique, dynamic, preemptive email security defense designed to accurately determine the difference between spam and legitimate mail. The preemptive solution employs three new, tightly integrated and centrally managed technologies:

1. Connection Management
2. Content Security
3. Industry Heuristics

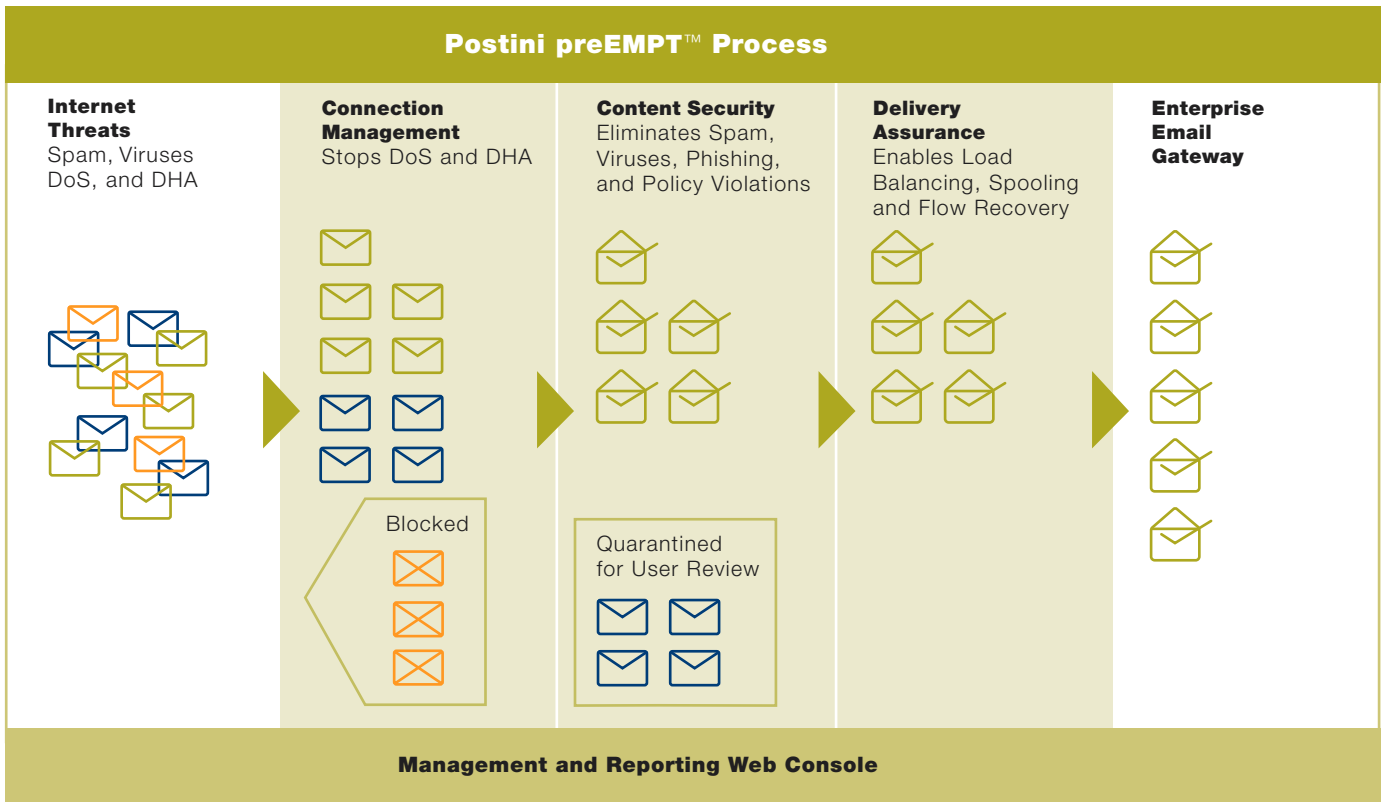
All three defenses employ thousands of sophisticated heuristics, which are complex and programmatic rule sets. Some of these rules look for spam characteristics while others look at non-spam characteristic to render a complete profile of the mail messages. Certain combinations of rules cancel each other out, while others reinforce each other. Built-in intelligence in the filters sifts through the variations and evaluates the relationships between rule results.

With this powerful trio, illustrated in Figure 1, Postini consistently takes top honors in independent industry spam evaluations, scoring both the highest accuracy rates and the lowest false-positive rates.¹

Technology #1: Connection Management

The Connection Management layer uses transport-layer heuristic filters to monitor SMTP connections and identify patterns of behavior associated with SMTP attacks and unwanted email traffic. The dynamic data monitoring and collection

Figure 1 Postini's preEMPT Security Defense



system examines dozens of aspects of SMTP traffic in real time. The Connection Management layer engine analyzes information for trends and suspicious source IP addresses, creating a continually updated snapshot of the last hour of worldwide SMTP activity.

