

Postini™ White Paper

How to Preemptively Eliminate the Top 5 Email Security Threats

Executive Summary

Are worries about spam and virus attacks to your enterprise email system keeping you up at night? The bad news is that they're not the only email security threats you should be worried about. The good news is there's an easy and effective way to arm yourself against all threats, even the ones you may not be aware of. Postini's Preemptive Email Technology (preEMPT™) provides an integrated solution to completely and preemptively protect against all of these threats.

First, let's take a closer look at the top five email-borne security threats, including ones originating from inside your network that you may not have considered before.

1. Viruses
2. Spam
3. Directory harvest attacks (DHAs)
4. Denial-of-service (DoS) attacks
5. Internal policy violations

Threat #1: Viruses

Viruses have been around for years, but that doesn't make them any less dangerous or easy to eradicate. New, more destructive viruses and worms are being unleashed at an alarming rate. As the world's largest managed email security service provider, handling over 170 million messages per day, Postini is in an excellent position to track and evaluate email security threat trends. The company reports that 50 percent more virus attacks were launched in 2003 than the prior year. The January–March 2004 *Mydoom* virus outbreaks were the biggest the Internet has encountered to date; Postini quarantined over 12 million copies of the virus in just the first five days of its release.

Threat #2: Spam

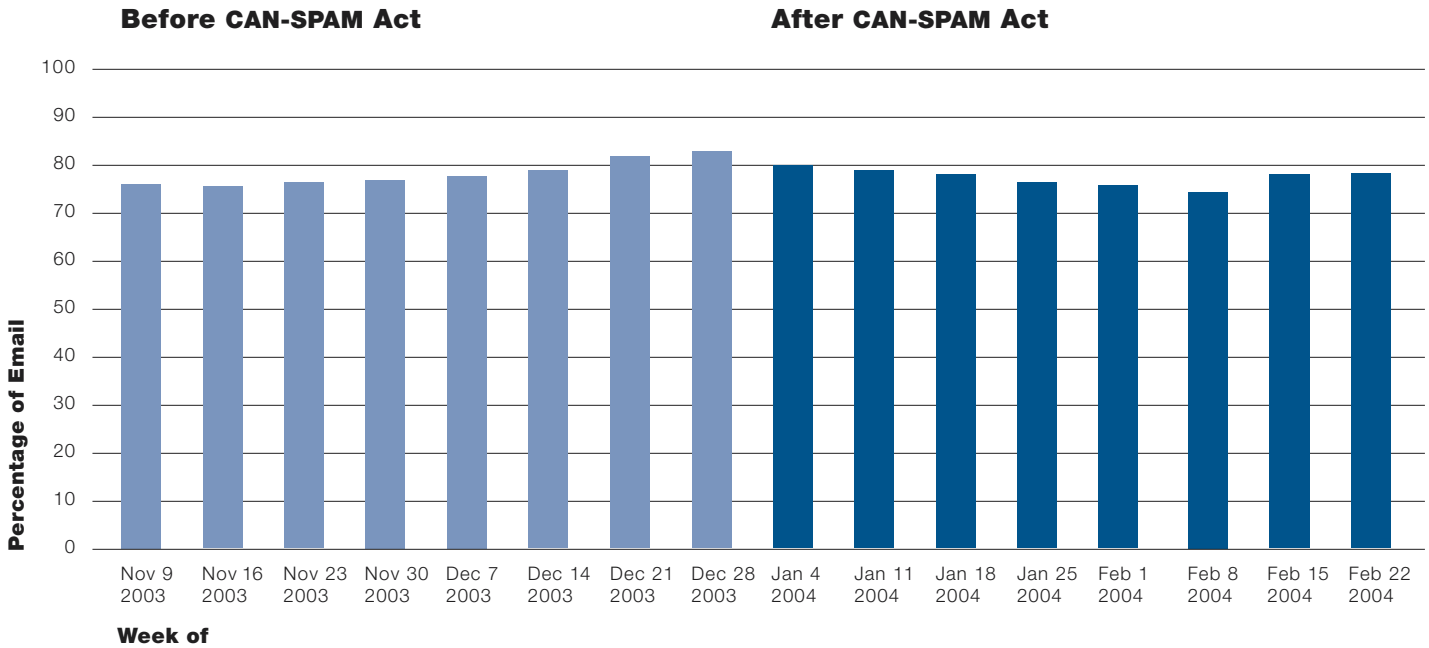
Postini estimates that in the next year spam will increase to 80 to 90 percent of total email. Moreover, the boundary between spam and viruses is blurring. New viruses turn desktop PCs into spam-spewing “zombies.” Postini has also detected a new type of spamming technique called “phishing,” used to dupe recipients into providing confidential personal identity information. You can expect the occurrence of these spam-virus hybrids to increase and develop into even more dangerous and damaging threats.

