

# How Small Business is Solving the Spam Problem



an Osterman Research white paper  
sponsored by

**DigiPortal Software, Inc.**

## Why You Should Read This White Paper

---

Most computer users in the workplace would acknowledge that email has become the single most critical productivity application that they use on a daily basis. However, over the past several years, the volume and sophistication of spam has grown to the point where it has made email almost unusable for users that do not have appropriate defenses in place that prevent this unwanted email from reaching their inbox. Because more than three out of five emails reaching the typical workplace user of email are messages that advertise unwanted products or services, email for an unprotected user can actually become more of a burden than an aid to productivity. For smaller organizations, the problem is even worse because budgets and other resources are often insufficient to adequately address the problem.

*Over the past several years, the volume and sophistication of spam has grown to the point where it has made email almost unusable for users that do not have appropriate defenses in place that prevent this unwanted email from reaching their inbox..*

What is needed, therefore, is a means of eliminating spam inexpensively and efficiently – a method that will filter out unwanted spam while not falsely identifying valid email as spam. This white paper describes one approach that smaller organizations can employ that will virtually eliminate the spam problem while restoring the productivity benefits of email.

In order to more fully understand the problems faced by smaller organizations when dealing with spam, Osterman Research undertook a primary research survey specifically for this white paper, some of the results of which are discussed below.

## The Current State of Anti-Spam Defenses

---

Virtually 100% of smaller organizations have deployed anti-virus defenses at various levels of their network, including at the desktop (38% of organizations), server (33%), gateway (18%) and at the hosting provider or ISP (10%). Similarly, the vast majority of smaller organizations have also deployed anti-spam defenses at various layers of their network, although more commonly at the server and gateway levels than at the desktop.

Despite the prevalence of anti-spam defenses, nearly two-thirds of organizations report that they are concerned or very concerned about the overall amount of spam that their organization receives – second only to their concern about

viruses, worms and related threats impacting their network, as shown in the following table.

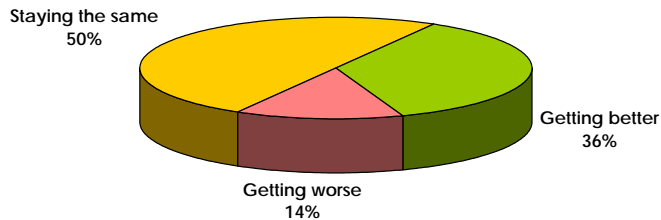
**Leading Problems in Managing Messaging Systems**

Problem	% of Respondents that are Concerned or Very Concerned
Viruses/worms/Trojans impacting networks, systems, etc.	72%
The overall amount of spam received	62%
Phishing attacks reaching end users	52%
Email fraud other than phishing reaching end users	52%
Time spent by employees eradicating spam	48%
Spam/porn relayed from a compromised PC in the organization	47%

Further, one-third of smaller organizations report that their overall problem with spam compared to one year ago has actually gotten worse, while another one-quarter report that the problem is no better than it was a year ago, as shown in the following figure. More than one-half of organizations report that their problem with false positives – valid email mistakenly identified as spam – is no better than it was a year ago or is now worse.

*If an organization of 100 users devoted only one-tenth of an IT staff member's time to maintaining anti-spam defenses – a mere four hours per week – the cost of labor would be \$65 per email user, or ten times as much as for the larger organization on a per-user basis..*

**Effectiveness of Anti-Spam Systems Over Time**



The inability for many smaller organizations to gain ground in the war on spam is due to a number of factors, not least of which is the 'cat-and-mouse' game that most anti-spam solution vendors must continually play with spammers. Because spammers are intent on penetrating anti-spam defenses by using a variety of techniques designed to thwart defenses against the content they send, anti-spam defenses that rely on Bayesian filtering, blacklists and keyword filtering must continually be updated in order to keep up with the newest techniques developed by

spammers. Most static anti-spam defenses will simply degrade over time to the point where their utility as a means of preventing spam from reaching the end user will be minimized.

### Key Differentiators for Smaller Organizations

One of the fundamental problems for smaller organizations in their war against spam is that their requirements for email and anti-spam defenses are nearly as sophisticated as those of larger organizations, but the resources they can devote to email management are dramatically lower. For example, an organization of 10,000 email users can easily afford to devote a full-time individual to updating anti-spam filters and tweaking them for that organization's specific requirements. If we assume that the IT staff member devoted to anti-spam defenses in an organization of this size will have a fully burdened salary of \$65,000 annually, the annual cost of labor for maintaining these defenses would be only \$6.50 per email user per year. However, if an organization of 100 users devoted only one-tenth of an IT staff member's time to maintaining anti-spam defenses – a mere four hours per week – the cost of labor would be \$65 per email user, or ten times as much as for the larger organization on a per-user basis.

