

Under the skin of email deliverability

March 2011

Contents

About this document

Executive summary

.....

Steps to improve deliverability

- Spam complaints.....8
 - Use a dedicated IP address.....8-9
 - Build your reputation slowly9
 - Content 10-11
 - Frequency of message 12
 - Data Hygiene..... 13-15
 - Blacklists 16
 - Authentication 17
 - Monitor..... 18
-

Further reading and useful links

About this document

Email deliverability is a hugely complicated topic.
It's a subject that is pretty complex and can fill many with fear and dread.

However, despite there being numerous documents on the subject in the marketplace, they are generally highly technical and aren't necessarily marketing-friendly. My intention with this paper is to produce a document for the marketing professional who has a limited understanding of technical jargon.

About the author

"I've worked at Red C Marketing for 5 years and have managed email programmes for a whole host of different clients from a number of differing sectors including home shopping, retail and insurance."

Steve White (Account Director)



Executive Summary

When I first arrived in the industry 5 years ago, the issue of email deliverability was a relatively simple one. If you managed to avoid *spam* words such as 'Free' and 'Sale' then you could generally guarantee a delivered message. However, over the course of the last 5 years, the measures and factors that influence email deliverability have changed significantly... and they continue to do so.

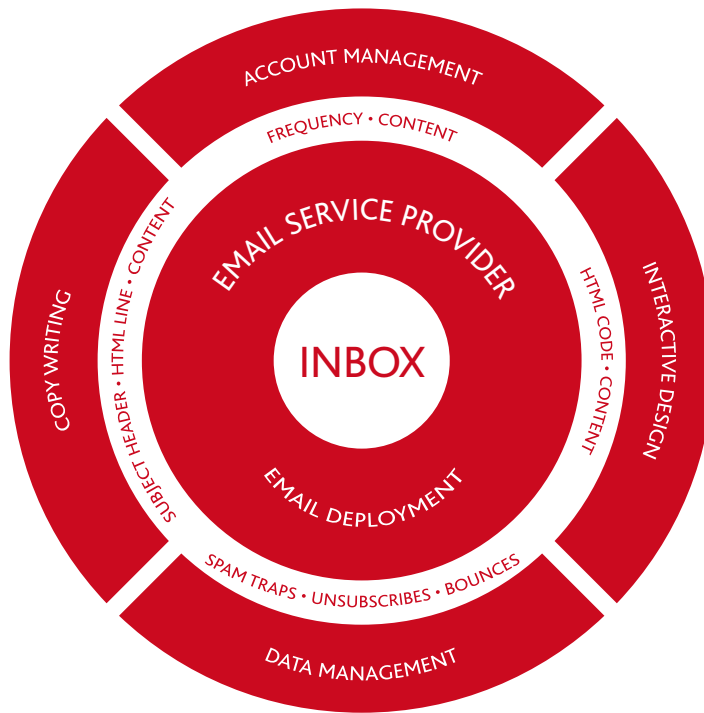
The primary reason for this change is the massive volume of spam that Internet Service Providers (ISPs) have to deal with on a daily basis. According to the most recent McAfee Quarterly Threat Report⁽¹⁾, there are approximately 130 billion spam messages broadcast every day. The difficulty for ISPs is that they have to try and identify and eliminate this spam activity without damaging permitted email broadcasts.

When 90% of all email is spam then they really do have quite a job on their hands if they want to keep one step ahead of the spammers. If there is any doubt as to the legitimacy of your email messages then you are going to be treated as spam. You can't blame them can you?

In today's email marketing landscape the key factor that determines whether or not your email messages reach their intended target is your 'Sender Reputation'. Like a credit score, your sender reputation is an indication of the trustworthiness of your email source. Your reputation is determined by several factors such as the volume of email, the number of complaints you receive and the number of bouncebacks.

I have outlined a number of 'must-dos' that if applied should go a long way to improving your email deliverability. However, these simple steps require the support and co-operation of all the departments involved with your email programme; the IT department, your designer, your copywriting team, your data department and the marketing department. They should all be accountable for your email deliverability record. Your email service provider (ESP) should then be tasked with monitoring your reputation and deliverability ratings.

