Spam Wars

By William Powell

There's a war being waged. It's a battle for your in-box, a battle against spam, and it's being fought by people just like you. Well, almost.

An increasing number of computer users are taking it upon themselves to rid the world of spam—or at least keep it in check. They subscribe to services such as SpamCop and Brightmail, use email filters such as those offered at SPEWS.org, or fight for tougher legislation with lobbying groups such as CAUCE. They're fighting against the tide.

Gartner Research estimates that spam accounts for half of all corporate email. Surprising, isn't it? Spam filters keep much of it from reaching your in-box, but what slips through creates an increasing drain on productivity. Ferris Research estimates that drain will cost corporations US$10 billion in 2003. Brightmail reports that nearly 40 percent of all email is spam. That figure is up 32 percent from late 2001.

Some people actually buy the products that spam advertises. Estimates for follow-ups run 0.1 to 1 percent. That may sound insignificant, but consider that eMarketer estimates that 76 billion messages are sent out annually through legitimate opt-in email marketing campaigns and that, all told, 2.3 billion spam messages are sent daily. Even at a 0.1 percent return, the dollars start adding up. Jupiter Media Metrix expects expenditures on legitimate email marketing alone to reach US$9.4 billion by 2006.

So, there's plenty of money to be made through spam, but that still doesn't answer the question of how spammers are surviving by pushing questionable or even nonexistent products. In a recent *Wired* news investigation, it's estimated that spam advertises an actual product only 10 to 20 percent of the time. No product should mean no revenue, right? Wrong. Spammers are making money, but not how you'd think. To a spammer, your email address alone is worth plenty.

Many spammers are interested only in mining lists of active email addresses with specialized bots (computer programs) that scan the Web, harvesting email addresses, credit card numbers, and any other kind of information that they can dig out in the process. That information is then sold to other spammers, unscrupulous marketers, and unwitting individuals trying to make an easy buck while "working from the comfort of their own home." The running price for 10 million email addresses is $100. There's no shortage of buyers. Directory harvesting, the latest form of email address collection, targets company email servers and can generate a wave of spam in just a few hours.

Though many spamming operations fail, there are those that thrive. Visit ◁⑴ http://ares.penguinhosting.net/~leftreveggplant for pictures of the house that spam built. It belongs to one of the world's largest known spammers, Alan Ralsky. The house is equipped to send up to 1 billion emails per hour; Ralsky routes his email through foreign ISPs.

On Usenet groups such as ◁⑴ news.admin.net-abuse.email, spammers are the enemy. Anti-spammers uncover spammers, report them, and blacklist them. In kind, spammers frequently strike back. The National Organization of Internet Commerce, an organization sympathetic to spammers, once threatened to post the email addresses of millions of AOL members in retaliation to AOL's anti-spamming policy.

It's a battle of the white hats versus black hats, as spam fighters refer to it. Unfortunately, it's not playing out like a

Nearly **40 percent** of all email is spam— up **32 percent** from late 2001.

Hollywood Western. There are plenty of gray hats entering the fray. Internet service providers tweak spamming policies to appease advertisers accused of spamming, small-business owners with a legitimate product buy into a way to "market your product to millions for just $99," and a host of email newsletters and mailings are sent by businesses that provide no way for the recipient to opt out. The line blurs because no one has drawn a clear line in the sand. There's still no national legislation banning spam.

One new area where the line between good guys and bad guys is blur-

ring, to the alarm of anti-spam advocates, is with the proliferation of companies, many claiming to be not-for-profit, that offer to remove you from lists for a monthly or annual fee. Even if they're well intentioned, you're just throwing your money away, says Scott Hazen Mueller, chairman and founder of the Coalition Against Unsolicited Commercial Email and editor-in-chief of *spam.abuse.net.* "Only the spammer can remove you from the list. You have no way to induce him [or her] to do so except, ideally, to report him for spamming. That may induce him to 'listwash' you—remove you," he says.

Spam Busting

Even if you aren't ready to join the ranks of spam fighters, here are a few things that you can do.

● Learn how to read an email's full message header, so that you can properly address a complaint to the spammer's Internet service provider. For a comprehensive how-to on reading a header ◁ www.stopspam.org/email/headers/headers.html.

● Never reply to spam. That doesn't work and can make things worse. The email address listed in the "From:" field is rarely the spammer's and typically belongs to a hapless email user.

〉 〉 〉 〉

Additionally, never click on a link to be removed from a mailing list. That's where spammers get you. Game over. You're on the list as a working email account.

● Create an email account dedicated to friends and family. Create another account to use when signing up for legitimate services. If you're unsure about giving an email address on a form that requires one, fake it or set up a junk account with an Internet-based email provider.

● Organize your email at work by sorting messages into folders or by Outlook's option to organize messages by color. By assigning messages from your co-workers a given color, you'll be less likely to discard them while deleting spam.

William Powell *is an associate editor of* T+D; *wpowell@astd.com.*

The Web *covers Internet technology trends, news, and tips. Send comments, questions, and items of interest to theweb@astd.org.*

The Language of Spam

Spam is creating a subculture of colorful characters and a language all its own. Learn the lingo before someone pens a bad screenplay and turns spam fighting into a Hollywood blockbuster. Here's a sample:

Joe To "joe" someone is to forge email messages or Usenet postings so as to make another person or domain appear responsible for it. Usually done in order to harass the person or domain being "joed." Named for joes.com, an ISP which was damaged as a result of being joed.

LART Loser attitude readjustment tool. Often used as a verb to mean any punitive action taken against a net abuser.

Lumber Cartel Apocryphal organization, which some junk emailers claim are paying those who oppose spam. According to the spammers, the lumber companies fear a loss in profits as a result of people using junk email rather than paper junk mail.

Munging The falsification of one's own email address on a Usenet posting in such a way that a human can figure out what the real address is, but a program cannot. This is done to evade email address harvesting programs used by spammers to target their junk email.

Rogue An ISP that permits net abuse by its customers, or which itself engages in such activities.

Source/Definitions provided by Andrew Nellis's "Net Abuse Jargon File" www.ncf.carleton.ca/ip/freenet/subs/ complaints/spam/jargon.txt

Spam Links

This is a short list of dozens of Websites devoted to the war on spam.

● SpamFaq.net **www.spamfaq.net**

● Spam.abuse.net **http://spam.abuse.net**

● CAUCE: The Coalition Against Unsolicited Commercial Email **www.cauce.org**

● Spam Haus Project **www.spamhaus.org**

● Spam Cop **http://spamcop.net**

● SPEWS.org **www.spews.org**