A reader who wishes to remain anonymous wrote to me as follows about yet another example of the thoroughgoing sleaziness of spammers. I have removed specific names because I don’t know how trustworthy the report is and I’m not keen on getting sued; I also removed the profanity.

* * *

I recently began receiving unwanted messages from a site totally devoid of interest for me. I tried to get them off the Internet in my usual way by seeing if I could find a legitimate Web hosting service or ISP Internet service provider that was providing services to them to boot them off, but I failed. So I did something I very rarely do and that I discourage people from doing: I used the spammers’ remove instruction.

As expected, it was not a pleasant experience. The spammer’s Web site has a contract with a company that makes a product to stop pop-up ads; that company advertises by putting pop-up ads on the visitor’s screen and then commiserating with the victim about how awful pop-up ads are! Naturally, I turned off pop-up ads at my firewall; no effect. I had to disable Java and JavaScript in my browser to get this [singular bad word] off my screen. Can you believe these [plural bad word]??

There was no effect of the supposed deletion. I continued receiving spam from these [plural bad word] in the days that followed by request for termination of this junk.

I went back to the site hoping to find something else I could do; at that point, I noticed that the URL for removal included a numerical ID number; curious, I changed the last digit by one to see what would happen. I discovered that the new URL promptly showed a screen claiming that the system had deleted someone else’s e-mail address – and it was someone from my own university!

Further investigation of their database showed that the e-mail addresses that were from my school were all faculty members. There were many other users from the “.edu” domain in the list of addresses. My guess is that these [plural bad word] have stolen the addresses of faculty members from a wide range of university Web sites.

Do you have any suggestions on what we can do to stop these creeps from stealing our e-mail addresses from Web directories?

* * *

Alas, no, I cannot think of any foolproof method of stopping unscrupulous people from using faculty (or any other) e-mail lists that are posted on public WWW pages. The only thing I can think of is retaliatory. Before I go any further, it’s important that I state clearly that I am not an attorney and this is not legal advice. For legal advice, consult an attorney with expertise in this
area of practice and who is licensed to practice law in your jurisdiction. The following comments are simply suggestions based on my understanding of the situation.

First, you have to state that your e-mail lists are copyright by your university and that all rights are reserved. Discuss the following text with your university attorney as a beginning (it’s based on VeriSign’s warning in its Domain Name Service listing when you do a WHOIS to find the owner of a particular domain):

“The data in the Particular University Faculty E-mail Listing are provided by Particular University for information purposes only, and to assist persons in obtaining information about or related to Particular faculty. Particular University does not guarantee the accuracy or completeness of this list. By using this Web page, you agree to use these data only for lawful purposes and that under no circumstances will you use these data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to Particular University (or its computer systems). The compilation, repackaging, dissemination or other use of these data is expressly prohibited without the prior written consent of Particular University. Particular University reserves the right to terminate your access to the Faculty E-mail Listing or any other portion of its Web site in its sole discretion, including without limitation, for excessive querying of the Web site or for failure to otherwise abide by this policy. Particular University reserves the right to modify these terms at any time. By using this Web site, you agree to abide by this policy.”

Now, anyone unscrupulous enough to add people to a junk e-mail list without asking is unlikely to pay any attention to such a warning or even to see it; harvesting e-mail addresses is usually automated. Nonetheless, there’s possibly relevant lawsuit that reached the California State Supreme Court in March 2002. An angry employee of Intel sent 30,000 (non-commercial) e-mail messages with his opinion to Intel employees using their company e-mail addresses. Lower courts have ruled that he abused the property of Intel; the American Civil Liberties Union and the Electronic Frontier Foundation are backing the employee’s defense that he was entitled to express his opinion (see http://www.siliconvalley.com/mld/siliconvalley/2948781.htm ). If this case goes against the respondent (employee), it might provide precedent for suing the spammer who abuses University e-mail addresses.

So in other words, maybe we can sue the [plural bad word].

* * *

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@compuserve.com>; 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.