Attack of the Killer

Spam can be a drain on productivity. Managed service providers are one way to take on unwanted e-mails.

WRITTEN BY ESTHER SHEIN

PHOTOGRAPHS BY DOUG KNUTSON

LIFE INSIDE THE Minnesota Twins organization is the way it should be—all about baseball, hotdogs, and Cracker Jack® with no worries about its growing spam problem. As a small organization with some 175 users, the four-man IT department needed to keep its eye on more mission-critical issues, not deal with employee complaints about the onslaught of offensive and annoying e-mails.

Still, the team needed to strike out spam. Productivity was being compromised as users spent a good hour or two a day sifting through e-mails promoting free trips, mortgage approvals, and pornographic content. Putting individual spam filters on every PC was far too time consuming for the Twins's small IT staff. So they went on the offense and offloaded the problem to MessageLabs, a managed service provider (MSP), which provides them with e-mail filtering and virus-protection services. The arrangement has been a home run. MessageLabs stops about 99 percent of all spam arriving in an estimated 7,000 to 8,000 e-mails per day. "This saves us lots of time, and our server is free of malicious e-mails," says Erik Vermeulen, PC support specialist and network administrator at the Minnesota Twins, based in Minneapolis.

Not all businesses are as lucky as the Twins. Spam infiltration is a growing problem, costing North American businesses without the requisite network protection about $5 billion a year—an average of $10 per user, per month, according to Ferris Research, a consultancy specializing in messaging and

collaboration. In addition to sapping productivity, spam raises liability concerns in the event a company fails to prevent inappropriate material from entering its network. Yet aside from the nuisance and liability factors, spam, surprisingly, is not the main culprit clogging bandwidth in corporate networks.

"In most cases, the amount of network bandwidth that spam takes up is not tremendous, in spite of what the vendors say," according to Richi Jennings, practice leader for spam at Ferris, based in San Francisco. Although it's estimated that the amount of spam traveling across the Internet is anywhere from 50 percent to 70 percent of all e-mails, "e-mail is only one application and is not a huge portion of traffic," Jennings explains. Therefore, the impact on bandwidth is not nearly as significant as the amount of time organizations are taking to try to rid the network of incoming spam, he adds.

Yet, with e-mail usage surpassing phones and faxes as the number-one business communications tool, the spam problem can't be understated and, certainly, cannot be ignored. A recent Ferris survey found nearly half of respondents (46 percent) believe that spam is "a major concern" or "one of the biggest issues" they face. That's why many IT managers, like Vermeulen at the Minnesota Twins, have turned to outsourcers to handle the problem for them. "E-mail is vital, and yet cleaning up this sewage isn't actually at the top of anyone's to-do list in terms of delivering competitive advantage, and that makes it ideal to outsource it and make it someone else's problem," says Andrew Lockhart, director of product marketing at Postini, a managed service provider in Redwood City, CA, which specializes in e-mail security solutions, including blocking spam.

Beyond outsourcing, other tactics for combating spam include installing filtering software on PCs and servers, which must be constantly monitored

and updated, or installing an "appliance," a separate computer preloaded with software that does the filtering and is more low maintenance. "That can be quite good for small companies, but very expensive,'' says Jennings.
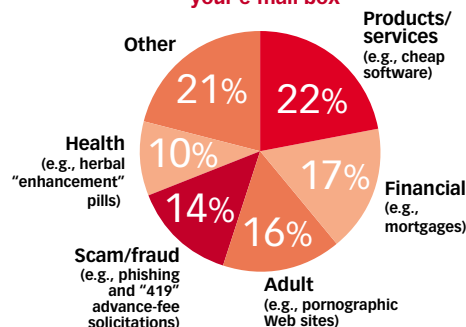
MSPs to the Rescue

With the managed service model, incoming e-mail is rerouted to the provider, and bad e-mail is "scrubbed" out. Lockhart estimates that only 1 in 12 e-mails coming into Postini is legitimate, and that a mere fraction is all the customer ever sees. "If you built a castle and you're going to have a moat, do you put it inside or outside the castle walls?" he asks. "Outside—you want to stop the stuff before it comes inside." Managed service providers also provide an edge in the fight against spam because they are familiar with certain IP addresses that are notorious for sending spam, and automatically block them, Lockhart says. "We know who's naughty and who's nice and we can block them without having to look at the e-mail message itself," he explains. "It's like if you get a phone call and you look at the caller ID, you know who you want to talk to and who you don't."

