

DMA Deliverability White Paper Review



WHITE PAPER



Table of Contents

About This Document..... 2

Executive Summary..... 3

Major Factors that Impact on Deliverability..... 5

Ten Steps to Improved Deliverability 8

Further Reading and Useful Links 17

About This Document

Email deliverability has become a formidably technical subject, and it would be easy to write a formidably technical document on the subject. That was not our intention - there is plenty of detailed technical information available on the subject, and the *'Further Reading'* section will point you in the direction of some of those sources.

Rather, this document has been written for the email marketing programme owner who has realised that their broadcasts are starting to experience delivery problems and are trying to identify why this may be the case. It highlights 10 of the major issues that affect email deliverability, and provides common-sense guidance on how to deal with them.

About The Authors

This document has been published by the Deliverability Hub of the Email Marketing Council of The Direct Marketing Association (UK) Ltd.

Published Date: January 2010

Written By: Guy Hanson Database Group Interactive
Simon Bowker eCircle

Edited By: Jonathan Burston CACI
Skip Fidura dotAgency
Sara Watts Data Media & Research
Komal Helyer Digital Marketing Services
Richard Gibson Return Path

Executive Summary

Over the past few years the emphasis on email deliverability has changed substantially. Previously, the key question was a fairly simple one: “Why are my emails getting blocked, and what can I do to make sure that they aren’t?”

However, the email broadcasting landscape is now comprised of more challenging terrain, and the question is no longer one of black and white – there are now many shades of grey as well! Most broadcasts will achieve at least partial delivery. The new deliverability challenge involves focussing on the portion that is not delivered, and then on ensuring that what has been delivered actually ends up in the inbox.

The primary reason for this change in emphasis is largely because of the massive volumes of spam that Internet Service Providers (ISPs) are attempting to deal with. According to the most recent McAfee Quarterly Threat Report, there are approximately 130 billion spam messages broadcast every day. The challenge for ISPs is to be able to identify (and eliminate) this volume without incurring collateral damage in the form of preventing permissioned email activity.

The secondary reason is around the very definition of ‘deliverability’. Historically the term ‘delivered’ did not include any inbox placement measurement and could more accurately be described as the ISP acceptance rate, i.e. the number of emails sent less the number of bounces that were returned. However, it is important to note that ISP acceptance does not mean the subscriber actually sees the message; there are still filtering processes which determine whether or not the email ends up in the inbox. The management and improvement of deliverability is therefore no longer simply a function of minimising bounce rates, but also of ensuring that the email ends up where it will be seen and actioned – in the inbox.

For email marketers to understand these threats involves understanding who the key players are, and how they operate. Sender reputation providers, spam filter vendors and blacklist operators all have a role to play, and each one uses a different approach to tackle the problem. The first part of this document examines who the key players are, and how their products or services are used to manage the spam threat.

Armed with this understanding, e-marketers then need to understand what steps they should be taking to make sure that their broadcasts are compliant with the requirements of these key players. The second part of this document provides 10 commonsense recommendations which, if adopted, will go a long way to ensuring that the sender’s emails end up where they are going to be seen and actioned – in the inbox.

This document is not intended to be a technical manual, and the 10 steps do not contain detailed instructions on how to implement each of the recommendations. However, in the final

section (*'Further Reading and Useful Links'*), there are a number of references that readers can use to find out more about these key concepts, and how to go about achieving them.

Once implemented, the remaining question is what should be regarded as an acceptable inbox delivery rate for a permissioned sender. This is a subjective question, but a frame of reference is provided by a recent piece of research carried out by Return Path where 'Accepted Rate' (effectively delivery to inbox) stands at around 85% for Europe ¹.

Having implemented the recommendations outlined in this document, most e-marketers should be able to produce delivery metrics that are at least broadly comparable, and often better than the above 'accepted rate'.

