

'DADDY, DADDY... THAT MAN SAID #\$@%!'

Gordon Woolf* looks at the dirty deeds upsetting the smooth flow of email

This isn't really about that offal of the Internet: spam. It is about ordinary messages from ordinary people which aren't getting to their destination because of spam and the administrators and ISP managers trying to stop it.

We would all like to be rid of those messages offering us free access to porn sites (if you'll just give us your credit card number for safe keeping!), and the way to get bigger mammary glands or longer organs of another kind.

According to Brightmail <<http://www.brightmail.com/>>, one of the firms providing anti-spam services to big business, including some major ISPs, junk e-mail now takes up 38 percent of the average inbox, up from a merely annoying 8 percent a year ago. However, in among that spam, there could be that email that you wanted urgently. It could be held up, or deleted, because the sender used a common word for excrement just as he, or she, does on the phone every day. Or maybe he mentioned a certain drug, which, a computer industry newsletter found caused their newsletter to be rejected by more than 1000 mail servers. (Ask your doctor for the common name of sildenafil citrate).

The event which set me on a trail to find out more about such censorship was an email in a Listserv group for desktop publishers, hosted by a US university, and of which I am a co-owner. The email, from an Australian incidentally, was a tirade of invective about the operating systems produced by a certain Bill Gates and the problems in getting his computer to work. The strange thing is that 99 percent of the invective was apparently acceptable, because what triggered the censoring software was a quite common and hardly blue word. The word? Well 'it' was preceded by the sound one makes to keep someone quiet and followed by a three-letter acronym for an ancient form of telegraphic print output. Is that enough of a clue? Perhaps we'll all have to become cryptic crossword addicts.

In this case the mail censoring software installed at a subscriber's ISP sent a message to the Listserv software and sent a copy of that message to the subscriber. The message requested the sender to "Please remove any inappropriate language and send it again." However, the message then went on to state what the offending word was, so the poor subscriber, who had to be protected from such "offensive language" was told just what the language was that they were not being allowed to read.

This may seem like the child who learns a new word and uses it as in the title of this article, but this is not a joke.

Janet Roberts wrote an article for the website "E-zine Tips" recently titled "Forward: The New 'F' Word". It seems that some such software can be triggered by the word 'forward'.

Programs we are talking about have names such as MailMarshal, SpamKiller, Postal Inspector, and iHateSpam. Used assiduously, they can be very useful and MailMarshall puts up a strong case for filters at its web site <<http://www.marshallsoftware.com>>:

"Employee viewing and trading of pornographic, offensive or otherwise unproductive material has emerged as a key concern of many business managers. Not only are these activities wasteful of time and resources in themselves, they may also involve the employer in legal issues of harassment."

I cannot disagree with that. Equally, I see the usefulness of a program which means that if a company decides that "no employee sends or receives executable files, except for members of the IT department, MailMarshal allows you to make it so".

The program identifies files by the code, not just the file extension, which is a step up on how it used to be done. However it is in the area of content filtering based on text that I am expressing concerns.

What has happened is that the real spammers, realising what these content filters are doing, will avoid those words. So the real spam tends to get through while the innocent email gets stopped. By the time the anti-spam software sees a pattern, the junk emailers have moved on, and it is mum's message saying "I have great news!!!" that gets blocked.

The battle continues: Brightmail has around a million dummy email accounts to receive spam so they can see patterns as soon as they develop. They have a matter of minutes to update the spam filters of their clients from when an email gets through their existing filters and lands in any of those addresses. Brightmail may update their clients' filters at a rate of five or six times an hour.

Janet Roberts told of the publisher of an email newsletter called Road Bike Rider who said his newsletter had been rejected as a 'chain letter'. This newsletter requires the double opt-in process: the subscriber has to send an email message or fill in a form to subscribe, and then receives an email which has to be answered including a specific alpha-numeric code, or has to enter that code on a website, proving they are the person with that email address.

