Why do I keep getting bounces for spam messages from mailing lists I'm on?

Why do I keep getting bounces for spam messages from mailing lists I'm on?

You may have seen bounces to a mailing list you are on indicating that spam mail could not be delivered to some of its recipients, such as the following:

```
The original message was received at Fri, 15 Dec 2006 09:39:53 -0500 (EST)
from W92-130-BARRACUDA-2.MIT.EDU [18.7.21.223]

   ----- The following addresses had permanent fatal errors -----
foo@alum.mit.edu
    (reason: 554 5.7.1 Rejected as Spam see:
http://alum.mit.edu/help/spam/rejected.html)
    (expanded from: <sample-list@mit.edu>)
bar@media.mit.edu
    (reason: 554 5.7.1 Message rejected as UBE (spam):
BAYES_60,EXTRA_MPART_TYPE,FROM_LOCAL_NOVOWEL,HTML_IMAGE_ONLY_08,HTML_MESSAGE
,INVALID_DATE,SPF_PASS,UNPARSEABLE_RELAY)
    (expanded from: <sample-list@mit.edu>)
```

To understand why sample-list is getting a bounce in this case, it's necessary to understand a little about how email works. Email messages have two different places where a return email address can be set. One of them is known as the envelope-from address, which you can often see listed as the Return-Path header. The other is the From: header that you typically see in your mail client.

Both of these addresses are just like the return address on a piece of regular mail – anyone can claim that it's from anyone else.

In the case of the bounce, the original spam message was set with an envelope-from of sample-list (the From: header is completely irrelevant), which is why sample-list is receiving a bounce.

Oftentimes, people misinterpret the bounce messages to mean that other mail servers, in this case, alum.mit.edu and media.mit.edu, are mistakenly sending bounces back to the envelope-from address. This is actually not the case (most of the time). When the spam is sent to sample-list, MIT's incoming mail servers inform the sending computer that it has accepted the message. MIT's mail servers then redeliver the mail to everyone on the mailing list.

In some cases, the mail cannot be delivered because other mail servers, such as the media.mit.edu and alum.mit.edu mail servers, reject it, because they consider it to be spam. These mail servers are *not* sending any bounce messages in this case, but are simply informing MIT's mail servers that they are not accepting them. This is the standard accepted practice, as mail can be misclassified and silently dropping mail is poor. For more technical details and an explanation of why this is the standard practice, see http://www.tldp.org/HOWTO/Spam-Filtering-for-MX/whysmtptime.html

Since MIT's mail servers have already accepted the mail, they are no longer communicating with the actual sender. To inform someone who was supposedly the sender that they were unable to deliver the mail, MIT's mail servers then send a bounce message to the envelope-from address. While annoying in the case of spam messages, sending this bounce message is necessary to inform the supposed sender that the message could not be delivered.

As with alum.mit.edu and media.mit.edu, MIT's mail servers actually also do reject some portion of spam such that it never arrives in your MIT INBOX or Spamscreen folders, but the sender is informed (without generating a bounce message) that MIT's mail servers did not deliver the mail.

You may wish to work around this annoyance by filtering such spam bounce messages in your mail client by configuring a filter for messages from MAILER-DAEMON@* that are addressed to something other than your personal email address.