1. "The Global Email Deliverability Benchmark Report, 2H 2009"

Major Factors that Impact on Deliverability

1. Sender Reputation

In the not-too-distant past, the primary driver that determined whether ISPs would accept and deliver emails was the content of the email, and email marketers were very careful to ensure that their emails did not contain any of the trigger words that would cause them to run foul of these content-based filters.

More recently, however, this scenario has changed with the primary current consideration being that of sender reputation. This is something akin to a credit score for email broadcasters, and is informed by a range of factors such as the volume of email that a sender broadcasts, the number of bounce-backs that they generate as a result of rejects and/or unknown users, and the number of spam complaint notifications that they receive.

In a recent study¹ by Return Path (a leading global provider of sender reputation data), it was found that approximately 80% of email delivery problems are directly attributable to a poor sender reputation. It is therefore vital for email marketers to know what their reputation scores are, and to take remedial action if those scores are poor.

Sender reputation data can be used by ISPs in a variety of different ways:

- whether to simply accept or reject email traffic
- to determine what level of volume throttling (see section 4) to apply
- in conjunction with other approaches such as spam filtering, authentication, etc.

It is easy to find out what score is currently being achieved by your email marketing activity (provided that you are generating sufficient levels of activity to register with the monitoring companies). Simply take the IP address that the email activity is being sent from, and use one of several publicly available websites (links at the end of this document) and run a lookup against that address.

It should also be mentioned that sender reputation is not necessarily IP address-specific. Increasingly, metrics are being managed at domain level, placing an onus on broadcasters to move away from operating 'good' and 'bad' IP addresses.

Most of the sites will also provide useful information into some of the key metrics that are used to calculate the reputation scores. In this way, you can identify where your email programme is falling short, and take appropriate action to rectify those shortcomings.

A key point is that responsibility for sender reputation rests with several different parties. Marketers cannot abdicate responsibility for sender reputation to their technology partners, and the reverse holds equally true. While an Email Service Provider (ESP) will be responsible for aspects such as infrastructure, bounce handling and ISP relationship

management, the marketer will control how the data is being collected, frequency of contact, quality of targeting, and so on. All of these factors affect sender reputation, and both parties have vital roles to fulfil in this regard.

1. See http://www.returnpath.net/resources/archives/ResenderStudy_101206.pdf

2. Spam Filtering

There are a variety of spam filter solutions in the market place, and they operate at a number of different levels:

- desktop client filters
- server filters
- gateway filters

Some of the best known spam filter providers include:

- McAfee
- BrightMail
- Cloudmark
- MessageLabs
- Postini
- Spam Assassin
- IronPort
- Barracuda

These filters adopt a range of different approaches to the way that they process emails. Some of the most common approaches include:

- **Bayesian Filtering:** Particular words and sentences have particular probabilities of occurring in spam email and in legitimate email. These filters learn to predict emails to be spam based on the probability of appearance of different word combinations.
- **Fingerprinting:** This process calculates a checksum that uniquely identifies an email for use in spotting duplicate messages. A checksum is an automated routine that uniquely identifies an email, for use in spotting duplicate messages (or near-duplicate messages – which is how bulk broadcasts of marketing emails are often viewed by the parties who receive and process them). The checksum is computed by evaluating the email's content, and is usually based on: the Message-ID: header; or if it doesn't exist, on the Date:; From:; To: and Cc: headers together; or if those don't exist, on the body of the message.

- **Heuristic Filtering:** Works by subjecting email messages through thousands of pre-defined rules against the message envelope, header and content. Each rule assigns a numerical score to the probability of the message being spam. The result of the final equation is known as the Spam Score.

3. Blacklist Operators

Blacklists contain records of e-marketing activity that has been identified as spam-like in nature. ISPs, spam filter vendors and domain administrators will use this information as a guideline to determine whether they will process or reject incoming emails.

