



**Email Deliverability:
How We Got Here and
What Marketer's Should do About It**

Published by the Deliverability Hub of the Email Marketing Council of
the Direct Marketing Association (UK)

June 2007

Written By Skip Fidura, Warehouse Marketing
Edited By Darren Moore, BT
Matthew Simons, Acxiom Digital
Tink Taylor, dotMailer

Email Deliverability: How We Got Here and What Marketer's Should do About It

Introduction

The first step in any marketing campaign is getting the message to the consumer. Regardless of how good the copy and creative are and how compelling the offer is, a campaign will fail if your target audience never sees the message. In other marketing disciplines this step is taken for granted by the marketer. Booking a slot on television, buying space in a broadsheet, or dropping the mail pack into the post pretty much guarantees that the consumer will see it. This leaves marketers to apply their creative energies to ensuring that the consumer pays attention to the message through effective targeting, strong copywriting and compelling visuals.

Email marketers, on the other hand, do have to worry about getting their messages in front of the intended audience. Even if they get the message past the Spam filters, there is no guarantee that the message is going to be placed in the primary inbox nor is there a guarantee that the message will have the look and feel as the marketer intended.

This white paper will first look at why the ISPs block emails and the economic impact that it has on marketers. We will then examine the current methods for filtering and blocking emails and strategies to prevent being blocked and getting unblocked if that is necessary. Finally, we will look into the future for a glimpse of where this issue is heading.

What we will not be looking at here are the shades of grey in deliverability. For the purpose of this document (except where otherwise stated), we will define deliverability in terms of whether the email was accepted by the mail server or not. At the next level, deliverability can deal with what happens to the email after it has been accepted by the mail server - does it get delivered to the inbox or the bulk folder; do the images render; do the hyperlinks work; etc.

Why do ISPs block legitimate emails?

Email as we know it was invented in 1972 by Ray Tomlinson. Prior to this users could "send" emails to other users on the same computer (at this time computers were mainframes with multiple users sharing its relatively limited computing resources). Tomlinson recognized the need to be able to send messages to other mainframes connected to ARPANET (a network built to facilitate collaboration between researchers at various locations in the United States and the precursor to the internet). He picked the "@" to indicate when a message was to go to a user on another computer. The system developed by Tomlinson would evolve into Simple Message Transfer Protocol (SMTP) which is in use today.

Jon Postel, a contemporary of Tomlinson's, described this system as a "nice hack." Unfortunately email is still fundamentally built on this "nice hack," which has led to the deliverability problems we face today. ARPANET was a closed network used by universities, companies, and agencies doing research for the Advanced Research Projects Agency, which has variously come under the auspices of the United States Department of Defense. As such, there was no need to build into the system even the most cursory security checks to confirm that the email actually came from the sender. In most cases the recipient would know the sender and there was little or no

Email Deliverability: How We Got Here and What Marketer's Should do About It

benefit to be gained by spoofing¹ someone else's email address. Even if the designers of SMTP could have predicted the technological advancements that led to the PC revolution and the rise of the internet as a ubiquitous tool in our everyday lives, they didn't or chose not to act on this prediction. This oversight has allowed the rise of spammers, phishers² and virus spreaders.

Another distinguishing characteristic of email is its low cost of set-up and management. It is relatively simple to buy a server and configure it to send millions of emails per day. After that, all the spammer needs to do is maintain an internet account. If the cost of the server and the internet account are spread across millions of email addresses harvested by bots or gleaned from dictionary attacks³, the cost per contact is a fraction of pence. It takes very few conversions (whether that be selling dodgy Viagra or capturing personal banking details unwittingly given over by naive consumers) to make this venture wildly profitable. Combine this earnings potential with the ease in faking the source of the email and you have the perfect recipe for criminal activity.

Size of the Problem

The volume of spam is a global problem that impacts all email users. In January 2007 Postini estimated that 94% of all emails sent were Spam. It detected over 25 billion Spam emails in December 2006 - an increase of over 15 billion from the same month in 2005. This figure is higher than the 70% to 90% Spam figures that have been reported over the past few years. At the same time, MessageLabs reported that only 74.68% of emails sent in December were Spam. While these statistics are at odds with each other, the picture they paint is clear - Spam is a major problem.