What terrifying phrase got this publisher into trouble? It was "forward this issue to your cycling friends".

The censoring software stated that it had been banned under a rule to block chain letters which looked for the expression "forward" followed by 'many' or 'all' or 'friends' or 'anyone' or 'others' or 'people' or any word starting with 'every'.

TidBits, a long established and well respected email newsletter that caters mainly for Mac users, but which is also read by many who value its overall insight into the world of computers, has also run into trouble. Writer Adam C Engst states: "The mushrooming volume of spam has caused the value and utility of email to drop significantly for many people already, and the way overzealous server-side content filtering makes email unreliable stands only to worsen the very problem it's attempting to fix."

I'm mentioning email newsletters because they are legitimate senders of a lot of email, and so see any effects magnified a thousand times. The filters which stop email newsletters being received by people who have asked to receive them are the same filters which will stop Uncle Albert's message or the order from a major client. A publisher of medical books told me that newsletters for that community are having many problems because they mention all kinds of nasty words

A common response from some users is that losing some legitimate messages is worth the reduction in spam. But is your mail sufficiently unimportant that you don't care if some of it never arrives? Adam comments: "We don't automatically treat infections with amputation".

The ISP I use for my dial-up service (I live outside the current MelbPC service area) automatically adds a "***SPAM***" prefix to doubtful mail. It seems to work fairly well, but has marked one or two messages as spam which most definitely were not. However, it is up to me whether I delete such messages as I scan through them."

Another way that service providers can deal with filtering is to quarantine messages caught by content filters, so users have the opportunity to recover important messages -- but you have to find out that a message has been blocked.

The real problem is spam itself, and the Internet community will have to address spam at a fundamental level. There have been numerous proposals, ranging from legislation to modifications to the SMTP (Simple Mail Transfer Protocol) system. Others are trying to find ways to ensure that spam doesn't pay, but even the Nigerian scam has succeeded in duping some who receive it.

The big men of spam claim (if you can believe anything from a spammer) to be making

millions of dollars -- but the Wall Street Journal recently interviewed the other end of the scale, a single mum with two kids who sends 60 million emails a month. Laura told the newspaper that if she gets 100 responses from every 10 million messages, she will make \$200,000 this year in commissions.

The email addresses she buys can be created by suppliers who hurl tens of thousands of common names at e-mail systems to see what sticks. When the attack yields a live address, the spammer adds it to his database. In such ways the spammers may find even legitimate addresses which have never been used.

Geoff Duncan, who runs the TidBits email comments: "Email, often hailed as the Internet's 'killer app,' is in danger of becoming an unreliable, arbitrarily censored medium - and there's very little we can do about it."

Brightmail estimates that spam increased by 600 percent in 2002. Filtering that works may save money, but filtering that backfires has direct costs. Part of that cost is passed off to the sender, but part stays with the organization doing the filtering, to support users who didn't receive expected email or dealing with remote administrators to figure out what's going wrong.

When a legitimate email is rejected because it contains the words "undress" and "blonde" without any connection between the two, one may want to ask "Does email have a future?"

*Gordon Woolf is a MelbPC member, who writes and publishes books on publication production, but who also runs an email newsletter and helps administer a long established email discussion group. He can be contacted at gordon@worsleypress.com

THE TOP SPAM OF 2003

What was the top spam of 2003? According to AOL the ranking was:

- 1 "Viagra online...". (and similar offers of boosted performance)
- 2 "online pharmacy" (any medicine you want)
- 3 "get out of debt" (just say you don;t want to pay)
- 4 "get bigger" (boosting the size of body parts)
- 5 "Online degree" (any job just needs a bit of paper)
- 6 "lowest mortgage rates" (Mortgage spam is a classic)
- 7 "lowest insurance rates" (pay and hope you never claim)
- 8 "work from home" (be your own boss)
- 9 "Hot action" (Sex is the key to everything)
- 10 "As seen on Oprah" (Does the show run 24/7?).