The ways in which an email sender can become blacklisted take several different forms:

- RBL (Real-time Black List)
- DNSBL (Domain Name Server Black List)
- SURBL (Spam URL Real-time Blocklists)

In some cases the email sender can be reported directly to the blacklist operator. Alternatively, the blacklist can be managed independently of consumer feedback, with the lists being populated on the basis of the operator's own observations and expertise.

Some of the better known blacklist operators include:

- Spamhaus
- Spamcop
- MAPS (Mail Abuse Prevention System)

There are a number of web-based tools which an email broadcaster can use to identify whether their email traffic is being blacklisted. Should blacklisting be identified, point 7 (Blacklists) of the next section provides some tips on how to get the listing lifted.

Broadcasters should be aware that these operators also make use of their own spamtraps¹. This places a premium in terms of ensuring that best practices are applied to the way that email addresses are sourced (see next section – 'Improve Data Collection') so that email broadcasters do not get blocked as a result of broadcasting to spam trap addresses.

1. Spamtraps are usually email addresses that are created not for communication, but rather to lure spam. In order to prevent legitimate email from being invited, the email address will typically only be published in a location hidden from view such that an automated email address harvester (used by spammers) can find the email address, but no sender would be encouraged to send messages to the email address for any legitimate purpose. Since no email is solicited by the owner of this spam trap email address, any email messages sent to this address are immediately considered unsolicited. (Wikipedia).

Ten Steps to Improved Deliverability

1. Improve Data Collection

With the rapid rise in the importance of sender reputation, the quality of the email address data that is being used is absolutely vital. For this reason there are several actions that an email marketer should take at the point of data collection that will improve deliverability on an ongoing basis:

- Strengthen the permissioning mechanism: There is a proven relationship between the permissioning mechanism that is used to sign up the new member and their responsiveness. Positive opt-in (where the box is unchecked) is preferable to passive opt-in (where the box is pre-checked). Remember that a pre-checked opt-in box on its own cannot amount to consent to receive unsolicited commercial email under UK and European legislation. Double opt-in (where a confirmation email with a link to activate the registration) is preferable to single opt-in. Bear in mind that this is a best practice recommendation and not a legal requirement – although preferable to a single opt-in, a double opt-in is not required by law. Go for the strongest mechanism that your programme will support.
- Double entry of the email address: Many incorrect email addresses are simply the result of a ‘finger fumble’ as the email is being typed in. This can be overcome by requesting the double entry of the address, with the two fields being cross-referenced against each other – it is highly unlikely that the same mistake will be made twice. This also eliminates a potential source of spam traps, as some ISPs track common mis-spellings (‘hotmial’ instead of ‘hotmail’, for example) as a means of tracking whether or not appropriate list hygiene is being maintained.
- Send a validation email: Even if double opt-in is not being used as the permissioning mechanism, it is good practice to generate a confirmation or welcome email. This has some useful side benefits:
 - immediate validation of the new email address
 - opportunity to positively reinforce the initial brand experience
 - request to be added to the trusted senders list
 - apply progressive registration approach to learn more about the new member

The subject of data collection is dealt with in greater detail in the Email Marketing Council’s ‘Email Marketing Best Practice Guidelines’ document. See ‘*Further Reading and Useful Resources*’ for additional information.

2. Implement Authentication

With the explosion of ‘phishing’ emails (where a spammer adopts the identity of a legitimate domain owner), it is essential for the various parties who process emails to have a mechanism that proves that the email really has been sent by the party that it is claiming to originate from.

Responsibility for authentication will depend on if the sender is using an ESP, or relying on its own email broadcasting infrastructure.