THE EMAIL DELIVERABILITY HUB:



The 'must-do' steps

1 SPAM COMPLAINTS

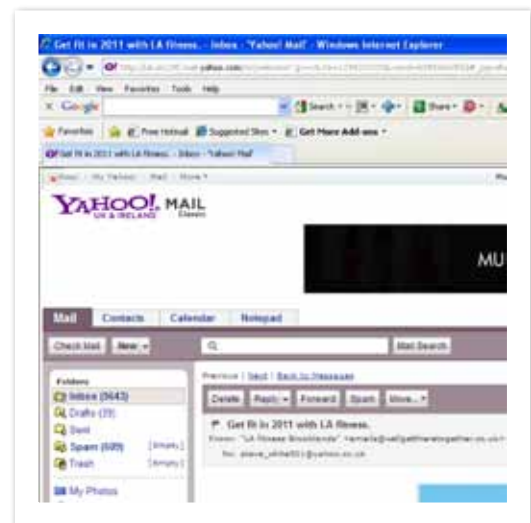
Your 'sender reputation' is greatly influenced by spam complaints; so much so that this alone can determine whether your email message is delivered or not.

The number of complaints it takes to affect the reputation of an IP address is a closely guarded secret, as is the frequency in which ISPs change these rules. However, America Online recommends that you should be looking to keep complaints below one per 1,000 delivered messages. If you were to exceed this amount, and ignoring other factors, you could be looking at your emails either being filtered or blocked altogether.

Throughout this document I detail several reasons as to why recipients of your email programme might feel the need to mark your email as 'junk' and recommend ways in which you can avoid this unwanted action happening to your email programme.



Hotmail: You can mark your emails as junk or even as unsafe.



Yahoo: You can mark your emails as spam.

2 USE A DEDICATED IP ADDRESS

ReturnPath have reported that 77% of delivery problems were based on reputation⁽²⁾. So, given the importance of reputation, I would advise that the necessary investment is made to ensure that your reputation is solid.

A costly but, in my view, vital step for ensuring that your reputation is of a good standard is to refrain from sharing an IP address across multiple brands and/or departments. When you share an IP address with other departments you are then relying on them to deploy the highest standard of best practice. If other departments were to fall foul of an ISP then the consequences would not only be dire for the perpetrator/s but you would also suffer the same consequences, such as having your emails junked, filtered or blocked.

By having your own IP address you are solely responsible for your own destiny and you're not relying on other departments to showcase those same levels of best practice.

2.1 BUILD YOUR REPUTATION GRADUALLY

Your sender reputation is not transferable, if you have had a fantastic reputation in the past that counts for nothing when you start afresh with a new IP address.

If you find yourself with a new IP address not to try too much too soon, as ISPs prefer for 'new' reputations to be built gradually over time. This can be achieved by sending small batches of emails and gradually building the distribution volume up over the course of three to four weeks.

⁽²⁾ ReturnPath: Content secondary factor when email gets clocked or junked (2006)

The 'must-do' steps (continued)

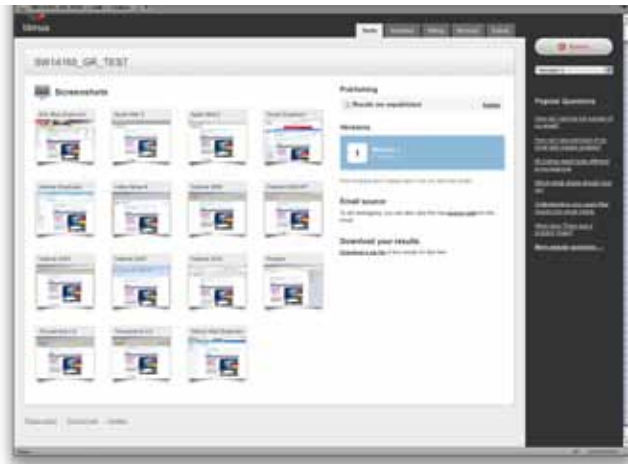
3 CONTENT

Although email content isn't regarded as being as influential as it once was, it is still very much a factor that needs to be considered and closely monitored ⁽³⁾.

Spam filters monitor email content for incorrect or non-standard code, spammy content and a whole host of other factors. Emails are in fact given scores by ISPs and it is believed by many that if you have scored 4 points or more then you stand a good chance that your message will be junked, blocked or delayed ⁽⁴⁾.

There are many ways of checking your email templates before distribution:

- You can check how your email renders by sending it through an HTML validator or spam content checker such as Litmus (see below) or Campaign Monitor.



Use Litmus to check how your email renders.