As shown in Figure 1, the January 2004 CAN-SPAM Act has so far had no effect on spam, primarily because Internet technology allows spammers to hide their identities, and some spammers merely move their operations offshore where U.S. laws cannot touch them. It is also clear from the rise of virus attacks that the threat of vigorous enforcement with severe penalties has not deterred virus writers either.

Threat #3: Directory Harvest Attacks (DHAs)

Also called “dictionary attacks,” this technique steals proprietary information from corporate directories. During a DHA, spammers attempt to deliver messages to multiple addresses, such as johndoe@yourcompany.com, jdoe@yourcompany.com, and john@yourcompany.com. Addresses that are not rejected by the receiving mail server are determined to be valid. A successful

Figure 1 Legislation Isn't Helping to Reduce Spam



DHA can net a spammer thousands of corporate email addresses in just a few minutes. These addresses are compiled and sold to other spammers worldwide; companies who have had their email addresses harvested are vulnerable to an ever-growing amount of junk mail.

Unwittingly, a company's own mail servers can compound the network traffic problem by generating thousands of bounce messages in response to invalid email addresses. The increase in activity creates traffic spikes that are essentially self-inflicted denial-of-service attacks that can completely shut down mail servers. By the time log analysis identifies a suspect IP address barraging an email server with invalid delivery attempts, the valid addresses have long been harvested.

The sobering reality is that on average, 10 percent or less of SMTP connections handled by corporate mail servers are

legitimate email. Postini estimates that 30 to 40 percent of inbound SMTP connections through the corporate mail gateway can be traced to DoS and DHA attacks. These threats can overwhelm mail transfer agents (email servers) to the point of shutdown. As shown in Figure 2, that traffic is over and above the amount of spam and virus email.

Threat #4: Denial-of-Service (DoS) Attacks

DoS attacks are designed to disable a company's network by flooding it with useless traffic, disrupting network connections between machines, or disrupting services to network machines or users. They consume resources, destroy or alter configuration information, and even physically harm or alter network components.¹

As in the virus scenario, hackers can turn unsuspecting computers into "attack droids" by using automated self-propagating programs to scavenge

for computers on the Internet that are poorly secured, or that have out-of-date or non-existent anti-virus software protection. They then install programs that can remotely carry out the attack. Self propagation enables large attack networks to be built very quickly. A by-product of the network-building phase is yet another DoS attack, because searching for other vulnerable computers creates significant traffic as well.

Both DoS and DHA attacks exploit vulnerabilities in SMTP connections. These connection-level threats are difficult to detect and drain server and bandwidth. Unfortunately, first generation desktop and gateway/server solutions are not well equipped to detect these rapid-fire, multi-source SMTP connection-level attacks because they run behind the firewall and therefore can see only a narrow piece of the Internet.

Threat #5: Internal Policy Violations

An often overlooked class of email security threats concerns email that may violate corporate HR, legal or IT policies or industry regulations. For example, companies establish internal policies to enforce HR rules against the inappropriate use of language and content, such as profanity or sexually explicit terms, in internal or external company communications. These policies protect employees from a hostile work environment and protect the company from the risk of employee lawsuits.

The universality and ease of use of email make it a threat to intellectual property, so email policies are established to enforce rules against the disclosure of confidential company information or enforce compliance with industry security, privacy, and ethical practice regulations. Since email can also carry fun but time-wasting content like MP3 and JPG files, companies may also establish policies to monitor email attachments for appropriateness to business activities.

“Because Postini’s data centers sit outside the corporate firewall, they offer a level of security that was not before possible.”

