Whitepaper

Mail Deliverability Issues

August 25, 2010

Information in this document is subject to change without notice. Companies, names, and data used for example herein are fictitious unless otherwise noted. Some screen captures have been cropped and/or edited for emphasis or descriptive purposes.

L-Soft invites comments on its documentation. Please feel free to send your comments by email to: manuals@lsoft.com

Introduction

Several customers have written:

> *"We send out a weekly newsletter, but we get complaints from users who never receive their copy."*
>
> *"We have a user that gets all their emails except mailings from our list."*
>
> *"Why am I not getting copies of your weekly news magazine? My ISP changed their spam filters."*
>
> *"What is this newsletter from Company X? I never signed up for this!"*

Email deliverability has become an important issue in Email Marketing. Marketers ask, "What can we do to ensure successful delivery of the emails we send out?" Recipients ask, "Why don't I receive my regular mailing?" ISPs and others in the middle say, "We're drowning in a flood of unwanted email." Nobody seems to have a clear idea of what useful practices will ensure a greater certainty of success for all parties.

A good place to begin is by reviewing the fundamental principles of the Simple Mail Transport Protocol (SMTP). This document [RFC 821], adopted in 1982, is the defining standard by which email travels on the Internet. One important, but often overlooked fact is that email delivery is not guaranteed. The only requirement is a "best effort" attempt to deliver an email message. Another fundamental principle is that the receiving side of the email transaction has the complete power to determine, by whatever rules it deems fit and necessary (rules it need not disclose), whether or not to accept any, some, all, or no email from a sender. Acceptance of email according to SMTP is based on trust that the sender is following acceptable protocol and convention. It is also based on trust that the sender is who they say they are, but there is no provision for verification.

These principals help to explain why, in the current email marketing climate, that marketers and others sometimes fail to have their important and desired email messages delivered. They complain that their attempt to deliver is being "blocked" by some popular receiving ISP. They ask what they can do to "force" acceptance of their email messages. The answer, unfortunately, is that there is no way to force a mail server to receive particular messages. In fact, attempting to do so is frequently seen as a hostile act that reinforces the determination of the receiver to refuse acceptance.

Let’s take a look at a series of recommended good practices that promote success. These practices can be divided into responsibilities of the sender, responsibilities of the intermediate service provider, and responsibilities of the recipient.

Responsibilities of the Sender

As noted in the SMTP Protocol discussion above, email acceptance by the receiving party is not guaranteed and all decision-making power about acceptance rests with the receiving side. This imposes a much greater responsibility on the sender to ensure that the emails they send will be found acceptable. Sender responsibilities fall into two large areas: marketing, or those concerned with the recipient relationships; and technical matters, those concerned with provider relationships.

Recipient Relations

The single most important principle in the area of recipient relations (marketing) is to send only "confirmed opt-in" mail to the recipient addresses that you have. Confirmed opt-in recipients have positively responded to an email confirmation message sent to them when they signed up to receive mail. This confirmation message also tests for the validity of the recipient's email address. Unconfirmed "opt-in" addresses may be mailed to one time only, in an effort to obtain an "opt-in" confirmation. "Opt-out" mailings, on the other hand, send email to recipients without prior confirmation and continue to do so until they unsubscribe. This method should never be used in a commercial environment. Exceptions to the opt-out rule can be made for mailings to employees in closed corporate environments or to staff or students in schools. Neither of these is a "free choice" environment.

Marketers who create a climate of trust and respect for their mail recipients will have far fewer problems with mail deliverability. Mail will be less likely to be reported as spam and therefore less likely to be filtered out by the recipient or by ISPs. This climate can be achieved if marketers take the following actions:

- Fully disclose how you intend to use the addresses you solicit and confirm.
- Provide an explanation of what kinds of email will be sent, and how often.
- Provide a link to a publicly posted privacy policy.

Marketers need to provide an easy-to-use (one click + confirmation) and an easy-to-find (not buried in fine print on last page) unsubscribe mechanism. One reason frustrated users report messages as spam is they cannot find or do not trust the unsubscribe mechanism.

In the process of soliciting addresses from potential recipients, marketers should attempt to verify addresses at the point of entry. This can be a simple test for correct syntax, for instance making sure addresses contain no spaces, contain an @ sign, and contain at least one '.' (period) character in the domain part of the address. Tests that are more complex will test for valid top-level domains (.com, .net, .org, .edu, .mil, and so on.) and tests that are even more complex look for syntactically correct but obviously bogus addresses using repeated characters such as "1111@1111.111". Similarly, there are several interesting ways to misspell popular domains, for example, hotmail.com,that result in invalid, non-deliverable domains (htomial.com, hotamil.com, etc.) Guard your database from these obvious errors (usually typos). If such addresses do make it into your database, clean them out on a regular basis.