- It is also recommended you view your emails on a number of differing web browsers, i.e. Google Chrome, Firefox, Internet Explorer.
- I'd advise you set up 'dummy' email accounts with Hotmail, Gmail, Live, Yahoo etc..., so you can closely monitor first-hand how your email messages render.

If you are experiencing problems with how your emails are rendering then you should look at the way in which you build your emails. For example, if your email is being designed with the assistance of a design programme such as Dreamweaver or Frontpage then your email might contain 'dirty' html code, which will almost certainly be causing you problems. Why not build your emails by hand without the support from such programmes.

It is estimated that 50% of consumers have their images turned off by default so it is recommended that you don't design your messages with an over-reliance on images. The image/HTML ratio should be considered carefully from a deliverability perspective but equally it should be implemented from a customer experience point of view. If customers are struggling to view your emails content then they may well 'unsubscribe' or even click 'spam complaints'.

Be careful when structuring your subject headers as overly aggressive messages could generate a high complaint rate. Avoid all-caps, exclamation marks and what might be regarded as 'spammy' words. Consider using your brand name in your subject header as it's recognisable to the consumer and therefore generates consumer confidence.

Another key point when it comes to content is its relevancy. It is dangerous for businesses and retailers to take their subscribed email list for granted by sending messages that they haven't necessarily subscribed to. For example, if a customer has subscribed to a fashion related email programme but they then begin receiving emails promoting financial services - this course of action could lead to an increased complaint rate. Do not to partake in sharing data across differing brands as although this might be viewed within a business as being an effective method of stretching resources it could be viewed by a customer as being very confusing and again could trigger a complaint.

(3) "DMA; Deliverability White Paper Review"

(4) "Silverpop; Email Delivery Rates above 95%: 16 "Must do" to make it happen, 2009".

The 'must-do' steps (continued)

4 FREQUENCY OF MESSAGE

Establishing the right frequency of marketing message has always been an issue that has generated much debate amongst email marketers. Given the relatively low costs associated with email and the relative ease of email production there has always been the temptation to “blast” customers with messages as often as possible.

Although I don't advocate a haphazard “blast” approach I do believe that email frequency should be pushed as high as possible. The decision on how frequent you should be emailing your customers should be based on several factors such as the relationship you have with the customer, seasonality, product range, email content and your sign up promise.

If you do decide test the frequency in which you contact your customers then it is absolutely critical that your open, click, unsubscription and complaint rates are monitored rigorously. If your email programme does experience an increase in unsubscribes or complaints then it is a fair assumption that you are contacting your customer too frequently.

I would also advise that if you were to test your frequency levels, which I very much recommend you do, then you don't make radical changes immediately and instead you ramp up the frequency slowly. According to a JupiterResearch study (5), 40% of consumers unsubscribe from email programmes because “emails are sent too often”. This is quite a damning statistic, especially given that 26% of consumers unsubscribe by clicking the 'report spam' button, due to not trusting the 'unsubscribe' link. This will ultimately lead to an increase in spam complaints, therefore your frequency of message needs to be monitored closely.

5 DATA HYGIENE

Good list hygiene is absolutely crucial as a 'dirty' list will undoubtedly cause you significant problems when it comes to your sender reputation and, ultimately, your email deliverability.

DATA AUDITS

It is certainly good practice for your data list to be screened on a regular basis to identify poor data and it's a good idea to screen your list prior to it being used for the first time.

Things to look out for:

- Duplicate addresses
- Junk entries (qwertyuiop@asdfg.hj)
- Common mis-spellings ("hotmial" instead of "hotmail")
- Irrelevant addresses (foreign addresses for a UK campaign)

The quality of your data can often be improved at the source by introducing a double opt in function, as this will almost certainly eradicate mis-spelling or mistakes when email addresses are being inputted.

The 'must-do' steps (continued)

5 DATA HYGIENE (CONTINUED)

BOUNCEBACK RATES

It is recommended that a bounceback management process be introduced to any email programme. This will identify and process any email addresses that soft or hard bounce.



Deliveries		
Sent:		64
Delivered:		50 (78.1%)
Undeliverable:		14 (21.9%)
Hard (Permanent) Bounce:		12 (18.8%)
Bad Email Address:		6 (9.4%)
Destination System Unreachable:		6 (9.4%)
Rejected Due To Message Content:		0 (0.0%)
Soft (Temporary) Bounce:		2 (3.1%)
Temporary Contact Issue:		0 (0.0%)
Destination System Temporarily Unreachable:		2 (3.1%)
Deferred Due To Message Content:		0 (0.0%)
Unclassified:		0 (0.0%)

If you experience a hard bounce (i.e. failed delivery of an email due to a permanent reason) then they should be removed from your data list as soon as they are identified.