There are several approaches that an e-marketer needs to be taking to satisfy this requirement:

- Register a sub-domain specifically for the email activity. There are several benefits to be obtained from doing this:
 - the sub-domain can be linked to the broadcast server for SPF / Sender-ID needs
 - generates increased recognition as users become familiar with the sub-domain
 - can be added to the recipient’s trusted senders list
 - increased importance of domain-specific sender reputation monitoring
- Make sure that a Sender-ID or Sender Policy Framework (SPF) record is in place. This enables the receiving email server to carry out a lookup that validates whether or not the domain name that the email claims to represent is associated with the IP address that the email has been broadcast from. If this test fails, then the email may be rejected. There are several good links that can be used to assist this process, which can be found in the further reading and useful links.
- Make sure that Domain Keys Identified Mail (DKIM) is being utilised. This approach builds on Sender-ID / SPF (which validate the email’s delivery path) by going one step further and authenticating each email message. This is done by including a signature key which is generated by the sender and included within the email header. The receiving email server will accept the email if it can successfully decode the key. This approach is popular with major ISPs such as Yahoo!, and is also now a mandatory requirement for Return Path certification (see part 10).

3. Monitor Your Sender Reputation

Sender reputation is the single most important factor used to determine email acceptance by ISPs. A sender’s reputation is monitored by a variety of factors and is linked either to the domain or the IP address from which the emails are sent or a combination of both.

ISPs often use external companies to provide sender reputation data so that they can screen emails against it. Many of these suppliers of sender reputation offer lookup facilities

where users can enter an IP address and get a free report of their current sender reputation status. Sender Score (operated by Return Path – www.senderscore.org) and Senderbase (operated by Cisco systems – www.senderbase.org) are two of the better-known sites.

Typically, these sites will provide a high-level classification of how the email traffic originating from that IP address is currently ranked. In the case of Sender Score, this is on a scale of 0-100 (with 100 being a best case scenario), while in the case of Senderbase it's a traffic light-style system – good, neutral or poor.

Users will also receive additional information on some of the key metrics that are being used to calculate the overall reputation score. These can include:

- broadcast volumes: ISPs typically like to see 'smoothed' broadcast activity rather than 'spikes'. If possible, spread activity over a wider broadcast window to achieve this
- spam complaint notifications: Most ISPs operate spam complaint thresholds (typically between two to three complaints per thousand emails processed) with blocking becoming effective if these thresholds are exceeded. See point 6 (Feedback Loops) and Point 8 (Spam Complaints) for additional information
- bounce-back activity generated: Similarly, high levels of email delivery failure will also contribute to a poor reputation score. See point 5 (List Hygiene)
- spam trap activity: These take two forms. Spam traps are email addresses that have been deliberately made available so that ISPs can track broadcasters who are using lists that have not been correctly permissioned. They can also be used to track recency; if an email address has been dormant for a long time, it may be co-opted and monitored on the premise that it should be de-selected if it is no longer active. See point 5 (List Hygiene)
- blacklisting. This is a double-edged sword. Poor performance in the context of one or more of the metrics outlined above will be likely to result in one or more blacklisting. And once listed, there will obviously be negative implications for email deliverability. Point 7 (Blacklists) covers this subject in more detail

4. Manage Your IP Addresses Carefully

As has already been explained in this document, sender reputation is an important concept for large volume email broadcasters (i.e. more than 100K emails per month). IP addresses used to send emails play an important role in determining a sender's reputation and therefore should be carefully managed.

Marketers who are broadcasting their emails through ESPs should be careful to understand what practices are being used to broadcast their emails. In some cases, senders will find that they are sharing IP addresses with other senders, in other cases they might be offered their own IP addresses. There is no right or wrong solution as different senders might

benefit from different set-ups. When an ESP is using IP addresses shared across multiple clients, it's worth checking how carefully the IP addresses are monitored; if there are any acceptance levels in place to ensure only good senders are using those IP addresses, and who is responsible for monitoring those IP addresses. Equally senders, who prefer not to share IP addresses (and therefore reputation) with other senders, should take care to ensure that their own reputation is sufficient to ensure good delivery.

