

Email Marketing and Methods to Ensure Delivery – Refinery POV

There is a growing concern among email marketers regarding deliverability of their messages. As the battle against spam becomes more diligent, the delivery rate of marketing messages is threatened by the techniques many ISPs are using to protect their subscribers. Unfortunately, techniques such as blacklisting can result in false positives that penalize legitimate senders.

Many ISPs have turned to authenticating a sender and whitelisting those senders who are legitimate. There are several techniques and technologies being used to authenticate senders.

Four of those techniques are:

- 1) asking recipients to add the senders address to their address books or whitelists in their email clients or in the preference settings of their online email service providers;
- 2) employing server-side solutions that help to verify the sender as the owner and originator of an email message;
- 3) installing commercial software applications that help to increase email deliverability;
- 4) partnering with a recognized certification entity to ensure a higher rate of deliverability.

1. Ask users to add the “from” address to their personal address book/whitelist.

One method for targeting a recipient’s inbox – as opposed to their spam, trash, or quarantine folder – is to have the recipient add the sender’s “from” address to their address book or personal whitelist. This has become a more common and prevalent method to increase the probability that the sender’s mail will be delivered and not rerouted or blocked by spam filters.

Senders will often place a message at the top of their newsletter or email subscription page and again at the top of their email messages that resembles something like:

To ensure this email is delivered to your inbox, please add the email address [respond@yourcompany.com] to your address book or junk filter settings.¹

To ensure receipt of our emails, please add us [something@yourcompany.com] to your Address Book. Thank you!¹

To insure delivery of this newsletter, please add newsletters@yourcompany.com to your e-mail address book.¹

Some senders provide more detailed instructions for their subscribers as to how to add the sender’s address to the user’s personal address book or whitelist in a particular client or email service.

See <http://www.medscape.com/public/help/misc#safelist> for an example of this.

While this technique is simple, affordable, and may work well at the recipient level to ensure a higher rate of deliverability, it does nothing to bypass filters at the provider level. Regardless of what the user’s settings are in their personal address book or whitelist, if their ISP is filtering and blocking the sender, the individual recipient’s actions have no impact and the email is not delivered.

2. Employ server-side techniques to improve deliverability.

The following tactics can help increase the likelihood your email messages will be accepted by the receiving ISP and avoid future deliverability problems.²

Create a reverse DNS. Set up valid RDNS entries for outgoing mailing IPs. The receiving mail server will be able to verify the owner of the IP and as a result, the email will pass one of the many basic ISP spam checks.

Set up an SPF. SPF adds another layer of authentication to outgoing email and protects against phishing attacks on the brand. Some ISPs, such as AOL, require SPF to be implemented to be considered for their white lists.

Make only one connection. Send only one message per connection to an email server. Some systems try to deliver as many messages through a single connection as possible (like adding 500 email addresses to the BCC field). ISPs frown on this technique that is often used by spammers.

Limit sending rate. Large spikes in traffic can be seen as dictionary or denial of service attacks. A good rule is to limit transmission to 150-200K messages per hour. Feedback in the form of bounced messages must be accepted, so outgoing speed shouldn't hamper the ability to receive bounces.

Accept bounces. Some email systems reject bounce messages. These "bounced bounces" can raise red flags at the receiving ISP. ISPs resent sending a response that a recipient doesn't exist, only to have the notification rejected and the mailings continue.

Validate HTML content. One of the dirtiest tricks in a spammer's arsenal is invalid, broken, and malicious HTML code, used to obfuscate his payload. Make sure any HTML code is error-free and follows W3C HTML guidelines.

Avoid scripting. Security risks due to script vulnerabilities in email browsers have increased over the years. The result is most scripts, such as JavaScript and VBScript, are stripped out of messages. Some email systems reject messages outright if scripting is detected. For greatest compatibility, avoid using scripts in messages. Instead, drive readers to a web site, where dynamic components are easily rendered.

Understand content filtering basics. Understand the different kinds of filters and types of content considered high risk. Read bounce messages, track which messages had high bounce rates and low open rates, and see if offending content can be reverse-engineered.

Monitor delivery and bounce rates by ISP/domain. Periodically (if not after sending every message) run reports by major ISP and domain on messages. Look for unusual bounce, unsubscribe, spam complaint, and open rates at specific domains. A domain showing off-kilter results likely has a filter or blocking problem.

Monitor spam complaints. Even the best permission marketers with world-class practices receive spam complaints, particularly if they have a high AOL subscriber base. Monitor the number of spam complaints for each mailing, and establish a benchmark average. Look for mailings with spam complaint percentages that vary from the norm. See if the cause of the problem can be determined. Was it an overly aggressive subject line? Too many messages sent within a short time? An unexpected type of email? Another factor? A high percentage of spam complaints may result in an ISP blocking current, or even future, messages.

