

Combating SPAM Problems in a Corporate Environment

Perhaps no problem plagues the Internet as deeply as that of unsolicited junk E-mail, or SPAM. While there's no doubt that SPAM can be annoying to the end users, SPAM can cause problems for both the network administrators and for those who own or manage a company. The reason for this is that SPAM robs your company of productivity and of system resources.

SPAM and Backend Mail Systems First, let's take a look at the system resource that are consumed by SPAM. Any time that an E-mail message is sent to someone in your organization, the message must first pass through your organization's Internet connection and through the firewall before reaching your Exchange Server. Regardless of how much bandwidth your organization may have, there is a finite amount of data that the Internet connection can handle in a given amount of time. This means that if your organization is using their Internet connection at or near its total capacity then any time you receive a junk E-mail message, other legitimate messages are kept waiting until bandwidth becomes available. Once a message passes into your organization, it must pass through your firewall, which then hands the message off to the appropriate Exchange Server. Both the firewall and the Exchange server use CPU cycles and memory when processing the message, resources that would be better used elsewhere. Keep in mind that each E-mail message that your organization receives consumes a tiny amount of resources such as bandwidth, memory, CPU cycles, etc. Most organizations would never even notice the impact caused by receiving a few junk E-mail messages. The real problem is caused by the sheer volume of junk mail that pours into many organizations. Before I implemented SPAM protection in my own organization, I was receiving more junk messages than legitimate messages; upward of 200 junk messages a day. When an organization is plagued by excessive SPAM, disk space on the Exchange Server also becomes an issue. To most people, the idea of storing SPAM is absurd. However, a recent IDC report estimates that 44% of users retain E-mail messages for a year or more. Even if your users aren't storing SPAM, Exchange is designed to retain deleted items for a period of time. Therefore, those SPAM messages that your users are deleting are still stored on the server for a period of time.

SPAM and Employee Productivity SPAM not only impacts the back end information systems, it can lead to a loss of productivity as well. The most obvious way that productivity is impacted is that if users are busy deleting junk mail then that's basically wasted time in which nothing productive is being accomplished. Furthermore, if a user is constantly flooded with SPAM, then there's a good chance that in the midst of deleting the SPAM, important messages may also be accidentally deleted. On more than one occasion I personally have accidentally deleted important messages from clients while cleaning out SPAM. This has sometimes resulted in a loss of income. Further more, if your employees jobs involve sending E-mail messages to clients or doing Internet based research, their Internet access could be greatly slowed because the steady flow of inbound SPAM is consuming a large portion of the company's Internet bandwidth. As if that weren't enough, SPAM sometimes contains malicious scripts, viruses, etc. I recently helped a friend who owns a trucking company deal with a SPAM problem in their organization. The organization was receiving so much SPAM that it was becoming difficult to even use E-mail. Each user was receiving dozens of messages every hour. The real problems started though when the company received an outrageously expensive phone bill. One of the users had apparently opened a message containing a malicious script that caused the PC's modem to dial a 900 number. In the end, I was able to get rid of the dialer, but the SPAM problem had grown so far out of control that everyone in the company had to get a new E-mail address. Of course that meant informing all of the clients of the new contact information. To make a long story short, this entire ordeal was a huge problem for this small company. One of the more overlooked ways in which SPAM effects an organization's productivity is in the amount of time that users spend deleting it. A recent IDC white paper estimates that one in every five E-mail messages that a person receives is SPAM and that the average employee spends about 5 seconds getting rid of each SPAM message. Personally, I think that the ratio of SPAM to legitimate messages is much higher than one in five. Typically, in an average day I get about 30 legitimate E-mails and well over 200 SPAM messages. Let's assume that IDC is correct though and that one out of every five messages that your employees receive are SPAM. Now, let's assume that the average employee gets 50 E-mail messages per day, ten of which are SPAM. If IDC is correct in saying that it takes 5 seconds to look at and delete a SPAM on average, then an employee that receives 10 SPAMs a day wastes 50 seconds dealing with SPAM. At first, 50 seconds of wasted time sounds trivial. However, if an organization had 2000 employees, then the employees would be collectively wasting 10,000 seconds or 27.7 man hours per day. This works out to 7,222.2 wasted man hours each year. If the average employee earned \$15 per hour then the company would be looking at a financial loss of \$108,333.33 per year in wasted man hours, just because each employee spent a mere 50 seconds a day dealing with SPAM.

