Privacy Journal
AN INDEPENDENT MONTHLY ON PRIVACY IN A COMPUTER AGE
PO Box 28577
Providence RI 02908

December 1997, Vol. 24, No. 2

How to Diminish (but Not Eliminate) Electronic-Mail 'Spam'

By Simson L. Garfinkel

In one of the first court cases involving unsolicited mail sent over the Internet, a court in Texas has ordered a college student to pay nearly $19,000 in damages and attorneys fees for using a fraudulent return address in his electronic messages.

The defendants in the case, Craig Nowak and Nowak's company, C.N. Enterprises, earlier this year had sent out thousands - and possibly millions - of e-mail, advertising a list of "free cash grants" for college students. All of the information on Nowak's list was freely available through other sources.

Although the practice of sending out bulk e-mail, a process commonly called "spamming," is not illegal per se, Nowak tried to mask his identity by using the return address "@flowers.com" for each e-mail message. "The software program we used said you could just use any random name" for a return address, Nowak told *Wired News* in May. "I don't know why I picked 'Flowers.'" By picking "@flowers.com," Nowak assured that the messages that could not be delivered would be sent to Tracy LaQuey Parker, an Internet author and the owner of the domain flowers.com. Parker received thousands of bounced messages, crashing his computer. He also received numerous threats and angry messages by outraged Internet users, who thought that he had sent the original message. So he sued. The court ruled that Nowak, who operates out of San Diego, had no right to use the domain flowers.com and that he had caused Parker actual damages, including lost time, lost income, lost business opportunities, and lost use of his computers. The court awarded $13,910 in actual damage and $5,000 in attorney's fees. *Parker v. C.N. Enterprises and Nowak*, 97-06273 (Dis. Ct., Travis Co. Tex., Nov. 20).

Meanwhile, America Online has been conducting its own legal action against spammers. On Oct. 31, the company won a preliminary injunction against Over The Air Equipment, a Las Vegas sex merchant. AOL claimed that the company had fraudulently sent millions of ads for "cyber-strippers" to AOL members.

Several anti-spam bills have been introduced in state legislatures and in Congress. One, S. 771, the Unsolicited Commercial Email Choice Act of 1997 introduced by Sen. Frank Murkowski, R-Alas., would require that all unsolicited messages carry the header "Advertisement" and that Internet service providers equip their computers to filter out these advertisements on a subscriber-by-subscriber basis. Some spammers have backed the bill because the law would legitimize their craft. In Canada, the Canadian Direct Marketing Association has guidelines against spamming unless the individual gives permis-

In This Issue

ISSN 0145-7659

sion (available from CDMA 416/391-2362, ext, 226, fax 416/441-4062, World Wide Web *www.cdma.org).* While legal action and legislation may sound promising to some, it is still the exception on the Internet today. Rather than turning to the courts or lawmakers, most Internet service providers are developing technical solutions to shield their users from unwanted e-mail.

One technique, also pioneered by AOL but adopted by competitors, allows users to select the names of domains that they wish not to receive mail from. For example, some unwanted e-mail comes with a return address in the "@savetrees.com" domain. By blocking mail with this return address, the user will not receive those messages. Rather than forcing users to chose each domain that they wish to block, America Online maintains an extensive list of domains that have been associated with spam mail and allows a user to block them all with a single mouse click.

Another technique is to block Internet connectivity from known spammers. This technique relies on the fact that some spammers have their own high-speed connections to the Internet. By subscribing to a list of these sites, an Internet service provider can arrange for messages originating at these sites to be automatically blocked at the source. One of the most effective modes of blocking systems is the Realtime Blackhole List, created by Internet pioneer Paul Vixie. The system arranges for messages from spammers to be automatically routed to a "blackhole" from which they cannot escape.

Still another way to shield users from unwanted e-mail is to examine the From: addresses to determine whether or not they are valid e-mail addresses. For example, some spam comes from the address E270no018 @GreatNetProgram.com, even though there is no domain GreatNetProgram.com on the Internet. This type of e-mail can be automatically blocked. But automatic blocking is not without its own problems: occasionally these programs cast too wide a net and block legitimate electronic mail as well. As with most things involving a computer, the devil is in the details. (Details on anti-spamming technical solutions can be found at *http://spam.abuse.net/.* Details of the Nowak lawsuit can be found at *http://www.zilker.net/nospam/.* Details of S. 771 can be found at *http://www.senate.gov/~murkowski/commercialemail/.*)

Although some spammers send out their e-mail directly, most use computers belonging to innocent third parties to do their bidding.

Last January a spammer in New Hampshire sent roughly a thousand e-mail messages to Vineyard.NET, an Internet Service Provider on Martha's Vineyard, Mass., of which I am a part-owner. Each message had approximately 66 recipients listed in the TO: address. Thus, the 1000 e-mails resulted in roughly 66,000 messages being delivered to other Internet users. By sending his e-mail messages through Vineyard.NET, the spammer shielded his identity, implicated us in his schemes - and used our Internet connection to do his bidding.

Vineyard.NET is not the only Internet user that has had its computer hijacked by a spammer. Universities, businesses, and other ISPs have all had their resources used to send out spam mail by people other than legitimate users. Unfortunately, the standard software run on most UNIX and Windows NT computers lends itself to this sort of abuse. The only way to prevent hijacking by outsiders is to install special software that prevents "redirection" of e-mail from one outside address to another.

The good news is that technical solutions work. By installing all of the software mentioned above, Vineyard.NET was able to cut the amount of spam mail reaching its customers by 95 per cent. The bad news is that the spammers are aware of these technical fixes and are working hard to get around them. That's why, ultimately, the courts and legislation may be the only ways successfully to fight the problem of unsolicited commercial e-mail.

QUOTABLE

"There was a time when you could control where the visuals went, and now there is no control. A lot of actors will think twice in the future about doing nudity because their image isn't just downloaded, it's also manipulated."

Marvin Jones, author of *Male Nudity in the Movies,* quoted in *Chicago Sun-Times,* Oct. 19, 1997.