

## The Hidden Cost of Spam

When e-mail entered mainstream corporate America in the 1990s, business reaped a coup in productivity, and a revolution in how people in business communicate was born. No longer did employees need to catch their bosses or peers face-to-face in the office or even play phone tag. One could easily ask a question and the respondent could answer just as easily in his own time. People quickly discovered that sending an e-mail was much more efficient than picking up the phone. As an added bonus, an e-mail message created documentation of the message and the time it was sent, and people started sending message at all hours of the night just to prove how hard they were working.

Unfortunately, a disturbing trend has appeared in the last few years as e-mail marketers have discovered the high return on investment of bombarding large numbers of people with spam messages for products ranging from mortgages to sexual stimulants to porn sites. A very minimal response is required for these types of campaigns to have a high return on investment, which is very motivating for people involved in this activity.

Do you know how many spam messages enter your organization? People who measure spam report that in 2001 only 25 percent of all e-mail circulating was spam. Today, an estimated 75 percent of all e-mail circulated in the United States is spam. While this may seem like simply a nuisance, there are costs associated with this when the number of messages received every day is multiplied by the number of employees at the company and converted to salary costs, not to mention other costs. Let's look at the following:

- Time spent identifying, reading and/or deleting the messages
- The bandwidth consumed during the delivery
- Data storage on the file server
- Legal risks of racially or sexually harassing e-mails

### **Time spent dealing with spam messages**

Let us say that the average employee in your organization makes \$45,000 per year and spends just 10 minutes per day identifying and deleting spam messages.

Average time spent per day: 10 minutes

Average daily pay: \$175

Annual cost per employee: \$875

Based on these estimates, the cost of this "nuisance" is approximately \$875 per year per employee. If your office has 10 employees, this is an \$8750 problem per year. If you have 100 employees, this costs your business \$87,000 per year. If you could block 90 percent of these messages accurately, you could use the savings to invest in a new brochure, training for your employees or salary for a salesperson – anything that adds value to your bottom line.

### **The bandwidth consumed during the delivery**

A bit more esoteric than the easily measured cost of employee productivity loss, the opportunity cost of lost bandwidth needs to be viewed from the perspective of downtime, when the system is not available to support some business-critical activity. For example, your employees are probably blissfully unaware of the

creating innovative it solutions

network bandwidth consumption associated with downloading large files, playing online games or accessing streaming audio or video. These can all hamper network performance for all users.

Think about the last time your server went down. How productive were your employees? When large numbers of spam messages are filling up your e-mail boxes, this creates a partial “downtime” situation.

### **Data storage on the file server**

Whether it is your own server or an outsourced one, all of these spam e-mails require storage space, backups and e-mail system administration time. None of this is free. Just for argument’s sake, let us say that the average employee in your organization uses \$60 in storage and labor per year and 75 percent of the messages received are spam.

Average cost of storage per employee: \$60

Percentage volume of spam: 75%

Annual storage cost per employee: \$45

Based on these estimates, the cost of the privilege to have spam delivered to your business is \$45 per year per employee. If your office has 10 employees, this is an \$450 problem per year. If you have 100 employees, this costs your business \$4,500 per year. If you could block 90 percent of these messages accurately, you could keep this money where it belongs – contributing to your bottom line. The ideal situation is to prevent spam from entering the company network in order to reduce e-mail storage costs and increase network performance.

### **Cost of inappropriate e-mail content**

Another potential cost of internal occupational spam is litigation. Companies are liable for the content of e-mails and racially/sexually harassing e-mails can lead to substantial lawsuits. The alarming thought is that it only takes one e-mail to offend an employee and the cost could run into six figure sums. You can put in your own figures to the equation.

### **The Solution**

So what can you do about this problem? There are many products on the market that claim they will protect your organization from spam. Here are some points to consider:

- ***Is the anti-spam product a derivative of open source software?***  
The good and bad news about open source software is that it is generally free. Free is good for the consumer, but it is also good for the spammer. Spammers use these free tools to test their spam to see if it will get through the most commonly used (free) spam filters. A proprietary product that was developed from scratch is likely to be much more effective than one based on open source software. This also means it will be more expensive, but remember what we just said about the hidden costs of spam? The return on investment for this type of software is relatively short when you consider the cumulative effects of spam.
- ***Does the product also offer anti-virus protection?***  
If your e-mail is being screened for spam, this is also a good time to have it screened for viruses. Anti-spam software that also offers anti-virus protection can be a real bargain and save you even more money in increased uptime and time not spent cleaning up viruses.

- ***Where does the questionable e-mail reside?***  
Does the software quarantine questionable e-mail on the server, or do all messages arrive on the desktop to be screened in your inbox? A product that quarantines questionable e-mail to the server, before it reaches the desktop offers superior protection. Reviewing the questionable e-mails once per day or week is quicker and less frustrating than dealing with them one-by-one as they come in. Additionally, if the product also offers anti-virus protection, preventing the viruses from ever reaching the desktop decreases the chance that the virus will have a chance to do its damage.
- ***Can the end-users set up their own whitelists and blacklists?***  
There is a saying that one person's spam is another person's ham. Products that allow only the system administrator to create lists of domain names and users whose e-mail is allowed to get through or is blocked will not satisfy the needs of a diverse organization. The system administrator should be able to override the individual user's settings to block porn or other materials that could create a potential lawsuit, but each of the employees should be able to create their own lists.

### **Conclusion**

By combining the hidden costs of spam, the cumulative effect is significant. The return on investment for software that blocks spam and potentially viruses too is relatively short compared to the cost of doing nothing. There are many products on the market that purport to block spam, but it is important to consider the characteristics of the software listed above before making a purchase to get the most effective product within your budget.