

CNS eZine: Stop the Annoying Spam (Revised March 2005)

SPAM: Annoying unsolicited email that comes from most anywhere

If your inbox is filling up with messages from strange addresses, wanting to sell you online prescriptions, Viagra, pornography, Russian brides, or other unmentionable solicitation, you're not alone. On any given day, I receive about a hundred emails, and maybe twenty are legitimate.

Email solicitors get your address in a several ways. First, some solicitors generate hundreds of thousands of addresses using computer-generated routines. Next, if your address is listed on a website, marketers "spider" websites and pick up email addresses, and lastly, online marketers sell lists amongst each other for a fee. The next time you enter your email address on a website, think of how many times it can be sold. Considering the fact that even banks sell your personal financial information amongst their own subsidiaries, this is a rather common practice. Even if you get a legitimate "Opt-Out" link, the Spammer has 10 days to sell your address (CANSPAM Act) before removing you from the original list. Most of the Opt-Out links I receive don't work, so just delete the message.

How can you take a dent out of the volume? MSN and AOL users can get some of the garbage thrown out by their online spam filters. Investigate the spam filtering options with your ISP. If you're like me, I use Outlook, and my email client pulls all of my mail from my mail server and drops it in my inbox. For Outlook users (or Eudora or most any other email client), you can setup inbox rules. To do this, simply make a list of all the junk you want eliminated, by keyword. Be sure to include intentional miss-spellings of these words since spammers are wise to this procedure. For instance, Viagra has been intentionally miss-spelled as "iagra" so include some miss-spellings as well. This is something you'll want to adjust (and add more spellings) periodically, since you likely get the same message with the same miss spelling from several different sources.

How do I set up filtering? Setting this up in Outlook requires only a couple of minutes. First, create a new folder in Outlook named Possible SPAM. Next, on the main screen, choose TOOLS, MESSAGE RULES, and then MAIL. Click on NEW, click on "Where the subject line contains specific words" and "Where the message body contains specific words". Next, go to box three and create your rules for both, adding all those keywords you've assembled to both the subject line and body text areas. Lastly, click on "Copy it to the specified folder" and enter the new folder you just created, "Possible SPAM". The next time that Outlook polls for new mail, it will use the new rule and place any mail that matches your new criteria into the Possible SPAM folder. Check this folder often, to ensure that none of your normal mail will end up here. You can easily modify your settings for the mail filter to meet your needs. Once you're satisfied that absolutely none of the mail that ends up in the Possible SPAM folder is anything but SPAM, change the "Copy it to the specified folder" to "Delete it". You can still view the SPAM in the Deleted Items folder until you close Outlook.

What about the rest? Up until mid-2004, simple filtering techniques were effective in eliminating the bulk of spam. Because there are some creative programmers at spam outfits, the vast majority has reformatted their mail to HTML format. If you see an “image” of words in your email, rather than the true text itself, simple word-based filtering is inadequate. As of March 2005, I’d estimate we’re seeing about 90% of spam delivered in HTML to avoid the simple filters. The most effective means we’ve found, short of just “dealing with it” for the non-enterprise user, is to upgrade anti-virus software to “Internet Security” software. Vendors have taken note to the rising risks of spam, Active-X scripting, worms, and Trojans, and have incorporated very sophisticated methods of screening and detection. Our favorite (since we test the top 10 vendors each quarter) is Panda Internet Security. Since we regularly retrieve data from infected computers to our field laptops for customer data restoral, we’ve found that Panda’s product keeps our systems clean, both considering email-delivered threats as well as internet-based infections. Further, since it updates itself daily, we stay up to date. More information about Panda can be found on our website, PC Security page, at www.CompetitiveNetworkSolutions.com

What about opt-out links? That’s a double-edged question! Our experience is that most opt-out links simply verify that the spammer has reached a valid email address, and until legislation later this year puts some teeth into the CANSPAM act, simply delete the message or filter by sender or content.

Spammers are Creative!

Fake Sender: A good percentage of the Spam we receive appears to be from legitimate senders, but beware! Microsoft doesn’t send attached files via email to update your operating system, yet I’ve received several emails that “look” like it came from Microsoft. By analyzing the message header information, its clear that the sender is not anyone@microsoft.com.

Anonymous Sender: A small percentage of Spam comes from an “unknown” sender and typically has no subject line. Delete these as well.

Foreign email: If you don’t have any reason to communicate via email with someone outside of the US, add keyword filters in your email client to get rid of email when the domain (the address to the right of @) [contains '.de' or '.it' or '.ru' or '.au'](#)

The CANSPAM act only covers email solicitation originating from US companies, so its still fair game for the overseas users to act as “Spam Agents” on behalf of someone else.

What Causes SPAM? Spammers are no more than electronic mail telemarketers or virus and worm distributors. Since email is basically a free medium, SPAM Marketers can bombard millions of addresses per day from a single computer, rather than staffing a call center to call long distance. Virus and Worm distributors (please see our PC Security advice on www.competitivenetworksolutions.com) are spreading malicious code through other computers to hide their identity and origination.

Costs: For the enterprise user, some 10% of an IT Professional's time is spent dealing with SPAM. While the best filtering, virus protection, and user caution may be made, there comes a point where the security net is too high, and you'll begin blocking email that you want, so its not a perfect science yet. Further, a reported 25-30% of an email server's processing capability is being *stolen* by having to process, relay, or filter unwanted SPAM. This fact alone can cost the business user a considerable investment.

Best Practices: For the average user, maintain current virus protection software (and signature files), filter your inbox by as many known spellings of *words that you know you don't want*, and be prepared to actively manage your inbox. If it gets too crazy, consider changing your address.

David Parker is a 20-year veteran of the Technical Sector, and has managed Competitive Network Solutions, Inc. providing services as "Your Chief Technology Officer on Call" for over three years. He was recently featured on WMC Action News 5 as the "Computer Expert" speaking about the recent *My Doom* outbreak, and detection and prevention techniques. © 2005, Competitive Network Solutions, Inc.