Stop Spam Now
Published November 01, 2007

Unwanted e-mail clogs your inbox and hurts your productivity. Isn't it time you fought back? Consider these strategies for preventing, managing and responding to spam.

Photo by: iStockphoto

By: MATT ALDERTON

Unless you're an adult film star, a pharmacist or a professional bodybuilder, chances are that the dozens of e-mails you get every day about penis enlargement, breast augmentation, erectile dysfunction and weight loss medications are unsolicited, unwanted and unwelcome.

More than that, though, they're also unproductive. Spam—which refers not only to canned meat, but also to *any* unwanted e-mail message—accounts for 70 percent of all e-mail traffic, according to the most recent data from IT giant Symantec. And for small business owners in particular, that translates into a lot of time spent reading, filtering and deleting unwanted e-mail.

"Spam is annoying and it takes time," says David Rosenbaum, president and CEO of Real-Time Computer Services, an Ardsley, N.Y.-based computer consultancy. "It's an incredible problem, and it's a problem that's getting worse, not better."

The bad news, according to Rosenbaum, is that spam is here to stay. It's a problem that simply can't be solved. The good news, however, is that even though it can't be eliminated, spam can most certainly be challenged; it can be prevented, responded to and, even at its worst, managed.

The Spam Problem

More than anything else, spam is an economic problem, according to William Kilmer, CEO of Avinti, a Lindon, Utah-based company that specializes in stopping malware and spam. "It is one of the most cost-effective mediums to reach people," he says, "even at very low response rates."

In fact, spam evolved from the junk mail that once inundated brick-and-mortar mailboxes. But while that junk mail was expensive to produce—the sender had to pay not only for lists of addresses, but also for packaging and postage—spam is decidedly un-expensive. Sure, spammers still have to pay for addresses, but they don't have to pay a nickel in order to package or postmark their messages. They just have to hit send.

"Plus, somebody out there is actually responding to some number of these ads, or else there would be no economic incentive for sending them," Rosenbaum says. "People do respond to them, and that's partly why spammers keep sending them."

Adding to the spam situation, Rosenbaum points out, is the fact that the Internet is a global phenomenon. Spammers are located not just in the United States, but in countries across the world. Any effort to regulate or sanction spam must therefore be an international effort in order to be effective. And that, experts say, is a true long shot.

Act Now

A global "do-not-spam" list may be wishful thinking, but that doesn't mean that you have to put up with e-mail upon e-mail of horse tranquilizer ads and debt financing pitches. In fact, you shouldn't. Because when you ignore your spam situation, you give spammers permission to harm your business. Among potential threats:

- Spam hurts productivity, as time spent reading, sorting and deleting unwanted e-mail is time that could have been spent strategizing and producing for your company.
- Spam hurts customer service and sales, as it makes it harder to find and respond to legitimate e-mail messages, often resulting in the mistaken deletion of important correspondence.
- Spam hurts your computer, as it can contain viruses designed to infect and destroy your network.

A final, and increasingly powerful, menace is what Kilmer calls blended threats. "This is spam that includes hyperlinks to Web sites where users are infected with malware," he says. "This type of spam is not the normal sales pitches for hair replacement, male enhancements, fake watches or stocks. It is intended to infect people with malware that is generally used to hijack the computer for later use or to steal personal or corporate information."

Once just irritating, spam is more and more becoming malicious. "The reality is that spam was once just an issue of productivity and resource usage," Kilmer says. "Blended threats have now become a security threat."

Preventing Spam

Perhaps the easiest way to fight spam is to prevent it. After all, sending you e-mail is awfully hard if you've kept your name and e-mail address off of spammers' lists to begin with; they can't spam you if they don't know you exist.

The easiest and most effective way to keep your e-mail address private, and off of spammers' lists, is to keep your e-mail nomenclature under lock and key. Rosenbaum therefore suggests having several e-mail addresses; one that you make public

and another that you use exclusively with trusted senders and personal contacts.

"Small business owners need to pay attention to the availability of employee information outside of the organization," Kilmer adds. "An effective spam prevention policy would including making sure that employees are not freely giving out their company e-mail addresses, whether on Web sites, social networking sites or in other material that becomes publicly available."