Set up Sender ID. Sender ID, similar to SPF, is a Microsoft technology that has been opposed by several notable core internet advisories, including the Apache Software Foundation. However:

“All the major email service providers (ESPs) have announced their outbound email complies with Sender ID and SPF. Senders who have updated their DNS (define) entries to include their SPF records won't necessarily need to publish a new record for Sender ID, though Microsoft recommends ESPs may want to.

“Microsoft has begun to implement Sender ID checks on email coming into MSN and Hotmail accounts. It's only one factor in a scoring system to determine what email is spam. Microsoft says it will increase the weight Sender ID carries within that formula as the company sees how it works going forward.”³

DomainKeys. DomainKeys takes email authentication a step further than SPF and Sender ID. Like these technologies, DomainKeys uses information published in a sender's DNS (define) record. The twist comes at the send. Here, DomainKeys requires an extra step: a digital "signature" must be attached to each outgoing message.⁴

- When the recipient gets the message, they'll be able to:
- verify the domain name of the sender.
- confirm the message content hasn't been altered.
- match the "from" address to the sender's domain name to prevent forgeries.
- trace the message back to the sender's domain name.

DKIM. DomainKeys Identified Mail (DKIM) provides a method for validating an identity that is associated with a message, during the time it is transferred over the Internet. That identity then can be held accountable for the message.⁵ The responsible organization adds a digital signature to the message, associating it with a domain name of that organization.⁶

There is an obvious cost advantage to implementing these techniques for improving deliverability. There is no software or product cost as all of the solutions are either a matter of server settings or open source software installation.

There is, however, the cost of IT personnel to install and maintain these solutions. Also, there are ongoing debates as to the effectiveness of these solutions (particularly SFP and Sender ID) and limited adoption of solutions such as Domainkeys and DKIM.

3. Install a Commercial Software Application Solution

One such example of a commercial solution is **Port 25 PowerMTA**.⁷

The latest version - PowerMTA 3.2 - helps senders adapt to the next generation of e-mail by making it easy to comply with the latest authentication standards, adopt accreditation services, and monitor their delivery and reputation in real-time. PowerMTA 3.2 comes standard with CertifiedEmail imprinting features and functionalities, assuring delivery of approved senders' e-mail to the inbox.

This application can help to automate or simplify implementation of many of the previously mentioned techniques for server modification that can increase deliverability of email.

In addition to software costs, there is also the cost of IT personnel to become familiar with the software and to maintain and administer the solution.

4. Enroll in and be certified by a commercial whitelist service.

Many senders and ISPs are subscribing to commercial whitelist services that certify the senders as legitimate. One such commercial whitelist is Habeas. (<http://www.habeas.com/>)

The criteria necessary for certification with Habeas are similar to those that the sender should be employing on their own. Habeas merely certifies that these actions have been taken by the sender. Their certification is, in turn, recognized by ESPs and ISPs that subscribe to Habeas' service.

Here are the things Habeas looks for to certify a sender: ⁸

- Verifiable opt-in permission from email recipients
- Visible and functional unsubscribe capability on all emails and Web pages
- Unsubscribe requests processed within 10 business days
- Removal policy for email addresses that bounce repeatedly
- Clear, accurate subject lines that correctly describe email content
- May not send to harvested email addresses
- Clearly posted privacy policy
- System for accepting and processing complaint and abuse reports
- Valid physical postal address included in all email messages
- Require use of email authentication, such as SIDF/SPF
- Maintain recipient complaint levels below industry standard levels

See <http://www.habeas.com/en-US/Support/Knowledge-Base/Pre-Sales-Questions/How-many-ISPs-and-corporations-use-Habeas-to-identify-legitimate-email/> for more info about the ISPs and ESPs that are using Habeas' certification to legitimize email delivery.

There are other vendors providing similar services, however Habeas appears to have more relationships in place with the primary ISPs and ESPs.

There are monthly fees associated with the services Habeas, or any similar vendor, might provide.

References:

1. http://www.emallabs.com/best_practices/white_lists.html
2. <http://www.clickz.com/showPage.html?page=3483081>
3. <http://www.clickz.com/showPage.html?page=3597946>
4. <http://www.clickz.com/showPage.html?page=3485571>
5. <http://www.dkim.org>
6. <http://www.dkim.org/info/dkim-faq.html#basics>
7. http://www.port25.com/products/prod_index.html
8. <http://www.habeas.com/en-US/Senders/Certification-Requirements/>