Too Quick on the Trigger: Responding to Spam Alerts

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

If I have a minute to spare, I sometimes respond to unsolicited commercial e-mail (“spam”) by checking the header for forgery (see “On the case with Spam Spade, <http://www.nwfusion.com/newsletters/sec/2001/00319486.html>). If I can trace the real origin of the junk e-mail, I send the originating ISPs a note requesting that they look into the possible violation of their policies. Naturally, I never use the opt-out e-mail addresses or Web URLs because I don’t like the risk of having my e-mail address re-sold to other spammers as a good address.

A few days ago I received a junk e-mail message with the subject “(1etrades.com)I have an endless number........We are part of the same group........about search optimization.” The message was a bizarre piece of semi-English prose with largely incomprehensible gibberish that was apparently selling something; it ended with this text (Website names blocked out to protect the guilty):

“If you criticize me for being what I am then there is nothing I can say, nor do I care to defend myself so to remove:
mailto:remove@someaddress.net
REMOVAL PAGE remove@anotheraddress.net
To unsubscribe: http://www.yetanotheraddress.com/rem/
Under US EU LAW”

Having looked up the DNS registry entries for the three addresses listed, I sent a single message to all three requesting that they look into the situation and terminate services to offenders. Normally, I get either no response or a polite form letters thanking me for informing them of the situation and stating that they will look into the situation. Sometimes I have received a message stating that the offending account was investigated, found to be spamming, and therefore shut down.

Well, my message didn’t go over too well with one of the system administrators to whom I wrote. He sent the following message to a list of administrators for systems where I had once had e-mail addresses:

“Dear <bunch of people>
can you shut down Mich Kabay,
He is spamming myself because a customer has sent him an email.
If you do not stop 'Mich Kabay <mkabay@compuserve.com>'
I will make a further complain.

Uper and Mich Kabay are member of the same group then the Uper email had removal option.
3 opt in no one removal!
Two of the admins were at companies where I used to work. One of those admins wrote the following response to the sender:

“Mich Kabay no longer has an address on our <former employer’s> Mail server, and I have blocked all mail from mkabay@compuserve.com.”

Based on an unsupported claim from a person who received a single message from me requesting professional assistance, the administrator of a company has cheerfully prevented me from communicating by e-mail with all my former colleagues.

I left a voice mail message for the admin respectfully requesting that he rescind the ban on my e-mail, but this incident supports my belief that we must not act precipitously when someone makes an accusation of spam. Before shutting down _inbound_ e-mail from an e-mail address, I urge admins to communicate with the target of the accusation to see if there is another side to the story they have been fed. A similar principle argues against retaliating against the apparent origin of penetration attempts or denial-of-service (DoS) attacks: one may be retaliating against the wrong people.

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2002 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.