However, a more relaxed approach should be applied when dealing with soft bounces as immediate expulsion is too severe, given the possible reasons for a soft bounce (bounces back due to a fault or unavailability of space in the user's inbox). For example, you may decide that you remove an address after it has received five soft bounceback notifications over the course of a 60 day period.

SPAM TRAPS

Spam traps are email addresses that have been created or re-activated not for communication but to lure spam. They are to be avoided at all costs, as if you fall foul; it's a clear indication that you are managing your data in an inappropriate fashion.

There are two types of spam traps that are to be avoided:

1. Honey pots

Spammers often look to compile email lists by roaming the web looking for any email addresses that are listed on websites. If they find one, they copy the address and put it on their list. This process is known as email address harvesting and is usually automated using special 'address harvesting' software.

Some organisations involved in tackling spam put specific email addresses on a website for the sole purpose of attracting harvesting software.

These addresses are never used for any other purpose. They are merely listed on a web page in such a way that no human would ever discover them or seek to send an email to them. Any email sent to a 'honeypot' addresses must, by definition, be spam. The address owner never added the email voluntarily to any email list: they just put it up on a website. So it must have been harvested by a spammer and added without permission to a mailing list.

2. Dormant addresses

Email accounts often fall into disuse. They are abandoned by their owners or shut down - as a result the account is unable to receive email. Legitimate senders of email will stop sending messages to such addresses. They notice a dead address and remove it from their system. Spammers will just keep on sending regardless.

So some organisations (like webmail services) will take dead email accounts and, after a suitable period of time has elapsed, re-activate them for the purpose of trapping spammers.

Non-engagement

An area that is becoming more and more important is the issue of non-engagement. ISPs take a dim view of email broadcasters who persist in sending email messages to non-responding email addresses. It is recommended that a dedicated re-engagement programme be implemented to look at re-engaging email addresses that haven't opened an email for an agreed period.

It is not known what level of non-engagement triggers ISPs to act.

The 'must-do' steps (continued)

6 THE BLACKLIST

If you fall foul of spam traps or if ISPs receive complaints about your email programme you are then in real danger of being blacklisted. As the name suggests, a blacklist is a list or database of IP addresses that are viewed as being "spammers". The lists can be populated through consumer complaints but are just as likely to be populated independently of consumer feedback. ISPs subscribe to these blacklist databases in order to filter out spam sent across their network or to the subscribers.

There are hundreds of blacklists in operation but some are more influential than others. For example, Spamhaus, Spamcop and MAPS (Mail Abuse Prevention Centre) are all considered to be hugely influential and are used by the major ISPs.

It is increasingly easy to establish if you have fallen foul of an email blacklist as there are many websites that provide a quick way of checking if you have indeed been listed.

If you have been listed then it isn't necessarily the end for your email programme, as although it's clearly bad news the problem is rectifiable. It is possible to contact the blacklist owners to try and have the listing removed. Blacklist owners will generally provide information on their site to detail the 'de-listing process', but generally it will involve re-assurance that the offence won't happen again and evidence that a good level of best practice is being carried out in relation to the email programme.

7 AUTHENTICATION

Increasing numbers of spammers have been adopting the identities of legitimate domain owners in an attempt of getting their emails delivered to their intended targets. Therefore, it is essential for the various parties who partake in email distribution to have a way of identifying whether the email has been sent by the party that it is claiming to be.

One way of ensuring that your emails are authenticated is to add some code within the email header. In basic terms it acts as a signature that aligns your email to your domain address. The name of this code is the Domain Keys Identified Mail (DKIM). Incorporating this code within your email template should see the ISP accept the email, if it can successfully identify the code as being legitimate.

Example;

DKIM-Signature: v=1; a=rsa-sha256; d=example.net; s=brisbane;

Another way of helping to ensure that your emails are authenticated is by running them through a validation system called a Sender ID /or Sender Policy Framework (SPF). In very basic terms a SPF allows you to form a record of hosts that are allowed to distribute emails from a particular domain.

Ensuring that your emails are authenticated via SPF and DKIM is generally the responsibility of your ESP.

