

# **SPAM Revisited... Can It Be Canned?**

By Mike Dooley, Systems Administrator, NSDCAR  
February, 2004

When last I wrote of the infamous “spam” email issue, I held forth on all the effective methods you can use to avoid the nuisance of UCE, or Unsolicited Commercial Email. Since then, the government has come up with the “CAN-SPAM” initiative, which is proving to have little efficacy in stemming the tide of junk electronic mail. Since most UCE originates offshore, in nations that either do not cooperate with U.S. policy, or are outright hostile to the United States, enacting legislation to control the problem is just about as effective as mentioning the Emperor’s New Clothes. Spam just ain’t gonna stay in the can, now, is it?

With the advent of the latest crop of “worm” viruses, which carry their own email sending programs and can read your entire address book in a trice, mailing themselves to every contact, the game’s a little different these days. So different, in fact, that you no longer have to worry about email as the major source of infection... just visiting a website can leave your computer with several nasty little programs running on it that disrupt your ability to perform your daily tasks, and can even use your PC as a “server” to create and distribute more copies of the bug. As an example, the dreaded “MyMail” worm, now scouring the Internet in three or four different versions, is generating unprecedented amounts of traffic on computer networks the world over, and here’s why.

The worm embeds itself in your computer, reads any address books you’ve got stored, and begins mailing copies of itself to every address. On the receiving end, an antivirus program or email gateway stops the nasty little bug, and then dutifully sends you a non-delivery report, telling you why your email did not go through. Now, think about how many other people have YOUR email address in their address book. A virus-infected email is being sent in your name, as the MyMail worm fakes the “From:” address and inserts your name instead. Every recipient of that particular message now sends you another non-delivery notice, stating that the mail you sent was infected, or the attachment was blocked. Ad infinitum, the thing propagates all over the World Wide Web. Millions and millions of copies, responses, and notices are sent back and forth, with no human intervention whatsoever. Mail servers are grinding away, processing all the junk, and the Internet slows to a crawl with all the traffic.

It’s a new day out there, and preventing what was once a nuisance is now becoming a priority for computer administrators everywhere. It’s also a new day for every computer owner and user, and looming on the horizon is the possibility that those who ignore the need for antivirus software, or who continue to operate infected computers on the public network may face sanctions at best, and prosecution at worst.

How is your computer’s security measuring up? Do you employ an anti-virus program? Do you keep it regularly updated, via an automated process? Is your email account on a web-based server, like Yahoo or MSN? If not, are you running spam filters and anti-virus against your Inbox? If you don’t know what any of this means, are you consulting a qualified professional to take care of it for you?

We all know that practicing real estate is very different from living the lifestyle of a REALTOR®. Why would you expect that Cousin George, who’s “real good with computers”, can adequately address securing your home or office network? Consult an expert, educate yourself about market prices for such services, and enjoy the peace of mind of having periodic “tune-ups” of your information infrastructure. If your computer generates dollars for you, it makes good sense to give it the same degree of attention and maintenance that you would your automobile. Yet many still ignore everything about their PC until something goes drastically wrong.

It is worth mentioning that if American business on the Internet does not police itself, and take care of these issues with the best technologies available, then government will step in, and attempt to legislate a cure for it. Take responsibility for the security and health of your computing environment, and if you’re not up to the task, employ an expert. It could be the best business ‘partnership’ you’ve ever had!