Along with keeping out bad addresses, marketers should promptly and aggressively remove addresses that bounce (returned as undeliverable). Marketers should also attempt to weigh (and track) the relative importance of certain subscribers over others. People using "throw-away" free-mail accounts for a one-time email, may not have the same marketing "value" (staying power) as somebody with a paid account with a regular ISP. On the other hand, some loyal responders prefer a free-mail account for its ubiquitous convenience. By tracking actual responses (click-throughs) marketers will know which addresses are more "valuable".

Marketers need to be aware of and actively test their content against known anti-spam filtering programs. Sometimes innocuous content can rate a surprisingly high negative score in such filters. There are also services that will do this evaluation for you and make suggestions for alterations to lower the score and increase deliverability.

To have the highest success rate for reaching your email recipients, marketers need to gain a basic understanding of how SMTP email works in order to develop realistic expectations about how it can be used and why some messages are not received. Gaining the trust of your recipients by respecting their decision to accept or not accept your messages, keeping bad addresses out of your database, and designing your message content to avoid spam filters are all ways to improve email communications with your subscribers.

Technical Concerns

The following considerations are more technical in nature. This document is not meant as an extensive technical explanation of email server configuration, but as an overview of some techniques to make your email communications more likely to be accepted by ISPs and recipients. If you need further information or clarification, see your IT department.

Your outgoing mail server needs to have a Fully Qualified Domain Name along with both an "A" Record (forward lookup) and "PTR" Record (reverse lookup) in public DNS. This is so that receiving servers will be able to identify and verify (to the limited extent currently possible) that your server has proper credentials. When your mail server is properly identified, the mail coming from it will be much less likely to be blocked.

Do not allow your mail server to be configured to allow open mail relay. Permit mail relaying only from known and trusted mail sources, preferably inside your network. Also, be wary of email virus attacks that may also affect your trusted sources of email.

Test and monitor email queues and sample bounce logs to be sure that addresses that bounce are removed from your database. If you keep sending mail to a great number of bad addresses many ISPs could block your mail. This occurs because ISPs often count the ratio of bad addresses to good addresses in any large volume mailing (generally 1000 or greater). If they detect too many bad addresses, they will assume you are attempting a "dictionary attack" of randomly generated email addresses and cut you off.

Evaluate and consider participating in one of the various verification methods to validate the identity of the origin of your email so that recipients can trust the source of the message and are less likely to report it as spam. Seen as a rapidly evolving area of the email industry, there is a definite trend towards verification of the sender.

Monitor your email flows so that you will know what is “normal” for your environment. This will help you detect abnormal situations early, while it is easier to deal with problems. If possible, adjust your server's mail delivery rate so that the rate for larger domains is "comfortable" for that domain. Monitor various blacklists looking for your own server's IP address. If you find it, take action immediately. As little as two or three complaints from unidentifiable recipients may get your server blocked. Ensure that your marketer's unsubscribe process actually works promptly. If not, angry recipients, continuing to receive mail after they have unsubscribed, will report you and you will be quickly blacklisted.

Develop and maintain personal contacts with your larger destination service providers. When you are blocked, it helps if you know someone personally to call to enquire why. If they know you, they will probably give you a prompt reply. Follow as many good practices that you can, applying them first to your largest recipient domains and working your way down the list to smaller domains.

Finally, you should also make sure that you are running the latest version of your software packages.

Responsibilities of the Service Provider

Service providers ought to give users the greatest possible latitude for determining what they think is unwanted or undesirable. To this end, service providers need to inform and actively assist recipient users in configuring their choices in whatever filtering system is provided. Currently, many providers adopt a “not our problem" attitude as the first response to any queries from users. Sometimes a problem is not the provider’s fault. However, often it is and this attitude destroys trust between the user and provider. When changes are necessary to the system,

publicize them in advance and attempt to minimize the impact by assisting with the transition from old to new.

Providers' practices and policies need to be fully disclosed so that senders and recipients know what to expect. Cooperation with senders using various schemes designed to verify their identity and speed delivery adds to trust and building positive relationships. Another show of good faith and the will to make email work for all parties involved is for providers to supply a public point of contact for senders experiencing problems with their receiving domains.

