Date: Mon, 16 Jun 2003
From: James Lamb jamesl@lakeave.org
Subject: Re: Looking for a good email blocker

Spam is an incredibly difficult thing to fight, and it will take a combination of things to make a dent, and even then, you will not get it all.

But I feel like I should summarize the information already posted, and include a little more of my own.

First, how do they get your address?

- One, you put it on your website so people can contact you. But the spammers have programs that scour the web looking for email addresses.
- Second, you post in forums like these, or sign-up for access to other places which then turn around and sell your email address.
- Third, you could have a virus on your computer (or someone who knows your address has a virus on their computer) that reports the addresses back to a third-party.
- Fourth, a dictionary hack. A spammer tries to send to all kinds of logical combinations of words and names at a domain, noting which ones don't result in error messages. (a@shelbyinc.com, b@shelbyinc.com, etc., etc.)

How do you avoid spam?

While you can't completely avoid spam, there are ways to try keep it at bay.

At your ISP level - if your ISP isn't using something like

- Brightmail (AOL, MSN, Earthlink all use it), then that's why a lot of spam is coming in.
- Many ISPs also now scan mail for viruses. Ask your ISP what they are doing to help cut down on spam, or if there are any optional services available.

At your server level - if you're running your own mail server, buy

- virus and
- spam filters from a large company that regularly updates them.

At your workstation level -

- if you're using Outlook, SpamNet (www.cloudmark.com) is a really neat and useful tool. I'm noticing it's no longer free. Bummer.
- Also, the preview pane should be turned off. The preview pane -- a wonderfully useful tool -- sadly is a great way to let viruses in, or let your email address out (a spammer can send you an email with a graphic in it and when the preview pane requests that graphic, the spammer knows that you opened the email and therefore are a live email address.)
- Additionally, every computer should have virus software.
- You can also set rules/filters to put every email that is sent that does not include your email address in the To: or CC: into a separate "probably spam" folder for later review. Typically all legitimate email comes to you when you're the To: or CC: (I recommend forwarding a copy separately to someone instead of BCC'ing them.)

At your employee level -

- discourage the forwarding of jokes and attachments
- Educate them to NEVER, NEVER, NEVER follow the "unsubscribe" directions at the bottom of a piece of spam. They will unsubscribe you, but since this is proof that the email address is valid, they will often sell your email address to 3-5 other spammers

At the website level -

- Sometimes, it takes drastic measures. Instead of listing email addresses, maybe a form that's linked to a person's name, so the email address is never revealed until the staff member writes back.
- At Lake, everything's always been very open and it wasn't an option to not show email addresses. So I've had to modify the program that displays the pages so that a small graphical-dot is displayed instead of a period. So the spammers scouring our site will find jamesl@lakeaveorg and keep going because that's not a legitimate address. But to a person looking at it, the dot between ave and org is obvious. (And if you click on an email address, it does go into the form.)

At the organizational level -

- Avoid really obvious email addresses like "webmaster@" and "postmaster@". Sadly, it's come to this. My wife had alillamb@someisp.com and got all kinds of spam. alillamb03@sameisp.com gets almost no spam. I've had an address for years that is my first name, my year of graduation and the abbreviation of the school I graduated from, on the notoriously spam-bad hotmail and gotten no spam.
- Our director of IT has decreed as a policy that we will never have Outlook/Exchange here because of all the viruses written for Outlook. As a result, our spam is less, and viruses are almost non-existent. Those of us that come from other jobs where they used Outlook grumble at first but then after a few months realize how nice it is not to have an entire division of your own company spamming you because they all passed around some dumb joke attachment. So we use Groupwise. It's not Outlook, but it's improving.

Lastly, friendly-spam... that's the worst... person A gets a virus. person A has person B and person C in his address book. The virus randomly goes through person A's address book, selects person B and forges their name and address as the sender and sends the spam/virus to person C. It will really take some detective work to figure out who is really infected, but by exploring the headers (usually hidden by mail programs until you look at the properties of an email) you can usually determine who's infected and contact them. At one company we had such a problem with people adding our email address to their address books and then getting infected themselves that we had to end up changing our email address every six months or so. Inconvenient for them, but the only way we could keep from drowning under all the spam.