

Email Marketer Weighs in on the Pros and Cons of Spam Filters

*By Carrie Harrison
Vice-President of Sales
Forge Marketing
Carrie@Forgemarketing.com*

October 3, 2003

Forge Marketing recently partnered with Ipsos-Reid to find out more about Canadians attitudes toward email marketing. The survey revealed that 41 per cent of Canadians have installed spam filters to help fortify them against a deluge of unsolicited email. Now spam filters are causing a ripple in the email marketing industry.

To outwit the changing tricks used by spammers, software developers are coming up with equally resourceful spam filters. If you're an email marketer or communicator wanting to know what you're up against, here are a few tips about blacklists and the latest batch of spam filters in use today.

Sending an email as a blind copy to a group distribution list is a common practice; however, some ISPs automatically block emails containing lengthy blind copies or mass mailings – unless they know your IP address to be of a reputable source. If you are known to them as a permission-based mailer, they will let your mass emails through. If not, you may end up blacklisted.

As well, if you send out a group email and even just one recipient complains that it's unwanted, you could be blacklisted by that person's ISP. If the complaint goes to a large provider like America Online, you won't be able to send email to any recipients with an AOL address. You'll have to contact the provider and argue your case for blacklist removal.

Another way you can end up blacklisted is to use one of the many online outsource solutions promising to send out emails en masse for free or at nominal costs. The problem is that the outsource service-provider may be widely blacklisted because of its high-volume email output.

More importantly, these companies do not screen what is being sent out or to whom. This means that even if you are sending permission-based email communications, you may be labeled as a spammer by the ISPs because of someone else's spam mailing using the same free/cheap email solutions provider.

To avoid getting blacklisted, your company or your email marketing solutions provider should be proactive in creating relationships with major ISPs. This way, your IP address is known to them and you are essentially "whitelisted" instead.

When it comes to spam filters, there are a host of pros and cons. A password filter is fairly airtight. It will only accept email that contains a pre-set password in the subject line. Unless you know it, you can't get through. While a password filter is effective for blocking spam, it can block desirable email too.

A challenge/response filter, such as MailFrontier Matador or SpamArrest, sends an automated message that asks you to provide return confirmation of your email address. The system is verifying that you are an individual sender, not a machine generating spam. But many "requested" newsletters may also be blocked by these filters, if a company or an email solutions provider is not equipped to respond manually to these types of verification challenges.

Whitelist filters only allow email through from approved senders. The sender's address must be in the recipient's mailbox or the email will bounce back. There is no early warning system that seeks to verify the sender's legitimacy, so be aware that you may have no indication your email didn't get to its destination.

Spam Assassin is one of the more common rules-based filters available. It blocks email based on how it conforms to pre-determined rules, and catches spam by finding tell-tale signs like odd punctuation.

The good news is that many organizations use this type of filter and, if you are following all the rules of legitimate permission-based email marketing, you should have no fear of being filtered out. At the same time, the rules keep changing and companies are able to set filters to be so sensitive that even innocuous daily correspondence can get tossed as spam.

A community-based filter can be an effective tool. For example, Cloudmark Spamnet blocks email based on a group determination as to what is junk. Since the group decides what constitutes spam, personal and other material does get through. As a con, this type of filter may not catch the newest messages outside the group criteria and can admit too much spam.

An adaptive Inboxer is a filter that learns by analyzing examples of what is discarded as spam and what isn't. This system requires training, especially at the start. The system learns the user's preferences, so works at keeping out spam and accepting messages shown to be desirable to the user. Inboxer from Audiotrieve has been given high marks for effective filtering using Bayesian statistical techniques.

Anti-spam legislation now under review may prove to be the ultimate filter, reducing overall junk mail volume. There is already evidence, though, that spammers will simply go offshore or to other locations where spam is legal, and continue to ply their unwanted wares. Many also believe that legislation will be too difficult to enforce.

It is possible to pass through each of these filters by taking the time to understand how the common spam filters work and by using good email business practices. Ground rules for email marketers include: researching and installing spam filters for in-house pre-testing, proactively ensuring good relationships with ISPs, carefully monitoring campaign results, and meticulously ensuring that lists used are based on recipients who have opted-in and given you permission to send your messages.

It's the only way to keep off the blacklists, stay on the whitelists, and avoid being relegated to the junk bin.

Carrie Harrison is Vice-President of Sales for Forge Marketing, a North American leader in permission-based email marketing. Forge's own policy is "no spam, no exceptions."