Nucleus Research

Postini Preemptively Protects Your Network from the Top 5 Email Threats

There are plenty of vendors out there that sell point products to address some of these threats. In the past, your options were:

- Buy lots of software
- Buy appliances
- Download freeware
- A combination of the above

But all of these options still allow the threats on your network, and their limitations just lead to more problems. You could buy several products from these different vendors, but the products would not work well together, and each product would have to be separately configured and managed. This scattered approach just adds more complexity and work to your already stretched IT staff.

Postini would like to suggest a better alternative—a single integrated solution that preemptively addresses the top five email security threats. The comprehensive package includes spam and virus filtering, protection against DoS and DHA attacks, content and policy management, disaster recovery, and industry-specific content filtering—all tightly integrated and centrally managed.

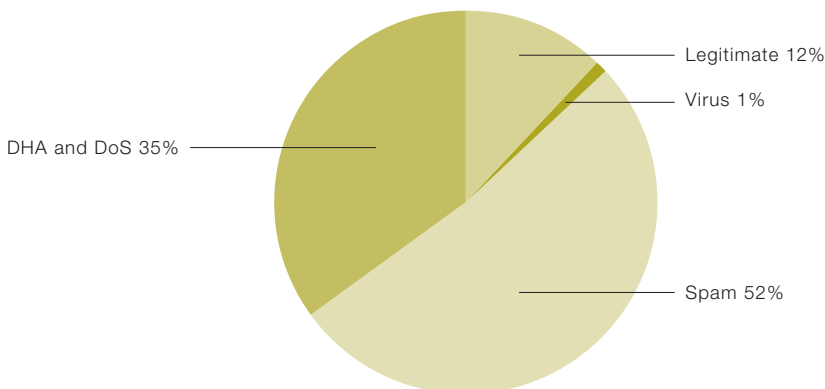
Postini Perimeter Manager™, a managed service solution, stops external email threats before they enter your network. It’s patented preEMPT approach is built on a foundation of four interconnected principles:

Off-premises filtering completely isolates and eliminates external email-borne threats—spam, viruses, and DHA and DoS attacks—from the company network. It also enables companies to apply consistent policies across their entire organization, no matter how large, diverse or widespread.

Pass-through processing examines inbound and outbound email in memory, in real time with no detectable delay using multilayer filters.

Multilayer protection handles all security threats. As shown in Figure 3, Connection Management examines SMTP connections and identifies suspicious patterns of behavior to effectively block DHAs and DoS attacks in real time. Content Security provides policy controls for examining send and recipient names, key words, and attachment type and size to block viruses and spam and enforce established HR, legal and IT policies.

Figure 2 Percentage of All SMTP Connections That Are Email-Borne Threats



Dynamically updated heuristics,

programming rules drawn from high-volume email processing, enable Postini to accurately differentiate email threats from legitimate mail, no matter how much the threats change. Postini consistently delivers the best identification scores in the industry in independent third-party testing.²

Unique Value of Preemptive Email Protection

Postini Perimeter Manager solves all of your email security problems with one convenient, worry-free, integrated security management solution.

Efficient and Effective

- As a dedicated managed service processing hundreds of millions of messages a day, Postini is uniquely qualified to provide the most statistically sound data sample for threat trend analysis.
- According to *Network World*,³ Postini captured the most spam and had the fewest false positives out of 16 solutions tested. Postini can also capture 100 percent of viruses and blocks DoS and DHA attacks. Email security problems essentially disappear overnight.
- Postini's service level agreement offers 99.999 percent availability so your company's critical communications lines are always open.

