

What if you could stop spam

and other email threats from ever impacting your network?

Now you can.

With Postini's patented preemptive email protection technology, you can prevent spam, viruses and other malicious attacks from ever reaching your email gateway, protecting your organization and offering the most comprehensive protection available.

LEARN WHAT YOU CAN DO to protect your organization today:

Read this month's issue for the "Essential Guide to Anti-Spam Solutions" and learn about Postini's Preemptive advantage.

LEARN MORE.

Contact Postini to learn more and qualify your organization for a free 30-day, no-risk trial.

www.postini.com
888.584.3150



© 2004 Postini, Inc. All rights reserved. Postini, the Postini logo, Postini Perimeter Manager and preEMPT are trademarks, registered trademarks or service marks of Postini, Inc.

The Essential Guide to ANTISPAM SOLUTIONS

September 2004

By Peter Bowyer

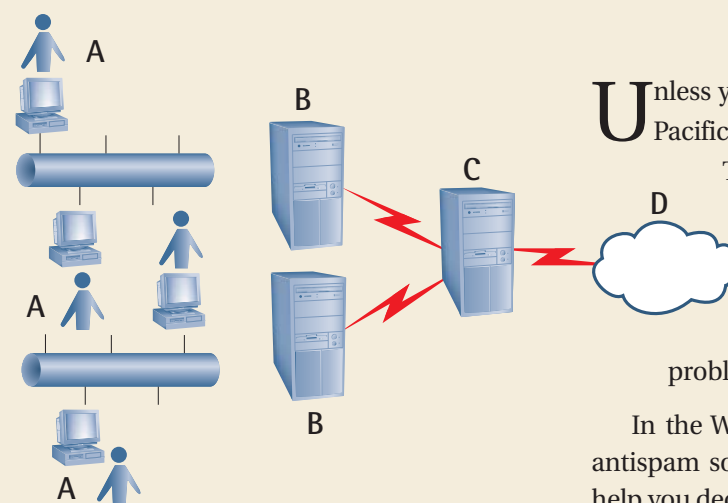


Figure 1 email system schematic

Unless you've spent the past few years in exile on a Pacific island, you know that spam is a hot topic. The trade press discusses spam daily, and the mainstream press runs regular features. Technical magazines carry advertisements for antispam products and services, all of which claim to have the problem licked.

In the Windows marketplace, no "one-size-fits-all" antispam solution exists. But this Essential Guide will help you decide what to look for when you're evaluating which type of antispam solution is appropriate for your organization.

Before we look at the different types of antispam solutions, we need to understand what parts of your email system are affected by spam. Figure 1 shows a typical email system.

Your system may be more or less complex, but it will have some of these components. Spam affects different parts of the system in different ways, and antispam solutions can work in different ways, too. Let's look at how spam affects each point in the email system.

The Essential Guide

September 2004

This special advertising section was produced by the *Windows IT Pro* Custom Media Group in conjunction with Postini. This supplement appears as an insert in the September 2004 issue of *Windows IT Pro* magazine.

Are you prepared

for the newest SPAM & VIRUS threats?

With Postini you will be.

The battleground in the fight against spam is shifting. With new tactics from spammers and hackers designed to defeat conventional anti-spam solutions, the incidence of spam and malicious emails carrying viruses and worms continues to increase—and grow more sophisticated every day.

LEARN WHAT YOU CAN DO to protect your organization today:

Read this month's issue for the "Essential Guide to Anti-Spam Solutions" and learn about Postini's Preemptive advantage.

LEARN MORE.

Contact Postini to learn more and qualify your organization for a free 30-day, no-risk trial.

www.postini.com
888.584.3150



© 2004 Postini, Inc. All rights reserved. Postini, the Postini logo, Postini Perimeter Manager and preEMPT are trademarks, registered trademarks or service marks of Postini, Inc.

Point A The Users

Spam causes a fall in productivity for users. In one respect, the impact on users is simply put: time spent dealing with unwanted email messages is time wasted. But users are affected in other ways, too. For example, if a user has dozens of spam messages every morning, he may not immediately spot urgent genuine messages. And if that happens too often, the value of email as a business communication tool will drop as users seek alternative mechanisms to get their message across.

Point B The Mail Servers

What figures did you use when you calculated how large the storage should be on your email servers? Whatever those figures were, the spam effect is multiplying the volumes of mail your servers have to store by between 5 and 10 times. How quickly will you have to upgrade the servers or add new disks? Much more quickly than you had planned, which leads to added time and money.

Email traffic between your servers is delivered according to a queuing mechanism. The queues take a finite time to process and deliver each message. With high volumes of traffic due to spam, genuine messages can get held up in queues behind the spam, and their delivery will be delayed.