Just based on transport behavior alone, the Connection Management layer can decide to throttle or reject SMTP connections if it detects directory harvest attacks (DHAs), denial-of-service (DoS) attacks, or statistically significant spikes in spam or virus activity. These email threats are stopped cold, before they can enter your network and cause any damage. Postini is the only anti-spam vendor on the market today that can identify and stop SMTP-based DoS and DHA attacks. That advantage comes

into significant play when you consider that 30 to 40 percent of all inbound SMTP traffic can be attributed to these transport-level attacks.²

Technology #2: Content Security

Once the SMTP connections are deemed valid by the Connection Management layer, email messages pass through the Content Security layer. Here, thousands of heuristic expressions examine email message and attachment content. As each heuristic expression assigns a spam or non-spam probability value, the software determines a composite value and the messages are either blocked or passed to the third layer for additional processing. Newer, more advanced content security solutions include many first-generation filtering capabilities,

such as white lists, black lists and key word lists. However, with Postini, these capabilities are augmented in two ways.

First, the Content Security layer includes a configuration engine that allows corporate IT administrators or end-users to configure spam blocking based on their specific email characteristics. The customizable filters can be configured to monitor the size and type of attachment files, key words, individual email activity, and sender and recipient names. Second, the spam detection technology is combined with traditional content policy management tools that allow your IT staff to easily implement consistent, company-wide rules and policies across the extended enterprise, and modify them to fit the demands of different users, groups or countries.

Technology #3: Industry Heuristics

From experience with its customer base of 2,700 customers, Postini has developed industry-specific heuristics that operate on both the transport and content layer, combining statistically significant patterns and characteristics unique to the legal and financial services industries.

The connection-level and content-level heuristics are optimized to recognize the subtle but specific characteristics of email within industry segments, lines of business or job functions. This higher level of filtering further refines the discrimination process to effectively recognize legitimate business traffic without increasing false positive rates.

For example, consider that more than half of all email traffic in the legal profession is exchanged among legal firms. Another large percentage of email is sent to or from associated organizations, such as courts, bar associations and information sources. Postini's Industry Heuristics dynamically recognize these ad hoc networks within industry segments and

are able to create validated communications channels between principles in the segment, allowing messages to be filtered less rigorously, or to even bypass spam filters. The filtering engines recognize traffic that has a high probability of being legitimate within the segment, even if it has properties that in another context would be considered spam-like—containing the word “mortgage” in the subject line, for example. The filters are also able to recognize specific content trends within messages.

But Industry Heuristics are not only useful for firms within the legal and financial industries. All Postini customers can benefit from this special feature, even if they belong to another industry. For instance, the in-house legal counsel at a manufacturing firm will benefit from the legal heuristics.

Conclusion

Unlike current email security methods employed by desktop software and gateway applications and appliances, Postini dynamically identifies spam in real time and prevents it from flooding your enterprise network. According to *Network World*,³ Postini's managed service solution blocked the highest

percentage of spam with the fewest false positives, while also screening out 100 percent of the virus traffic. Postini also helps block DoS and DHA attacks. Furthermore, intelligence built into the innovative technology recognizes legitimate traffic without requiring your IT staff to continually update or manage key word lists, rules, blacklists, white lists or Bayesian filters.

Postini's three new spam fighting technologies—Connection Management, Content Security, and Industry Heuristics—effectively and efficiently identify legitimate business communications in a sea of junk email. Most importantly, Postini works behind the scenes 24 hours a day, 365 days a year, continually analyzing billions of messages and implementing new techniques to outwit spammers so you will never have to.

Notes

1. <http://www.postini.com/press/awards.html>
2. How to Preemptively Eliminate the Top 5 Email Security Threats, <http://www.postini.com>
3. *Network World*, “Test: Spam in the Wild,” September 15, 2003, <http://www.nwfusion.com/reviews/2003/0915spam.html>



Preemptive email protection

Headquarters

Postini, Inc., 1600 Seaport Boulevard, Redwood City, California 94063

Toll-free 1-866-767-8461

Email info@postini.com

Web Site www.postini.com

For more information or to see if your organization qualifies for our free 30-day, no risk-trial of Postini Perimeter Manager, call toll-free 1-888-584-3150, email us at sales@postini.com, or visit us online at www.postini.com.

© Copyright 2004 Postini, Inc. All rights reserved. WP03-01-0403

Postini, the Postini logo and Postini Perimeter Manager are registered trademarks or service marks of Postini, Inc. preEMPT is a trademark of Postini, Inc. All other trademarks listed in this document are the property of their respective owners.