Mailing List Module

Dealing with Spam Filters

How to ensure that your message doesn't get stuck or quarantined in a spam filter

Table of Contents

Chapter 1

Introduction

Emails that are sent by the Mailing List module may sometimes be taken for spam emails. This article describes how some popular spam filters operate and gives recommendations on how to help your newsletters avoid spam filters.

This article contains the following chapters:

- **Introduction**
- **Dealing with Spam Filters**

1.1 Dealing with Spam Filters

Let's consider some popular spam combating methods and the actions you should take to let your emails pass through them.

- **Black and White Lists**
- **Conflict between the Back Search and DNS System Identification Methods**
- **Challenge-Response Systems**
- **Email Fields Verification**
- **Detectors of Mass Mailings**
- **Email Content Check**
- **Universal Solution**

1.1.1 Black and White Lists

The purpose of the *black list* is to ban the emails addresses and DNS names that are added to this black list. In turn, the *white list* is configured so as to allow only addresses that can be found on the white list. As a result, an email with either a banned email address or DNS entry may get trapped in the spam filter.

Solution:

Display a proposition to add the involved address to the receiver's white list if the test email was not received.

1.1.2 Conflict between the Back Search and DNS System Identification Methods

Back search systems seek to identify fabricated addresses of senders. *DNS system* matches IP addresses to domain names of sender hosts and vice versa. In such a case problems may occur. Back searches are needed to generate emails on known and trusted email servers that use known IP addresses. Unfortunately, many domain names are not associated with static IP addresses. Many small companies want to use their own domains but cannot afford to have individual static IP addresses and mail servers. As a consequence, DNS names of emails may be taken for spam DNS names.

Solutions:

- Use a mail server with the static IP.
- Make sure that email addresses that belong to the mail server used for sending emails are correct.

1.1.3 Challenge-Response Systems

Challenge-Response systems store a list of legal senders. An email sent by a new user is temporarily blocked. A message will be sent to this user with a request for response (usually it is a link or a response message). After the response has been given by the user concerned, he or she will be added to the list of legal senders.

Solution:

The receiver should manually add the sender to the list of legal senders.

1.1.4 Email Fields Verification

1. The 'From' field is blank.

   Solution:
   The sender must enter the correct email address.

2. The 'To' field is blank.

   Solution:
   Fill in this field with some email address, for example the sender's email address.

3. There are too many receivers of the email.

   Solution:
   Decrease the maximum number of envelope receivers.

1.1.5 Detectors of Mass Mailings

This method can be used by providers or on public mail servers (where email traffic is vast). If an email is directed to hundreds of thousands of recipients and the sender address is not in the list of major subscription mail delivery servers, such as Subscribe.com, it can be identified as a spam email.

Solutions:

- Decrease the maximum number of envelope receivers.
- Use a registered server of subscription mail delivery.

1.1.6 Email Content Check

1. For all emails the *hash-value* is usually calculated and saved. Then it is matched against previous hash-values. If the hash-value recurs many times, the email in question will be identified as a spam email.
2. *Using signature*. Note that an email signature is identified by spam filters as a mini-email, too. So make sure that you leave out all 'provocative' content.
3. *Linguistic heuristics*. A spam filter matches email content to spam terms (both words and phrases) having a probability rate.

Solution:

Pay attention to the content of email messages. Make sure they don't contain well-known spam phrases.

1.1.7 Universal Solution

Manually adding the sender in question to the list of legal senders by a receiver is supposed to fix all issues mentioned in this article.