I was struck recently by the kind of blooper that Peter G. Neumann's RISKS Forum has been highlighting for decades: automated responses based on faulty assumptions.

One of the themes illustrating the dangers of stupidly-defined rules blindly applied is anti-spam measures based on absurdly clumsy methods of identifying unsolicited commercial e-mail. Many correspondents have reported on simple-minded filters that block e-mail based on, say, the presence of particular alphanumeric sequences. Such discussions usually have to dance circles around the actual target strings for fear that the anti-spam measures will block the issue of RISKS. For the same reason, I dare not write the sequence consisting of three instances of the third-to-last letter of the English alphabet (you know, the one between W and Y) because so many filters identify any text containing that particular sequence as if they are inevitably pornographic messages.

Another example of a stupid rule instantiated into code is from a version of MS-Outlook, where at one point a few years ago, Bruce Sterling pointed out that the presence of the string "begin" followed by two spaces at the start of a line in an e-mail message was interpreted as the start of MIME-encoded text. All the rest of the message was therefore converted to an attachment. Microsoft's proposed workaround was to use some other word than "begin" in one's text: they suggested "start" or "commence."

About a week before writing this column, my CompuServe e-mail account was blocked because the password was changed. I called technical support; they informed me that my account had been flagged as being involved in spam. Tech support could do nothing further to help me, they said; only the Community Action Center could do so. The Action Center's logs showed that my account had been frozen because I sent an announcement about an upcoming security lecture in our university's monthly series to 70 recipients (all students) and then immediately sent another (actually the same) message to about 40 faculty members. It seems that CompuServe has very strict rules which automatically freeze any account that is identified as sending spam.

When I asked what the rules were so that I could avoid any further difficulties, I was categorically told that it is impossible to give the rules. The rules involve a combination of message size, number of recipients, and interval between messages with more than an indeterminate number of recipients.

I spent a while looking for any information about these (now practically mythical) rules in the Terms of Service and Spam sections of CompuServe, but I have found nothing whatsoever to help me avoid future shutdowns.

The specific example is not particularly important. The significant problem is the blind, Philistine pig-ignorance (to quote Monty Python's slaughterhouse architect) that presupposes an absolute identity between e-mail with lots of recipients and e-mail that qualifies as spam. If one of my programming students designed a system with this degree of stupidity I'd assign a zero for
the design.

Remind your programmers to test their assumptions before they engage in automated denial of service to paying customers.

As for me, after 17 years with CompuServe, I’ve switched to a different ISP with clearer rules.

* * *

For further reading:

Risks Forum archives <http://catless.ncl.ac.uk/Risks/>


* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www.norwich.edu/msia> for full details.


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@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

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.