Responsibilities of the Recipient

Does the recipient have any responsibilities? We suggest that they do, both to the sender of email that they want to receive and to their service provider. Here is a list of recipient responsibilities:

- Provide a correctly spelled email address to the sender.
- Positively re-confirm, when requested to do so (by email), that the mail is desired.
- Ensure that the proper information about the sender's regular email is entered in any "white list" or is otherwise pre-set in any filtering mechanism, so that mail identified in the specified manner will be accepted.
- Monitor mailings and report delivery failures, both to the sender and to their service provider and work to resolve any delivery issues.
- Use the correct unsubscribe procedures from sender's mailings, rather than simply reporting them as unwanted spam. Remember, you confirmed that you wanted this mail at one time.

Recipients need to stay informed on available filtering mechanisms by the service provider. Changes to the provider's system that may affect their ability to receive messages should be noted. Recipients may decide to change providers if they do not receive the level of service they expect or need.

Conclusion

In summary, email deliverability is a highly complex issue with many interrelated facets. It is also a highly volatile, frequently changing system. New outside influences such as laws may affect this as well. Success in delivering email with the highest reliability requires constant participation and cooperation of all parties and continuous improvement of practices.

How We Can Help

L-Soft provides you with several products and resources that make it easier for you to manage your email's deliverability. Our products contain features such as:

- **Automatic Bounce Handling**

  Automatically take care of your email delivery errors or bounces, saving you time and making your email management easier.

- **Spam Control**

  Compatibility with various third-party spam filters allows you to prevent spam from reaching your site. In addition, checking your messages before sending will ensure that your messages are not classified as spam by your recipients email clients.

- **Virus Protection**

  With built-in virus protection (for Windows and Linux), all of your messages will be scanned for viruses before delivery, keeping your lists safe and secure.

- **DomainKeys Support**

  A cryptographic authentication solution that adds signatures to email messages, allowing recipient sites to verify that the message was sent by an authorized sender.

- **Deliverability Assessment Tools**

  Deliverability assessment tools help you test and analyze your DNS configurations, including DomainKeys, SPF, and Sender ID, giving you concrete suggestions for improving deliverability.

- **AOL Feedback Loop Auto-Processing**

  LISTSERV can automatically process AOL Feedback Loop reports (these special reports are sent automatically by AOL to organizations that are on AOL's whitelist). Once configured, LISTSERV automatically parses the reports and implements the actions required by AOL's whitelist agreement. This helps preserve whitelist status and reduce the number of spam complaints from AOL users. For more information on this feature, please see the documentation for LISTSERV.

For more information on our products, please visit us at: www.lsoft.com

In addition, our manuals, whitepapers, and tech tips give information and advice on how to manage your email environment efficiently using our products.

Some L-Soft Tech Tips that you may find helpful are listed below:

- **Q: How can I assess my LISTSERV list deliverability infrastructure?**

  http://www.lsoft.com/news/techtiplsv-issue4-2006-us.asp

- **Q: How can I use SPF and DomainKeys to increase LISTSERV's deliverability?**

  http://www.lsoft.com/news/techtipLSV-issue3-2006-us.asp

- **Q: Can LISTSERV Maestro use DomainKeys to authenticate outgoing email messages?**

  http://www.lsoft.com/news/techtipMAE-issue3-2006-us.asp

- **Q: How can I make sure my email messages get delivered?**

  http://www.lsoft.com/news/techtipmae-issue2-2005-us.asp

- **Q: How can I get LISTSERV to check messages for spam?**

  http://www.lsoft.com/news/techtipLSV-issue2-2005-us.asp

- **Q: What are some of the list configuration techniques that I can use to protect my lists from spam?**

  http://www.lsoft.com/news/techtipLSV-issue3-2007-us.asp

References

[RFC 821]Simple Mail Transfer Protocol, available at: http://www.ietf.org/rfc/rfc0821.txt

[RFC 822]"Standard For The Format Of ARPA Internet Text Messages, available at: http://www.ietf.org/rfc/rfc0822.txt

[RFC 1123] Requirements for Internet Hosts -- Application and Support (in particular chapter 5, "Electronic Mail -- SMTP and RFC-822"), available at: http://www.ietf.org/rfc/rfc1123.txt

E-mail Marketing Best Practices whitepaper, available at: http://www.lsoft.com/resources/whitepaper.asp

L-Soft Contrasts CAN-SPAM Act with the European Union's "Opt-In" Directive, available at: http://www.lsoft.com/news/optin2003/canspamvseu.pdf

Best Practices in Marketing with Email Newsletters, available at: http://sherpastore.com/store/page.cfm/1992?a=adtech

Feedback Loop Auto-Processing documentation available in the Advanced Topics manual for LISTSERV: http://www.lsoft.com/resources/manuals.asp