Fighting SPAM So the real question now is how do you deal with SPAM? Several states have passed legislation making SPAM illegal, but I personally don't see the problem going away. Much of the SPAM is sent from foreign countries or from other states. This means that state level anti SPAM legislation is unenforceable. Microsoft has built mechanisms into Outlook that allow you to fight SPAM. The problem is that configuring Outlook to filter SPAM without using third party software is a lot of work. I have described the necessary procedures in the article found at http://www.brienposey.com/kb/filtering_spam.asp Additionally, Spammers are always using new spamming techniques, so the Outlook filters that work today may not work tomorrow. Even if you could keep an Outlook level SPAM filter up to date, there's a huge administrative burden since each user's Outlook profile must be maintained independently. The only real solution is to stop SPAM at the Exchange Server level, before it can make its way into the user's mailboxes. While no anti SPAM product is 100% effective, there are several good products for fighting SPAM at the Exchange level. My three personal favorites include GFI MailEssentials, Red

Earth Policy Patrol, and SurfControl. Each of these products does a reasonably good job filtering SPAM at the Exchange level, but each also has its strengths and weaknesses.

- Red Earth Policy Patrol 2.5
- GFI MailEssentials 9/10
- Surf Control 8/10

Red Earth Policy Patrol 2.5 Policy Patrol is a comprehensive e-mail-filtering tool that offers advanced anti-spam, anti-virus, content & attachment checking, disclaimers, archiving and reporting. Policy Patrol works with Microsoft Exchange Server 2003/2000/5.5, Lotus Domino and any other SMTP mail server (found at <http://www.policypatrol.com>). At the moment, Policy Patrol is the only one-stop solution that can filter internal as well as external mails (if installed on Exchange Server 2000 or 2003), whilst offering a full feature set including spam black lists and disclaimer features, and the option to apply different rules depending on whether the mail is internal or external. The product installs with relative ease and, with its pre-written sample policies, the administrator will be able to start protecting the network almost immediately. Policy Patrol also has many useful pre-set policies that allow the new installation to be put in place quickly and effectively while new policies are written. Using filtering, Policy Patrol cuts down on false positives by allowing word scores to differentiate between certain phrases and words. Using this approach, an administrator can ensure minimal disruption is caused while still maintaining high standards of protection. In all, this solution provides effective filtering and has the benefit of anti-virus to further protect your network from both known and potentially dangerous new threats, while ensuring that content is both legal and appropriate.

GFI MailEssentials Another of my personal favorites is GFI MailEssentials (found at <http://www.gfi.com/mes>). One of the reasons I like the GFI product is that it has some really practical methods for catching SPAM. For starters, the product looks at what language the inbound messages are sent in. A lot of SPAM comes from foreign countries and is not even written in English. If a message comes into your organization and is in a foreign language, the message can automatically be treated as SPAM if you choose. Another big plus is the way that GFI makes use of black lists and white lists. While all of the major anti SPAM products use black lists and white lists, the GFI product can also use third party blacklists. This means that the GFI product can take advantage of Internet databases containing the IP addresses of known spammers. What makes the product even more attractive is that the anti spam DNS blacklists checking (ORDBC etc.), custom blacklist and automatic white list modules are freeware. In addition, one can configure one disclaimer. These features will not time out after evaluation has ended! Another nice perk to GFI MailEssentials is that they are offering disclaimer software for free to users of GFI MailEssentials. The disclaimer product is an add on module that allows you to place a legal disclaimer at the end of end of outbound messages. Such disclaimers can protect your company against litigation arising from an employee's inappropriate use of E-mail. Perhaps my favorite feature of GFI MailEssentials was that it allows greater control of detected SPAM than some of the other products. For example, SPAM can be automatically deleted, forwarded to someone for review, or flagged as SPAM and sent to the user for review. This option to review mail flagged as SPAM allows for greater fine tuning and thus better SPAM detection accuracy than you would get from an out of the box configuration. If a message has been flagged as SPAM, you can configure GFI MailEssentials to deliver a fake non delivery report to the sender. The idea is that if you can trick the sender into thinking that your E-mail address is bad then there is a really good chance that you will be removed from the sender's mailing list. Product info - "Dealing effectively with spam"

SurfControl SurfControl is another good anti SPAM product (found at <http://www.surfcontrol.com>). SurfControl takes an eight step approach to filtering SPAM. First, SurfControl closes the mail relay host. This prevents spammers from being able to relay SPAM through your server on its way to other destinations. Closing the relay host is a nice feature, but can be easily done directly through Exchange. Next, SurfControl uses an anti SPAM agent to test each inbound message. Some of the tests performed on the messages include a dictionary based scan that looks for words and phrases commonly used in SPAM, and a client name DNS lookup. This lookup tests each address by comparing the sending domain's DNS entry against the IP address that actually sent the message. This tests for spoofed E-mail addresses. Messages are also checked against a live database of blacklisted senders. Senders can be blacklisted by domain, E-mail address, and IP address. One of the features that I liked the best about SurfControl is that the online database contains actual SPAM messages that have been hashed to produce digital signatures. When a new message arrives, the message's digital signature is compared against those stored in the database. Finally, if a message contains HTML code, the HTML code can be stripped from the message, removing any potentially harmful code.