Many companies go so far as to not even publish their e-mail addresses on their Web sites; instead, they publish online forms through which consumers can contact them. Of course, this might prove inconvenient and even annoying to potential customers. Companies must therefore make a choice between being conveniently accessible and being spam-free. Which is most important will depend on your industry, your sales pipeline and your target prospects.

Responding to Spam

Eventually—inevitably, even—your e-mail address is bound to make it into the hands of a spammer. In that case, there are several actions you can take in order to keep the spam from snowballing.

Your first response, Rosenbaum insists, should always be no response. "Many of these spam messages have a comment or a link at the bottom that says, 'To unsubscribe from this list, click here,'" he says. "Worst thing you can do."

Why? Because responding to spam—even to unsubscribe from it—confirms to the spammer that he has reached a live person. And while he may in fact remove you from his list, he will likely then sell your name to others, who will have no qualms about putting you on their lists.

Kilmer agrees that in the world of spam, silence is golden. He even advocates disabling e-mail bounces from your e-mail server in order to make your company even quieter. "The company should prevent what are known as dictionary attacks by not bouncing back e-mails to false addresses," he says. "Spammers use this technique, which involves guessing and combining names with an e-mail domain in order to construct a set of live e-mail addresses. They do this by sending e-mails to the varied e-mail addresses and tracking those that aren't 'bounced back' by the e-mail server as being false."

In other words, sending spammers a message that an address is false confirms to them again that another address is real. And in that case: Let the Viagra ads begin.

Managing Spam

When all else fails, and the spam keeps dripping into your inbox like an incessant leaky faucet, it's time to employ solutions that can help manage your insurmountable spam problems, if not eliminate them.

"There's a whole series of things you can do to try to keep the spam from coming in, even if your name is out there," Rosenbaum says. "Nothing's ever going to be perfect, though."

While *perfect* would be nice, *good enough* is great, according to most spam opponents. If you're among them, your best and basic options include:

- **Spam filtering software:** Spam filters, such as SpamAssassin, Spam Arrest and Spamihilator employ a variety of techniques that are designed to separate legitimate from illegitimate e-mail. They're good solutions for keeping your inbox clean, but they rarely get things right all of the time. "You run a trade off between false positives," Rosenbaum says, "which is where a filter has blocked a legitimate message, and false negatives, where it has allowed spam to slip through." If you use a spam filter, therefore, you must remember to constantly filter through your spam folder for important messages.
- **Built-in spam blockers:** Most e-mail services have some level of built-in spam protection, according to Kilmer, which can prove quite effective; you can even train your e-mail program to send messages with certain words in them directly to your spam folder. "Utilizing your e-mail client's junk folder is very helpful," he says. "It will pick up much of what other's products won't."
- **Whitelist software:** Many solutions, such as CA Anti-Spam and Symantec's Norton Internet Security, allow you to gradually build a whitelist of approved e-mail senders in order to train your e-mail client to effectively identify, filter and block spam.
- **Challenge-response systems:** Challenge-response systems work by identifying potential spam and holding it for delivery while the system generates a challenge question for the sender; if the sender correctly answers the challenge question—often by typing a series of randomly-generated letters—his or her e-mail is then delivered to your inbox. "These are very effective," Rosenbaum says, "and a complete pain in the neck."

No matter which anti-spam solution you choose, you'll discover that spam management is a constant balancing act whereby you're working to keep good messages in and bad messages out; businesses that balance well will be happier and more productive while those that balance poorly will be inundated both with spam and complaints from customers who were accidentally blocked.

Concludes Kilmer, "Emphasizing and exercising common sense is key."

Links referenced within this article

Symantec
http://www.symantec.com/enterprise/security_response/weblog/2007/10/the_october_state_of_spam_repo.html
Real-Time Computer Services
http://www.rcsinc.com/
Avinti
http://www.avinti.com/
SpamAssassin
http://spamassassin.apache.org/

Spam Arrest
http://www.spamarrest.com/
Spamihilator
http://www.spamihilator.com/
CA Anti-Spam
http://www.qurb.com/
Norton Internet Security
http://www.symantec.com/norton/products/overview.jsp?pcid=is&pvid=nis2008

Find this article at:
http://pronet.nielsen.com/smallbusiness/content_display/technology/e3iff716996ae2a7e214e2ba40182fe5d89

Click to Print

SAVE THIS | EMAIL THIS | Close

Uncheck the box to remove the list of links referenced in the article.