*If an organization of 100 users devoted only one-tenth of an IT staff member's time to maintaining anti-spam defenses – a mere four hours per week – the cost of labor would be \$65 per email user, or ten times as much as for the larger organization on a per-user basis..*

What smaller organizations need, therefore, is a method of maintaining an adequate, up-to-date anti-spam defensive capability that is effective at dealing with the spam problem and that is inexpensive to manage. The research that we conducted for this white paper showed that more than one-half of organizations consider it important or very important to reduce the amount of time that IT spends managing their existing anti-spam solution rules and quarantine.

### Organizational Desire for Anti-Spam Solutions

Any anti-spam defense designed for smaller organizations must possess a number of important capabilities:

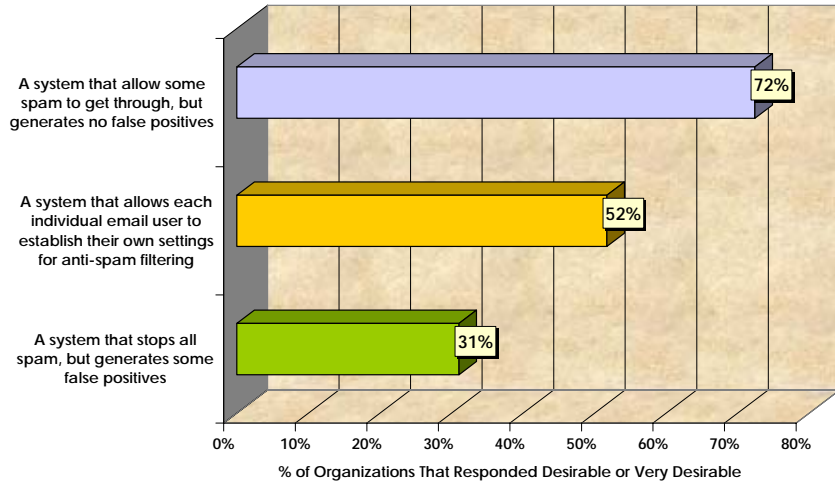
- It must minimize the amount of time that IT staff members spend on managing the system. Because the resources are typically not available in a smaller organization to continually update spam filters or make other adjustments in response to spammers' changing tactics, the ideal anti-spam defense will require virtually no maintenance in order to remain effective.

- It must generate virtually no false positives. Our research found that smaller organizations are very sensitive to the issue of false positives – the vast majority would prefer a system that allows more spam to reach end users while generating no false positives than one that stops all spam while generating some false positives.
- It should allow individual users to establish their own settings for anti-spam filtering, since what is spam to one individual may be valid email to another.

The desirability of various attributes for anti-spam systems is shown in the following figure.

*Smaller organizations are very sensitive to the issue of false positives – the vast majority would prefer a system that allows more spam to reach end users while generating no false positives than one that stops all spam while generating some false positives..*

**Desirability of Various Anti-Spam System Attributes**



While most organizations already have anti-spam capabilities in place, as discussed above, one-half of organizations report that they are planning to add anti-spam capabilities over the next one to two years, indicating that there is a widely felt need for better defenses against spam.

## DigiPortal ChoiceMail

---

ChoiceMail is an anti-spam program that allows individual users to manage their own inbox. ChoiceMail is not a spam filter, but is instead a permission-based email management system that blocks 100% of unwanted email as users define it:

- ChoiceMail creates a “whitelist” of all the email addresses in individuals’ address books. Every time a user sends a message to someone new, ChoiceMail adds the recipient to the whitelist so that it is always up-to-date.
- ChoiceMail sends email from anyone on a whitelist directly to the individual’s inbox. It also lets individuals write rules to accept email that may be desired, even from people not on the whitelist, based on keywords that might be included in emails from previously unknown senders.
- ChoiceMail includes tools that allow individuals to send obvious spam straight to a folder of junk mail for later review. However, unlike spam filters, these tools are not the entire product, but simply an enhancement to ChoiceMail.

*ChoiceMail creates a “whitelist” of all the email addresses in individuals’ address books. Every time a user sends a message to someone new, ChoiceMail adds the recipient to the whitelist so that it is always up-to-date.*

ChoiceMail quarantines any remaining, unrecognized mail. It automatically sends a “registration request” to each unknown sender that directs them to a Web page where they are asked for their name, email address and reason for contacting the recipient. Senders also are asked to complete a task, which is easy for a person but impossible for a computer, such as an automated spam-sending zombie. This process alone eliminates most junk email, since spammers cannot respond to the registration request.

When a sender does register, ChoiceMail alerts the recipient with a pop-up message. Individuals protected by ChoiceMail decide whether to allow the sender to communicate with them or not. While recipients can turn this registration feature off, most users do not because it puts the burden of identifying unknown mail back where it belongs – on the sender.

## Conclusion

---

Spam is a problem that continues to get worse, particularly for smaller organizations that do not have the IT budget to devote to sophisticated and costly anti-spam defenses. However, email is just as critical a business tool for smaller organizations as it is for larger ones, and so the spam problem needs to be solved for smaller organizations in a manner that will allow them to maintain the productivity benefits of email at minimum cost. DigiPortal's ChoiceMail is one such system that combines a very effective challenge-response system and rules-based management system that requires virtually no involvement on the part of IT to manage.

© 2005 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.