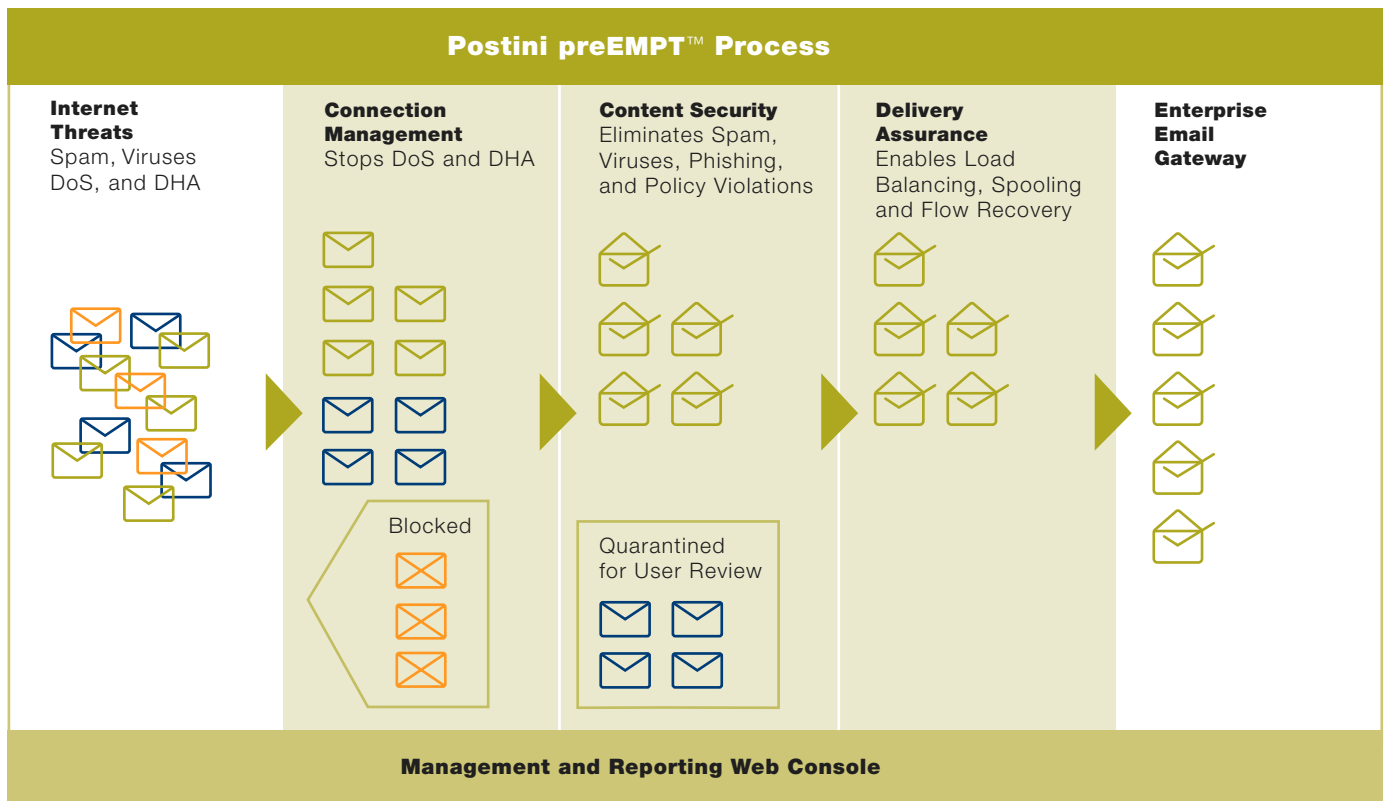
Easy to Deploy and Maintain

- Postini's managed service requires no additional hardware, software, or ongoing maintenance. The solution is designed so you can "set and forget."
- To start the managed service, all that's required is a simple DNS modification to redirect email flow from company mail servers to Postini's data centers.

Easy to Customize and Monitor

- Postini's comprehensive, centralized control and customizable content filtering enable your IT staff to easily implement consistent company-wide rules and policies across the extended

Figure 3 Postini's preEMPT Technology Covers the Top 5 Email Security Threats



enterprise, and to modify them to fit the demands of different users, groups, or countries.

- Real-time Management and Reporting Web Console provides an immediate view of spam, virus and DHA statistics.

Cost Effective

- The all-in-one solution conserves IT resources. Not only will escalating support costs stop, but your IT staff can go back to focusing on core revenue-generating support tasks.
- The scalable solution will keep pace with your company growth.

Conclusion

The challenge of combating email security threats is growing daily. Small and large companies are struggling to recapture their vital communications lines and to regain the smooth of operation of their networks and productivity of their employees. But now there is an effective solution. Postini's preemptive managed service stands guard between the Internet and your company network to eliminate security threats before they can enter and play havoc with corporate resources and intellectual assets.

Notes

1. CERT Coordination Center, <http://www.cert.org>
2. "Spam Shootout," *InfoWorld*, November 2003
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. WP04-01-0403

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.