Postini's pricing structure as well as the software's ability to let employees customize what e-mails they do and don't want was what sold Eric Kahle's company on outsourcing some of their

Junk Mail
A breakdown of spam clogging up your e-mail box

Other 21%

Products/ services (e.g., cheap software) 22%

Health (e.g., herbal "enhancement" pills) 10%

Financial (e.g., mortgages) 17%

Scam/fraud (e.g., phishing and "419" advance-fee solicitations) 14%

Adult (e.g., pornographic Web sites) 16%

SOURCE: Ferris Research

Steps for Stamping Out Spam

1. Have an acceptable e-mail usage policy that addresses what employees can and cannot send and receive.
2. Train e-mail users not to give out their e-mail addresses unless they trust the source.

3. Don't publish e-mail addresses on company Web sites—that's an easy target for spiders (software that crawls across the Web searching for e-mail addresses).
4. When e-mail addresses need to be on a Web site, publish ones that can be changed every day or two. The theory is a user will click on that e-mail address if they need to send an e-mail that day, but a spider may try to send spam tomorrow or at a later time.

e-mail security needs. Postini bases its pricing on a per-user model; for a 200-user account, for example, the list price can vary between $5 and $25 per individual annually.

As far as customizing goes, users can rank incoming e-mail by type from 1 to 5 on Postini's filter control scale. Kahle's company, a beverage manufacturer in southern California, has also set policies on what constitutes acceptable e-mail and what needs to be "locked out" for its 145 users. "We're pretty strict about what comes in," says Kahle, a network technician at the firm. "We have set parameters, and every user on our system has those parameters given to them. For example, we don't allow porn, we don't allow special offers, we don't allow get-rich-quick-style spam."

Prior to going with Postini about a year ago, Kahle estimates that between 60 percent and 70 percent of incoming messages were spam, and bandwidth consumption was greatly compromised. Although it varied by user, some employees had been spending up to an hour and a half a day deleting messages, he says, and the outsourced service has had a huge improvement on productivity.

Another benefit of the Postini service is a regular stat report on what viruses are coming in, what users are receiving more spam than others, and what space is being saved on their server—all of which are important because the mail server is only allocated as much room as is needed. The provider also offers a pooling feature, which means if the company is doing some maintenance on the network, and Kahle's group needs to reboot their e-mail server, the messages are pooled instead of being bounced back to the sender until communication is reestablished.

All of these features have left Kahle and his four-person staff more time to handle IT issues that give the company a competitive advantage. Vermeulen at the Twins's concurs, saying spam is no longer throwing them a curve ball.

"As a network guy, it means I have two extra hours a day that I can spend doing real IT stuff like looking at our network and server," he explains.

Esther Shein is a freelance writer and editor specializing in technology and business.

No CAN-SPAM do

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act) was signed into law by President Bush on Dec. 16, 2003, and took effect on Jan. 1, 2004. The law establishes a framework of administrative, civil, and criminal tools to help combat unsolicited commercial e-mail, also known as spam.

Industry observers say, however, the Act may not have the effect proponents intended. "We don't think it's having a big impact on spam, but it's setting the bar for saying what is and isn't acceptable in this society, and what types of behaviors are acceptable for direct marketers," says Richi Jennings, practice leader for spam at Ferris Research in San Francisco.

According to The Spamhaus Project, a Web site that tracks the biggest spammers worldwide, the Act is "a serious failure of the United States government to understand the spam problem." The project's position is the Act attempts to regulate rather than ban the practice of spamming. "We believe this is a serious mistake, and that CAN-SPAM will succeed only in increasing spam volumes and the number of spammers. Additionally, by signaling to the world that spamming is now legal, we believe that the United States is inviting a tsunami of spam from Asia," Project Director Steve Linford writes on the Spamhaus Web site.

As a provision of the Act, the Federal Trade Commission (FTC) in June submitted a report to Congress on the creation of a "Do Not E-mail Registry," similar to the Do Not Call Registry that was enacted last year. The report concluded that without effective ways to authenticate the origin of e-mail addresses, such a registry would not further reduce the volume of spam. The FTC instead proposed widespread adoption of e-mail authentication standards that would help ISPs and law enforcement to more effectively identify spammers.

For complete text of the CAN-SPAM Act, visit http://www.spamlaws.com/federal/108s877.html —*E.S*