Recipients Not the Only Victims of Spammers:
Some Senders Have Been Ripped Off

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

All of us get unsolicited commercial e-mail – spam – and often curse the senders, right? Sometimes the senders of spam get their comeuppance through retaliation from their victims. One notorious case of immediate, disastrous retaliation against a USENET spammer was described in a December 1994 article in *Network World* which I summarized in a column back in 1991<http://www.networkworld.com/newsletters/sec/2001/00408507.html>. The twit who inadvertently posted the same message on multiple USENET groups advertising his company’s products got a flood of abusive e-mail, but much worse was that someone posted the company’s 800 number on an alt.sex group as if it were a free phone-sex line.

However, today I want to remind readers that retaliating against the people named in spam is not necessarily a good idea. Sometimes these folks are actually the victims of spammers even more than we recipients are.

Have you ever received spam for completely inappropriate technology? I’m sure you have. As a university professor in a computer science department in Vermont, I’ve been surprised by wildly inappropriate advertising sent through spam. Here are some recent samples:

- Offers of Chinese 20-metre industrial concrete waste-water pipes weighing three tons each;
- Wonderful hair-cutting facilities in Arizona;
- Real-estate opportunities in upstate New York;
- Automobile repair service in Nevada;
- All the colors of the rainbow in cotton-synthetic cloth mixtures suitable for manufacturing clothing of any type;
- Starting a specialty coffee business.

The senders of these (sometimes intercontinental) misguided missives are actually the victims of criminals who have lied to them. The victims are naïve, unsophisticated business people – sometimes hardworking owners of small US businesses, sometimes bewildered managers of Chinese factories – who have accepted wonderful offers of cheap marketing via e-mail to enormous numbers of willing participants eager to hear from them and carefully filtered to maximize their rate of return on their investment.

Yeah, right.

One of the cardinal signs that a spam message is actually from a victim of this kind of flim-spam operation is that the poor schmucks put all their information down accurately in the message. Normal (that is to say, scum-sucking disgusting criminal sociopathic dirtbag) spammers usually choose misspellings of key words to avoid spam filters and include Web links for supposed further information or as part of their phishing technique. Business-exploitation spammers don’t care about avoiding spam filters: they’ve already made their profit by tricking their victims into
paying for the useless e-mail flood right up front.

So instead of writing foul obscenities to the people named in this kind of spam, why not try another tack? I write to the victims nicely with a canned letter (you can store macros in a variety of ways these days) explaining how they have been tricked by liars who told them a bunch of hooey about opt-in, willing recipients of carefully chosen recipients – and are actually just using any old list they can find or buy because it doesn’t matter to them how mad the recipients become. I also explain that the sender’s e-mail address has now been added to countless e-mail blacklists and that they may experience increased difficulty in reaching real customers. Finally, I suggest that the victims sue the criminals who stole their money and recover their cash.

Another benefit of communicating nicely with the victims is that we can get the word out to the wider society so that ultimately, fewer small businesses will be tricked by the spammers into falling for their scams.

Maybe with these multiple attack methods we’ll eventually see some reduction in at least one kind of spam.

* * *


Copyright © 2010 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.