Point C The Internet Gateway

If email shares the same Internet connection with other applications (e.g., Web browsing, Instant Messaging, Voice over IP—VoIP, video conferencing), unexpected increases in email volume due to spam can affect the quality of service you're able to deliver for those other applications. Without expensive traffic-shaping capabilities in your Internet routers, prioritizing critical real-time traffic such as video conferencing, is difficult. You won't be able to guarantee that you have sufficient bandwidth available. You might need to upgrade your Internet connection ahead of time to handle the extra traffic.

Point D Your ISP

You have to deal with spam addressed to your company. ISPs have a much larger problem—they have to handle the spam addressed to all of their customers. So ISPs experience the same problem, but on a much larger scale. ISPs must ensure that despite the increased volumes of email traffic they're carrying, they can still provide the levels of service you expect. Achieving this goal often involves investment in hardware and connectivity—cost that the ISP inevitably passes on to its customers, which is you.

As I mentioned earlier, you can deploy different types of antispam solutions at all these points in your email network. I'll look now at how each type of antispam solution works, and at how appropriate each solution might be for your organization (see text with figures 2 through 5).

Spam Detection Technology

The spam detection landscape, which is constantly evolving, has been likened to an arms race. As antispam developers come up with a new technique to recognize and block spam messages, the spammers counter this with new methods of their own to get around the filters.

Simple keyword detection used to be an effective measure—messages that contained particular words were easily recognized as spam. But we've all seen how spammers routinely disguise the text in their messages with

misspellings, unusual character spacing, and numbers substituted for letters. So the simple filters are no longer very effective.

Many antispam solutions use statistical methods to determine whether a message is spam. Some, using Bayesian algorithms that analyze the patterns of words found in spam and non-spam messages, are able to predict whether a message is spam based on evidence from all the previous messages they've seen.

Those methods rely on being able to analyze the content of an email message. But

recently, spam senders have been able to bypass this kind of analysis by sending messages that have little or no spam content. These spam messages may, for example, contain only a URL that loads an advertisement into the message from a remote Web server when the receiver views the message. This type of formatting doesn't give the content analyzer software much to go on.

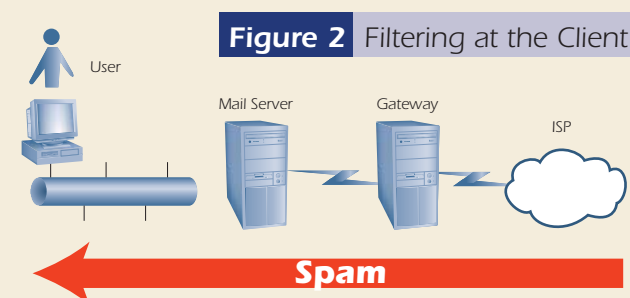
Fortunately, there are other mechanisms for detecting spam, which rely on the characteristics of how a message arrived at the server—for example, which IP address it came from, what other recipients it was sent to, whether other people have received spam messages recently from the same source, how

well the sending server complied with established SMTP protocols, and so on. These connection-level tests can be very effective at detecting spam messages, regardless of whether they have any content that can be analyzed.

A good antispam solution needs to apply these connection-level tests, as well as content tests, to give you good protection. Client and email server solutions are unable to do this effectively because they act after the spam has been received. Gateway, and especially MSP solutions that intercept the email traffic on its way to your network, are well placed to cover both angles.

The Essential Guide

TO ANTISPAM SOLUTIONS



Point A Filtering at the Client

Many antispam solutions install on a user's PC alongside an email client (e.g., Outlook, Outlook Express, Eudora). These products differ in the detail of how they detect spam and what flexibility they offer in dealing with it, but fundamentally they all do one basic thing—they review email messages in a user's inbox and delete or quarantine ones believed to be spam before the user gets to see them.

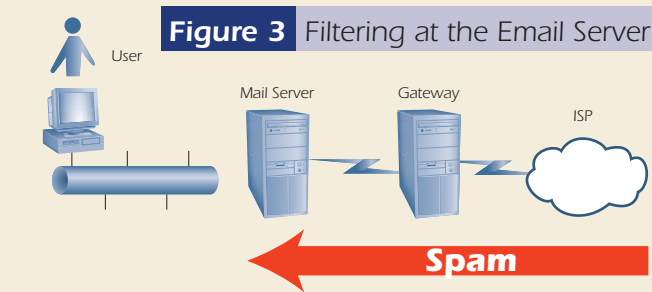
This type of solution is usually easy to deploy for an individual user, and it has an immediate beneficial effect on the user's productivity—the spam is gone from their

inbox. However, before the client software recognized and dealt with the spam, the spam traveled through the company's ISP, Internet gateway, and email servers before reaching the client PC, which could be on a remote connection. As a result, this type of solution has no effect on the problems we identified at those points in the email system. Although antispam products that filter spam at the client are good for individual users, these solutions are less appropriate in all but the smallest organizations.