Particular care should be taken if a sender deploys a new IP address as (initially, at least) it does not have a reputation score associated with it. The score builds as activity is tracked and metrics constructed. It is commonly held that the only thing worse than a poor reputation score is to have no reputation score at all. ISPs don't like surprises, and to be hit with a large tranche of email volume from a previously unknown IP address is almost certainly going to result in the broadcast getting blocked by one or more of the major ISPs. Senders who will only ever broadcast small volumes would generally be better served by a shared IP range where the volume is sufficient to gain a sending reputation.

For this reason, it is therefore important to 'warm up' a new IP address. Some of the activities that can be used as part of this process include:

- authentication: Make sure that all of the steps outlined in point 2 (Authentication) have been implemented
- throttling: Most email broadcast software now has the ability to 'throttle' broadcasts, i.e. to restrict the number of emails sent to X thousand per hour. Initially, traffic being sent from a new IP address should be restricted to no more than a few thousand per hour. This figure can then be increased as the reputation score builds.
- Throttling can also be applied for individual ISPs. Several have a stated policy whereby the volume of email that they will process per hour is a direct function of the reputation score that is associated with the originating IP address
- clean addresses: If email addresses have been obtained from one or more data sources, or if it is possible to sort the addresses as a function of recency, then it makes a lot of sense to prioritise the broadcasting of the addresses that are least likely to complain, bounce back, contain spam traps, etc.
- So, if one source uses passive single opt-in while another source uses double opt-in to collect its addresses, broadcast the double opt-in ones first. Similarly, addresses that have shown signs of life within the past 90 days are going to be more responsive than those that have been dormant for a year or more. Bear in mind that this is a best practice recommendation and not a legal requirement – although preferable to a single opt-in, a double opt-in is not required by law.

5. Practice Good List Hygiene

Good list hygiene is vital to the successful deliverability of an email campaign. To optimise list hygiene, a sender should consider the following points:

- data audit: Before the list is sent for the first time it should be screened to eliminate poor addresses. These could include:
 - duplicate addresses
 - known previous bounce back records
 - invalid structure (no “@” sign etc.)
 - junk entries (dfgdfgdfg@dfg.hj)
 - common mis-spellings (“hotmial” instead of “hotmail”)
 - profanities
 - potential harvested addresses (“sales@”, “info@”, etc.)
 - foreign addresses (not incorrect, but potentially no relevance to local campaign)
- bounce back management programme: A rigorous programme to remove emails that generate bounce-back notifications should be implemented. Hard bounces (i.e. indicating permanent conditions) should ideally be removed with immediate effect. However, because some hard bounce notifications are in fact false positives, DMA best practice guidelines recommend using two to three hard bounce notifications as the recommended number before any action is taken
- soft bounces usually indicate temporary conditions, but should be removed if they continually fail to achieve successful delivery. For example, an address will be removed from selection if it generates five or more soft bounce notifications over a 28-day period. This may change depending on circumstances; for an academic institution there could be a 60-day period to account for the summer holidays!
- spam traps: These have been highlighted in point 3 (Sender Reputation). They are tricky to identify as ISPs will never identify the actual spam trap address – that would be like gold dust for the spamming community!

Instead, broadcasters and their clients should be adopting best practice standards in terms of how their data is being sourced, and using recency as a selection criterion. A good rule to observe is that spam traps never respond. They will not generate an open or a click-through response.

Broadcasters should also sign up with programmes such as Microsoft’s Junk Mail Reporting programmes, which will provide reporting on a 12-hourly basis of email activity containing spam traps. While it is not possible to identify the actual address, segmentations can then be introduced to quarantine the address.

6. Use Complaint Feedback Loops

Complaint Feedback Loops (CFLs) have been in existence for a number of years. They enable email senders to retrieve details of recipients who have complained (complainers) with their ISP or webmail provider when receiving the sender's email. Currently amongst others AOL, Yahoo and Hotmail all operate a complaint feedback loop programme.

