

The cost of spam

A white paper from Vamsoft

Abstract

Egg and Spam; egg, bacon and Spam; egg, bacon, sausage and Spam; Spam, bacon, sausage and Spam; Spam, egg, Spam, Spam, bacon and Spam; Spam, sausage, Spam, Spam, bacon, Spam, tomato and Spam.

Today, reading your e-mail is like reading the menu in Monty Python's now infamous café: it's practically impossible to completely avoid the spam. In 2001, spam accounted for about 7% of e-mail traffic - but, since then, the volume has increased exponentially and spam now accounts for about 60% of all e-mail communications.

Dealing with this deluge of spam is an enormous problem for industry. While most businesses deploy some form of anti-spam solution to help combat the problem, such solutions are often far from perfect and can, in fact, sometimes create a whole new set of problems.

This paper will examine the costs of spam – both the obvious and the not so obvious – and outline the criteria which businesses should consider in order to be able to select the most cost efficient anti-spam solution.

Vamsoft Kft.
Budapest
Györök utca 11.
H-1113
Hungary

The cost of spam

Introduction

E-mail is an increasingly critical communication tool for most businesses. In 2005, there were approximately 675 million business e-mail users worldwide. By 2010, it is predicted that that number will have increased to 935 million. E-mail systems from companies such as IBM, Microsoft, Novell and Sun are used by businesses to send an incredible 6,000,000,000,000 e-mails per year – a number which is likely to have almost doubled by 2010. E-mail is not a luxury, it is a business necessity which is used by millions of employees each and every day in the course of their normal work.

Unfortunately, it is not only the volume of legitimate e-mail that has increased; the volume of spam has increased just as significantly and just as rapidly. While business users send about 6 trillion legitimate e-mails per year, spammers send an even larger number of unsolicited junk e-mails. Today, about 60% of all e-mail communications fall into the category of spam.

Dealing with spam has become a major headache for many businesses and the costs involved are far from inconsiderable. Ferris Research estimates that spam will cost businesses \$100 billion in 2007. That is \$50 billion more than in 2005 and \$90 billion more than in 2003 and equates to an annual cost of about \$130 per business user. Multiply that \$130 by the number of employees in your company, and you'll have a ballpark estimate of how much spam is costing. It's probably more than you thought, huh?

So, where exactly do these costs come from and what can a business do to lessen the cost of combating spam? Read on!

The cost to business

There are a number of ways in which spam impacts upon operational costs:-

- **Productivity.** Employees need to deal with the contents of their inboxes – and that includes dealing with their spam. While dealing with spam may seem like a relatively minor task, the aggregate effects can be far from minor. For example, should an employee receive 10 spam e-mails per day and spend 10 seconds on each, he'll expend more than 10 hours during the course of the year. In a company with 100 employees, that's 1000 hours lost to dealing with spam. Each and every year. Multiply those 1000 hours by the average hourly wage within the company, and the high cost of spam becomes immediately apparent.
- **IT resources.** To put it simply, spam sucks up resources. Bandwidth is needed to deliver the spam and disk space is needed to store the spam – and, of course, companies foot the bill for both. While the cost on a

The cost of spam

per-spam basis is extremely small, the aggregate costs can be considerable.

Even when an anti-spam solution is put into place, spam continues to cost businesses both time and money. Contrary to the claims of some developers, no anti-spam solution is 100% effective: some junk e-mails will always slip through the net – irrespective of how good that net may be.

- **False negatives.** Spam e-mails that are not identified as such by the company's anti-spam solution. False negatives end up in users inboxes and, as already outlined, result in lost productivity.
- **False positives.** Non-spam e-mails that are incorrectly identified as spam by the company's anti-spam solution. According to Ferris Research, it costs an average of \$3.50 to recover an e-mail which has been incorrectly deleted or quarantined. There are, however, other – and potentially far greater – costs associated with false positives. These are discussed in the next section (“The perils of the false positive”).

There are a number of other costs too. The cost of the anti-spam solution itself, for example, and the cost of the time needed to install and maintain it.

Additionally, there are also costs which simply cannot be quantified. Phishing scams may result in sensitive company information falling into the wrong hands. And any company which fails to block offensive spam could face legal action from its employees. While no such cases have yet been brought before the courts, in today's litigious society, it is something which is likely to happen sooner rather than later (see Resources).

The perils of the false positive

A recent court case highlighted the business risks associated with false positives. In May 2006, a Colorado-based law firm upped the settings on its Barracuda Spam Firewall 200 in an attempt to block out spam that was finding its way to users' desktops. Unfortunately for the law firm, the Spam Firewall not only blocked the spam, it also blocked e-mails from the United States District Court for the District of Colorado – including an order which set the date for a settlement conference. Because of its non-appearance, the law firm was ordered to pay the costs of opposing counsel, who did appear at the conference. “It is incumbent upon attorneys to adopt internal office procedures that ensure the court's notices and orders are brought to their attention once they have been received,” said Judge Michael J. Watanabe. The Judge went on to state, “That it would have been a very simple task to whitelist the United States District Court for the District of Colorado's domain name of “cod.uscourts.gov” to insure that such emails with this domain name would always be received.” The ruling left the hapless law firm facing a bill of several thousand dollars.

