

Eggs over easy, but, please hold the Spam

Contributed by Andreas Haberstroh
Thursday, 09 February 2006

Filters and black lists provide some relief, but Spam is still in the eye of the beholder.

Today an amazing email offer arrived: "Andreas, Enhance Your Breasts Now!" Being a man, I wasn't sure whether to be amazed or insulted by this offer — click, Delete! Spam knows no boundaries. Everyone gets it. The question is, what do we do about it? My initial reaction, "first, we kill all the spammers," breaks a commandment, not to mention a few laws, such as California Penal Code 187. So, what about the American Way — legislate!

Currently, our governments — local, state and federal — are trying to come up with legislation to bring some relief to our overstuffed inboxes. In California, we have two laws on the books: 17538.4 and 17538.45. These laws basically require anyone who sends unsolicited email (spam) to include ADV or ADV:ADLT (for adult-only content) in the subject line so that email users (and mail server programs) know it is spam. Failure to include these tags could result in punitive damages.

This is great in California, but what about the spammers in other states or countries? Federal laws — dating from the 106th Congress through the 108th Congress — are too numerous to list. And, can you trust Congress to make an anti-spam law that ACTUALLY works? Take the no-call list law as an example. Political parties and charities are exempt. In the weeks leading up to Election Day, I don't particularly want to get up from dinner have Joe Councilman try to get out my vote. (In our high-tech age this will likely be a computer doing a fine impression of Joe Councilman.) But the law exempts politicians. Nice loophole, eh?

So, the next battleground on which we fight spam is the Mail Server. This battle has been raging for quite some time. Large organizations own their own mail servers and combat spam with various filtering techniques. Most major ISP's filter spam now as well. Realtime Black List (RBL) involves a server on the Internet that has a list of "known spammers," or mail servers that unwittingly pass along spam. The receiving mail server checks for the message sender on an RBL. If the sending server is listed, the receiving server blocks the message. This isn't a perfect solution, but it's effective. Unfortunately, a few RBL services have been sued for infringing spammers' First Amendment rights. Many major RBL services now charge large fees to cover potential liability.

Another popular technique is rule-based filtering. The receiving mail server reads the message content and scores the message according to certain attributes. For instance, "free" in the subject line earns the message a point. A string like "click here for more information" in the message body earns it another point. Once the message exceeds a threshold of unwanted attributes, the server marks the message as spam. Yahoo! uses this method to sort mail into its Bulk folder.

Unfortunately, rule-based filtering is not foolproof. Legitimate, even user-requested emails can fail a spam filter's threshold test. For example, most rule-based filters will block USA Today's daily financial emails. So, that brings us to the last battleground, the user's mailbox.

Computers can automate many processes, but face limitations when we try to make them substitute for human decision-makers, as when we ask them to distinguish spam from non-spam. On iBusy's mail servers, our mail filter identifies about 85% of the spam messages as being spam, and about 1% of legitimate mail as being spam. If you were anxiously awaiting a message in that 1%, you may be sifting through a Spam folder.

What does all this mean? Only the user can distinguish spam from legit mail. If, after filtering by your company server and/or your ISP you still have an inbox full of incredible offers for Viagra and breast enhancements, you may have to take matters into your own hands. Don't reach for the Smith & Wesson, there is software out there to help you.

McAfee's SpamKiller and Symantec's Norton Spam Alert are two products that protect individual mail clients with rule-based and list-based filters. SpamKiller includes include as well as exclude filtering so you can allow mail from friends through. Mail Frontier's Matador sorts mail into three piles: known good mail, known spam, and suspect mail that the user must judge. If spam is making it hard for you to find email from friends and family — or from clients — there are tools that can provide you some relief. Ultimately, however, you are the most important part of the solution. And, a note to businesses who use email for advertising: email wisely. Your clients and potential clients will thank you.