Typically complainers are identified through the webmail programmes of the ISPs as those recipients who click the 'This is spam' button (or similar). The CFL provides the sender with the email addresses of the complainers so that they can exclude (unsubscribe) them from further mailings. They provide a key advantage to email marketers who wish to keep their list clean and avoid continuing to send to people who don't wish to receive their email programmes, yet don't take the time to unsubscribe.

CFLs are normally free to sign up for. The sender has to contact each of the ISPs, provide technical details about their sending systems. Once active, a daily feed of complaining emails will be sent back and can be excluded.

If you are sending your marketing emails through an ESP, then they would normally need to set these up for you. In many cases they would automatically do this for you, but it is something that you should check with them.

7. Monitor Blacklists

Blacklists, sometimes known as Domain Name Server-based Black Lists (DNSBL), or Real-time Black Lists (RBL), are lists of IP addresses and/or domain information of senders who appear to be sending spam or unwanted email. They are compiled by a variety of organisations ranging from charitable organisations that campaign against spam, to commercial ISPs who keep their own lists to block unwanted mail. Many of these blacklists are made public and can be referenced by any organisation wishing to filter spam from their email traffic.

In simple terms, once a sender's information is listed on a blacklist email will not be delivered if a receiver is referring to that blacklist when filtering inbound emails. There are several hundred blacklists in existence, although some are more influential than others and the impact of being listed is very much determined by the list upon which the sender finds himself. There are between five and ten very important blacklists which are referenced around the world by many different organisations and spam filters. Links to these companies can be found in the '*Further Reading and Useful Links*' section.

Senders who find themselves listed on these critical blacklists will have severe delivery issues in many places. Any sender experiencing delivery problems would be well advised to check in the first instance to indentify if they are being listed on any of the major blacklists. There are a number of websites (see list of Blacklist Operators in the '*Further Reading and*

Useful Links' section at the end of the document) which provide a fast way to check if a listing appears.

Once a sender has determined that a listing has occurred then it will be necessary to contact the blacklist owner and try to get the listing removed. Each of the blacklist owners will typically provide information on their site to describe the 'de-listing process'. Senders using an ESP to manage their email broadcasting would require the ESP to handle this process. The blacklist owners will often seek reassurance that the infringement (cited as the reason for creating the listing) doesn't happen again. That might require the sender to provide evidence of good practice or simply be based on the acceptance of trust and assurance that no further infringements happen. Repeat offenders will find the blacklist owners very reluctant to remove the listing, and rightly so.

8. Reduce Spam Complaints

Spam complaints as described in section 6 above can have a very big impact on the delivery rates a sender achieves. Most ISPs and webmail providers base their spam filtering decisions to some extent upon the number of spam complaints seen from that sender. If a list owner or sender has an unusually high complaint rate (percentage of emails received by the ISP that are clicked as 'this is spam') they will start to consider emails from that sender as high risk, which in turn may lead to blockages.

There are many reasons why recipients would decide to mark your email as spam (complain):

- they didn't subscribe (i.e. you made a mistake in who you sent the message to)
- they didn't recognise you as the sender
- you simply send too many emails - they weren't expecting your emails so frequently
- the information in your emails isn't interesting or relevant to them
- the unsubscribe mechanism is not easy to use – it's quicker to click 'this is spam' than unsubscribe
- they forgot that they signed up

There are two ways in which senders can reduce spam complaints:

a. Reactive approach

If you have feedback loops in place, then complainers will be removed from your list over time. This approach will only work for certain ISPs and will do nothing to help reduce complaints where no feedback loop is in place. It may also be too late to avoid blockages occurring if you rely on feedback loops to reduce your complaints and complainers.

b. Proactive approach

A far more effective way to reduce complaints is to proactively take steps to avoid the complaints in the first place. The following tactics can all help to ensure the complaints are kept to a minimum:

- clear and easy to understand opt-in mechanism using double opt-in or confirmed opt-in methods for collecting email addresses
- clear and simple method for opting-out, e.g. easily visible unsubscribe link, no small print or confusing language
- an active reply address that goes to a monitored inbox so people who reply asking to be removed can be heard
- manage expectations: make clear to your recipients when registering what you plan to send to them, how often, etc.
- reduce your send frequency. Too many emails can cause people to become frustrated
- give people choice. Offering recipients the chance to tell you their preferences can dramatically reduce complaints

9. Conduct Pre-Broadcast Testing

In all aspects of email marketing it is a good idea to test. This is also true when trying to avoid delivery issues. Testing before sending with major ISPs will help spot any content-related issues before the broadcast. Other factors, not necessarily related to delivery, can also be checked at the same time. For example, different webmail programmes can display emails in different ways. Testing this to ensure your message render correctly is always a good idea.

Many delivery issues can occur after a message has been sent or part way through the broadcast. For this reason it is a good idea to monitor the percentage of messages which are being delivered into the inbox versus the junk folder with the major ISPs.

There are a number of tools available through ESPs and delivery specialists such as Return Path and Pivotal Veracity, which check this for you. They work by seeding campaigns with a large number of sample addresses for each ISP and then automatically login and check whether they were delivered or not.

Using these results the tools can provide an estimation of the 'Inbox placement rate' or 'ISP acceptance rate' (not to be confused with delivered rate). By monitoring your inbox delivery rate you can quickly spot when blockages might have occurred.

10. Get Certification

There are a number of certification schemes in operation which allow a sender to bypass spam filters. They all operate through a process of the sender paying a fee and a verification process in order to certify that they are a good sender and follow best practice methods for sending bulk email communications. Once the certification is in place the senders can benefit by bypassing the spam filters as well as having images readily available for users to see without the need for downloading. There are two main certification programmes currently available. Return Path Certification (formerly bonded sender programme) is offered by Return Path and Certified Email by Goodmail Systems.

Return Path Certification is the scheme operated by Return Path, which doesn't charge users a per email fee but does involve an annual subscription fee. The scheme works by a process of verification to ensure the sender's practices are of a high enough standard to be certified a good sender. Once accepted on to the scheme the sender is then white-listed with all of the participating ISPs and domains including Hotmail and Yahoo.

Certified Email by Goodmail works through a process of the sender paying an additional price per email (1/4 cent USD) to bypass the spam filters of participating ISPs. At present, Certified Email has been adopted by a number of the major US ISPs, including AOL and Yahoo, which directly affect a large percentage of UK email lists.

Further Reading and Useful Links

The following section provides a list of useful documentation and website links that readers can follow for further information on the points that have been dealt with above.

Blacklist Operators

<u>Resource</u>	<u>Link</u>
• Spamcop	www.spamcop.net
• Spamhaus	www.spamhaus.org
• MAPS	www.mail-abuse.com

Authentication

<u>Resource</u>	<u>Link</u>
• Microsoft	www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard/
• Open SPF	www.openspf.org
• DKIM	www.dkim.org

Improve Data Collection

<u>Resource</u>	<u>Link</u>
• DMA Email Marketing Council Best Practice Guidelines (June 2007)	http://www.dma.org.uk/_attachments/resources/230_S4.pdf

Conduct Pre-Broadcast Testing

<u>Resource</u>	<u>Link</u>
• Return Path	http://www.returnpath.net/commercialsender/monitoring
• Pivotal Veracity	http://www.alterian.com/pdf/Pivotal_Veracity_UK_061109.pdf

Get Certification

<u>Resource</u>	<u>Link</u>
• Return Path	http://www.returnpath.net
• Return Path Certification	http://www.returnpath.net/commercialsender/certification
• Goodmail	http://www.goodmailsystems.com
• Certified Email by Goodmail	http://www.certifiedemail.net

General Resources

<u>Resource</u>	<u>Link</u>
• Email Marketing Council blog	http://www.spamcop.net
• Messaging Anti-Abuse Working Group	http://www.maawg.org
• Deliverability.com	http://blog.deliverability.com