An example of this type of solution is Qurb, from Qurb, Inc. (<http://www.qurb.com>).

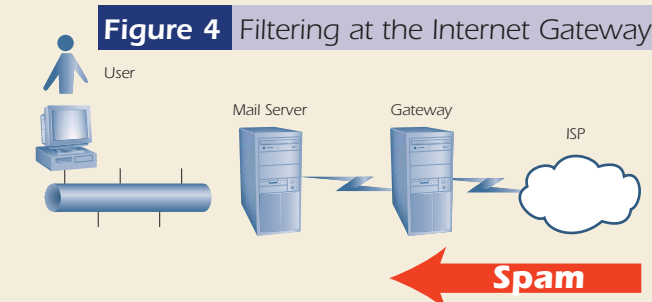
Point B Filtering at the Email Server

Antispam solutions that identify and deal with spam at the email server also provide good productivity gains. They avoid some of the round-trip that the client solutions miss—these solutions deal with spam at the email server before the spam arrives in a user's inbox. But they do this at the expense of creating extra work on the servers; you need more queues and processing power. If your email queues are overloaded with spam already, this type of solution may not help. The spam messages



still have to travel the length of your email system before they are detected, so there is no beneficial effect outside the server environment.

With the release of Exchange Server 2003, Microsoft began providing its own filtering solution known as Microsoft Exchange Intelligent Message Filter (<http://www.microsoft.com/exchange/downloads/2003/IMF/default.asp>). Users of earlier versions of Exchange Server must upgrade to take advantage of this product.



Point C Filtering at the Internet Gateway

Many vendors provide spam-filtering solutions that work at the point that email messages enter your organization—the Internet gateway. Some of these spam filters are software products that install on a standard Windows or UNIX server; others are all-in-one appliances that plug into the right place in your network and that you configure and manage through a Web interface.

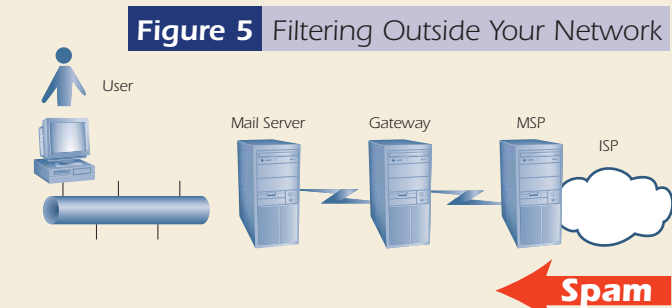
These solutions provide a good level of relief to your email infrastructure. If spam can be dealt with at the gateway, it doesn't clog up your email servers or your internal network infrastructure—the gateway solution allows only genuine email to enter your organization.

Gateway solutions require some reconfiguration of the way email traffic flows into your company, and if you have more than one Internet connection that receives email traffic, you must install a gateway solution for each one. You should also be aware that a spam-filtering gateway can become a single point of failure for your email network. If the gateway is intercepting every email message as it comes in, then email will stop flowing if the gateway goes down.

An example of a gateway antispam solution is Brightmail Anti-Spam, now owned by Symantec (<http://www.brightmail.com>).

Point D Filtering Outside Your Network

A fourth type of antispam solution, a filtering solution provided away from your network by a managed service provider (MSP), has the features of the gateway offerings but also has some extra benefits. A simple change to the DNS records for your domain will cause all your email traffic to be delivered by the MSP's resilient servers. Those servers filter the email traffic for spam and only deliver to your gateway the mail you actually want to receive. No unwanted traffic flows through your Internet connection.



If your organization has a complex infrastructure with multiple ingress points for email traffic, the MSP's solution can handle this type of environment and route the right traffic to the right gateways—in fact, this solution can provide load-balancing and resilience services as well.

MSP antispam solutions are easy to deploy and are suitable for small and large organizations. Typically, neither infrastructure changes nor management of extra servers are required, and if you change how email comes into your organization, the service should be able to handle these changes easily. An example of an email MSP is Postini Perimeter Manager (<http://www.postini.com>).

All of these solutions will bring productivity gains to your users because they no longer have to deal with spam messages in their inboxes. But the best all-round protection for your network from all the effects of spam could come from an MSP solution.

A 25-year IT professional, **Peter Bowyer** has a pedigree in email and collaboration technology going back to the 1980s. He worked with early adopters of cc:Mail and Lotus Notes, and contributed to academic study projects in the field of Computer Supported Collaborative Working. In 1995, Peter founded The Microsoft Exchange Forum, a resource for those brave enough to deploy early versions of Exchange. During the past 5 years, Peter has consulted with large ISPs and E-businesses, helping them develop and deploy robust email and application platforms supporting millions of users.