The 'must-do' steps (continued)

8 MONITOR

ISPs are constantly reviewing their rules around deliverability as they have to keep one step ahead of the 'spammers'. It is therefore imperative that you are constantly monitoring your performance when it comes to your sender reputation and deliverability rates.

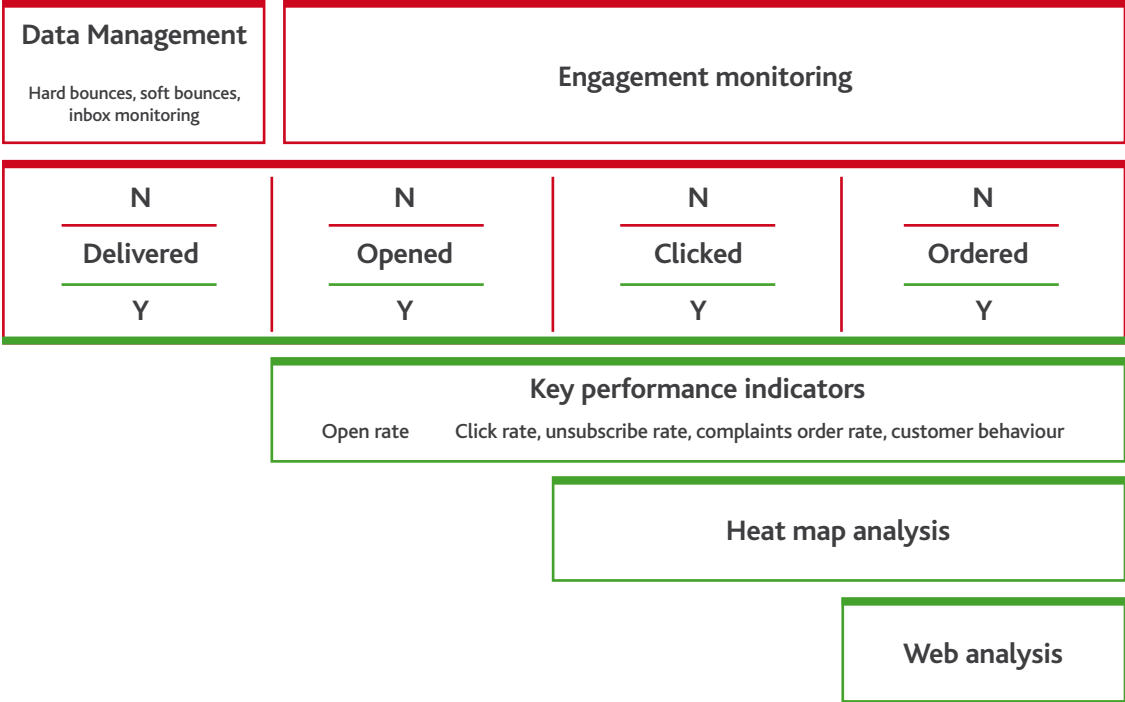
Keep track of the following performance indicators;

- Hard bounces
- Spam complaints
- Unsubscribes
- Blacklists that you've been added to
- Inbox delivery rate by ISP (i.e. Hotmail)

In addition it would also be advisable if you were able to track performance via email type (newsletter, promotional, services), timing (season, day of week), frequency (increased or decreased activity) and perhaps even content and style.

The monitoring of your email programme doesn't necessarily need to be something that you carry out in isolation as there are services available that can help with this process. Many ISPs use feedback loops, which are used to notify email senders when they hit an unknown complaint rate.

PERFORMANCE INDICATORS:



Summary

There is no doubt that the subject of email deliverability is one that requires a great degree of attention, as ISPs and their filters become more and more sophisticated in fighting the “good fight” against spammers. However, the good news is that you can control your email deliverability by investing the right amount of time and resource to its continued management.

Each of the factors that I have highlighted in this document all impact your reputation and ultimately your email deliverability, but it isn't known as to how these factors rank in importance. For example, is it more important to steer away from using spam words in your subject header than it is to limit your email interaction with non-engaged email addresses? No one knows, apart from the guardians of the inbox – the ISPs.

Further reading and useful links

Returnpath - www.returnpath.net

Goodmail - www.goodmailsystems.com

Email marketing Council blog - www.spammcop.net

Deliverability.com - www.blog.deliverability.com

MarketingSherpa - www.marketingsherpa.com



Red C, Anchorage 1, Anchorage Quay, Salford Quays, Manchester M50 3YL