The cost of spam

Yes, the judge was right: it would indeed have been easy for the law firm to have whitelisted the Court's domain. Whitelisting is a method of instructing a spam filter to ignore e-mails from certain addresses or domains. To whitelist an address or domain, you add it to a database which is referenced by the spam filter. E-mail from any address or domain which is in the database is automatically allowed to pass through the spam filter and is delivered to the intended recipient. Whitelisting is a simple and effective way of reducing the likelihood of false positives – but, unfortunately, it's far from being foolproof. In a company that has regular dealings with a large number of other organizations and individuals, creating and maintaining a whitelist can be a job of nightmare proportions. The possibility of human error exacerbates the problem: it's extremely easy for an address or domain to be overlooked or to be entered incorrectly – and, as demonstrated by the above case, such omissions or errors can prove to be extremely expensive.

"In the legal context, misidentifying legitimate mail – whether from opposing counsel or from the court – as spam can have significant and costly consequences and can lead to missing key events, being out of the loop, or just plain old miscommunication. I would have in place a program that automatically whitelists the address or domain of the courts in which the lawyer regularly practices or every single court in the country," said Venkat Balasubramani, a Seattle-based lawyer who specializes in internet and technology matters.

Law firms are not the only businesses which can be damaged by false positives; with so much of modern commerce being conducted electronically, any company which relies on e-mail is at risk. Contracts can be lost, sales can be lost, reputations can be damaged and, of course, any company which appears to ignore e-mails from its customers may very quickly be abandoned by those customers.

That's not where the problem ends. False positives also diminish productivity. Should employees find that they need to frequently examine deleted or quarantined items in order to check for misidentified e-mails, they might as well be checking their spam; the time expended will be the same. For this reason, false positives can very quickly erode the ROI which the anti-spam solution was expected to achieve.

The solution to the problem is, as stated by Venkat Balasubramani, to use a program which automatically creates its own whitelist. This functionality is now featured by a number of spam filters. How does it work? Basically, every time an e-mail is sent, the recipient of that e-mail is automatically added to the whitelist. Such self-learning whitelists have the potential to significantly lessen the incidence of misidentification.

The cost of spam

What should you look for in a spam filter?

From the many anti-spam products on the market, how should you identify the product which will best suit your needs? What should you look for? Some key points are discussed below.

- **Server-based solution.** To achieve maximum efficiency and deliver the maximum possible ROI, the solution must be server-based. Client-based solutions are time consuming and costly to deploy and maintain and, as they do not deal with spam at the gateway, they do not eliminate infrastructure costs.
- **Multiple detection mechanisms.** To accurately detect spam requires the deployment of multiple detection mechanisms. The constantly evolving nature of spam means that no single detection mechanism is able to produce accurate or reliable results.
- **Automatic whitelisting.** To minimize the incidence of potentially costly misidentification of e-mail, addresses must be automatically added to the whitelist.
- **Easy review by users.** Even the best anti-spam product will sometimes misidentify e-mail. To avoid impacting on productivity, an anti-spam product must provide users with an easy and speedy way to review deleted or quarantined items.

About Vamsoft's ORF Enterprise Edition

ORF is a server-based spam filtering extension for Microsoft IIS SMTP Service and Microsoft Exchange Server 2000 and 2003. ORF's features include:-

- **Multiple detection mechanisms.** To deliver the maximum in accuracy, ORF leverages multiple detection technologies including DNS and SURBL blacklist checks, greylisting, keyword filtering and attachment filtering.
- **Automatic whitelisting.** In order to minimize false positives, ORF automatically adds any addresses to which you send e-mail to its whitelist.
- **Easy review by users.** ORF enables you to mark e-mails caught by the filter with a customizable flag to enable easy and speedy review by users.

The cost of spam

ORF also supports Recipient Validation Testing using Active Directory, an SQL database or an external text file, reverse DNS and HELO blacklist testing, enables the production of detailed reports and much more.

To find out more about ORF, please visit:-

<http://www.vamsoft.com/orfintro.asp>

About Vamsoft

Since 1995, Vamsoft has been developing innovative applications for businesses and government and their customers include more than 6,500 businesses of all sizes, universities and ISP's.

To find out more about Vamsoft's products, please visit:-

www.vamsoft.com

About the authors

Brett Callow and Rhonda Turner are technical consultants providing services to a number of leading international technology companies and have been extensively involved in the planning and development of various industry-standard IT certification examinations. Brett has been awarded Microsoft's Most Valuable Professional (MVP) designation for the last 4 years. MVPs are exceptional technical community leaders from around the world who are awarded for voluntarily sharing their high quality, real world expertise in offline and online technical communities by Microsoft. To contact the authors, e-mail brett@mvps.org.

References

Ferris Research Industry Statistics

<http://www.ferris.com/research-library/industry-statistics>

Porn spam could land EU firms in hot water

<http://www.silicon.com/research/specialreports/thespamreport/0,39025001,39120300,00.htm>

Spam filter costs lawyers their day in court

<http://www.washingtonpost.com/wp-dyn/content/article/2007/07/13/AR2007071300606.html>

Pace v. United Services Automobile Association, Case No. 05-cv-01562-LTB-MJW, D. Co., 2007 U.S. Dist. LEXIS 49425, July 9, 2007

The cost of spam

<http://spamnotes.com/files/31236-29497/Pace.pdf>