ROB KOLSTAD

motd

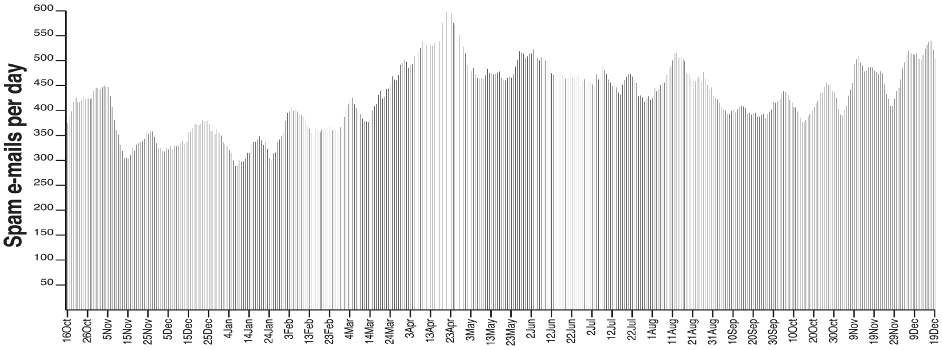
THE ONLY GOOD SPAM COMES FROM HORMEL

Dr. Rob Kolstad has long served as editor of *;login:*. He is SAGE's Executive Director, and also head coach of the USENIX-sponsored USA Computing Olympiad.

kolstad@sage.org

Let's review some of the latest news about spam.

- Message security firm MX Logic reported that November compliance with the USA's CAN-SPAM act hit 6%, doubling October's 3% compliance rate. They add that 69% of spam is sent through "zombies," usually home computers controlled by spammers to send email on behalf of bulk mailers. In related news, a Maryland judge ruled that Maryland's anti-spam law is unconstitutional, since it "seeks to regulate commerce outside the state's borders."
- Iowa ISP Robert Kramer sued 300 spammers in an effort to stem the 10,000,000 daily spam emails he saw (in 2000). A U.S. District Court judge ruled that one spammer must pay him US$720M, and another must pay US$360M. Widespread opinion is less than optimistic about actually collecting these damages.
- Anti-spam firm Postini reports that 88% of email is now spam; 1.5% of those messages contain viruses. MessageLabs says as high as 6%, depending on the report. Every related news story I checked predicted that 2005 will see the true rise of phishing. (My own mailbox has seen no relief at all from spam. The graph below shows the rolling average of the number of my personal spam emails for the past 15 months.)



- The loss of productivity due to spam is gauged at anywhere from hundreds of dollars per year *per employee* on up. Administrators sometimes find themselves buried in spam or in requests to make it stop. Phishing is a US$137M–500M industry, depending on whose numbers you believe.

Now let's think back to the Golden Age of Email. You remember: each electronic message evoked thoughts of Christmas, like a package of joy waiting to be unwrapped. The bell rung by biff to signal a new message set off a Pavlovian salivation of anticipation at a new missive—perhaps it was a product order, a business prospect, or greetings from a long-lost friend. Those were the days!

Alas, those halcyon days of communication of a certain purity are gone. The tears have been shed; we've moved on.

What happened? In a nutshell, some lawyers in the Southwest tested the waters of Internet advertising and found them bountiful. Subsequently, every budding entrepreneur with a scam, fraud, herbal pharmaceutical, erotic Web site, or home-mortgage connection has decided that "almost-free" advertising can make big profits. It's almost as though someone is creating billboards that read, "If you can#t splel VaigrA, you cn mkae big $M$O$N$E$Y$ wtih b.ul.k adtervising on teh I*N*T*R*E*N*E*T."

Some institutions are trying to stem the tide. We have black lists, white lists, and grey lists. We have black hole (non-)routing, sender protection frameworks, and, best of all, 150 vendors raking in two-thirds of a billion US dollars in 2004 just to slow the scourge. Venture capitalists pumped US$23M into anti-spam firms in August 2004 alone.

Current solutions seem to fall roughly into these categories:

- Stopping spam at the gateway to the local network (e.g., a list of unacceptable IP addresses)
- Filtering of spam using software (maybe by a third party)
- Laws that suggest spamming should be stopped
- Blocking by (a very few) ISPs of outgoing email connections from computers that seem to have been compromised

Perhaps looking at the bigger picture will help, since these measures are having an all-too-limited effect.

- Almost all spammers are motivated by money, although a tiny fraction are concerned with disseminating a political, a religious, or even a bizarre scientific message. The low up-front investment for universal and affordable access to the Internet (DSL, cable modems, businesses, hosting companies, even Internet cafes) drives down the entry cost. Crackers who take over others' computers (creating "zombies") send out more than two-thirds of the current flood of spam. Spammers would have no interest in this endeavor if they could not obtain customers. Behind-the-scenes reports reveal that spammers profit as do all scam artists: by selling dreams, appealing to greed, and selling items widely perceived to be unavailable in mainstream markets.
- Spammers enjoy anonymity. There are no means to complain about or avoid spam; requests to be removed from spammers' lists are widely believed to be ignored or, worse, are used as confirmation of the address.
- Spammers obtain their revenue at the credit-card-processing bureau, but the connections among their emails, credit card accounts, and true identities are not discernible by mortals.

Stopping any of a spammer's three enablers will thwart them:

- Remove access to cheap and easy sending of bulk emails.
- Remove anonymity: make spammers stand up personally for their products and services.
- Remove their ability to collect money easily and secretly.

I initially thought removing anonymity would solve the problem. Creating a positive identification token for tens of millions of Internet users is a very pricy proposition, and one not likely to serve the purpose. It appears that many people would gladly sell spammers their token for relatively small amounts of money.

Removing the other two enablers might yield better results. ISPs can either completely block outward port 25 traffic or restrict it to a set of well-known email servers. One would think it would be in the ISPs' best interests to shut down spammers. It's worked for Comcast, with 5.7 million subscribers. They implemented exactly this idea in June, stopping about 700 million emails per day.

Removing the ability to collect money is a very simple step to slow spammers: Identify a spam offer as fraud by purchasing the product and confirming that it is fraud, then (presumably with legal backing) work backward through the credit-card folks to shut down the offender. This seems like just the thing for our U.S. Federal Trade Commission. Existing legislation gives them plenty of ability to prosecute those who break laws not just once but millions of times. If the laws do not enable this, the laws need to be fixed. The "mood of the people" is such that this should work out quite easily. In fact, the state of Virginia sentenced a spammer to prison for nine years (though the constitutionality of that law is probably under study now as well).

Note that these proposals stop the problem at its source, not after it has consumed network bandwidth (not free), passed filters (not free; the manpower to deploy them has a cost), or even made it all the way to inboxes (where "just press delete" is a stupidity no longer even amusing).

The filtering folks, the black-hole list maintainers, commercial firms, and an heroic set of thousands of administrators are doing a great job of slowing the infection of this parasite on the Internet. None of them, however, has the ability to stop the problem at its source. ISPs and federal agencies do—and in many countries.

Why is spam OK? Why do we have to "take it"? I think we should do a much better job of encouraging those who *can* stop spam to do so.