It would be easy to pass off Spam as a victimless crime and to regard those who are taken in by dubious offers and unwittingly give over their personal banking details as people who should have known better. Spam and Phishing, however, are not victimless - there is a real cost related to these activities over and above those borne by those who have been misled.

If 80% of all email traffic is Spam, then the ISPs and Internet Email Providers (IEPs) such as Yahoo and Hotmail need to maintain 4X in extra hardware and processing capacity to handle this volume. Imagine having to own five cars because you had to plan to have four missing whenever you needed to go out.

These wasted costs are not limited to the large ISPs and IEPs, however, as corporations face a double whammy. First, they have to maintain the same level of excess capacity - because email has become such a mission critical tool for the modern business this is even more important than it is to the consumer ISPs and

¹ Spoofing is the practice of hiding the sender's real identity by making the email appear to come from a reputable source.

² Phishers are adept at making emails appear to be from reputable sources, such as a bank, the purpose of which is to defraud readers out of the personal banking or credit card details so they can gain access to these accounts.

³ Spammers use a variety of methods to harvest email addresses. One method uses a bot or spider, which is a program that works its way through the internet looking for email addresses. Another method is called a dictionary attack where the spammer uses software to try every combination of letters and numbers that could possibly be used at a domain.

Email Deliverability: How We Got Here and What Marketer's Should do About It

IEPs. Second, corporations face the hidden costs of lost productivity related to dealing with Spam - from employees having to filter these unwanted messages out of their inbox to the downtime that comes from virus attacks. A study released by Nucleus Research in May 2004 put this cost at \$1,934 per employee per year.

At this point we can see a business case developing that ISPs, IEPs and corporate domain owners need to do something to protect their organisations from the cost and security exposure stemming from all forms of Spam. In response to this threat, domain owners have started using various tools to block unsolicited commercial emails from entering their systems and forcing a class system on the emails they do accept by either labelling the messages as spam, filtering them into a special folder, such as the bulk mail folder, or limiting their functionality by blocking images or link destinations. It is not the intention of the ISPs however, to block commercial emails that have been requested by their users. They explain that any of these that are blocked are 'false positives' or emails that they would see as legitimate that are getting identified as spam and blocked in error. They further claim that these false positives are small in number, are an unfortunate by-product of the system and part of doing business for marketers.

Impact on the Marketer

There are some in the email marketing community, however, that argue that ISP/IEP blocking is systemic and more than just a few false positives. Everybody can see how a campaign or a mishandled list could cause a temporary block, but the fact that the bigger ESPs have been forced to hire whole departments to handle ISP/IEP relations is evidence to some that the ISPs/IEPs are taking things too far.

This argument may have some validity and it is important that the industry continue to work to build good relations with the ISPs and IEPs. All of this, however, is not going to do the marketer any good when they are sending out that all important campaign. What they need to know is how a block could affect the ROI on the campaign and whether the additional costs to remove the block are justified in this instance.

Cost of a Block

In its simplest form the cost of a block is calculated by multiplying the expected return per email delivered by the number of emails blocked. As shown below where total cost of the block is T_{CB} , the return per email is R_E and the number of emails blocked is B .

$$T_{CB} = R_E \times B$$

Depending on your program, R_E can be made up of lost revenue due to sales not being made or by additional cost associated with servicing customers through a more expensive channel. An example of this additional cost would be where a company includes tips and tricks, search our support, or FAQs in the email to avoid having the customer call the contact centre. A more mission critical example would be with order confirmations.

Email Deliverability: How We Got Here and What Marketer's Should do About It

While this certainly makes up the bulk of the costs it is not the whole cost associated with a block. There are both campaign related overheads and corporate overheads that should be factored in as well. The campaign related overheads include anything that was spent specifically for that campaign such as design and creative, data purchased, lost advertising revenue, cross charges paid to the internal data centre, etc. The corporate overheads would include primarily staff costs to run and support the campaign. These elements can be added to the original formula where C_{OH} is the total campaign overheads, T_{ES} is the total number of emails sent⁴ and C_{CH} is the total of the corporate overheads that can be applied to this campaign. So the expanded formula looks like:

$$T_{CB} = (R_E + ((C_{OH} + C_{CH}) / T_{ES})) \times B$$

The next element of cost would be the opportunity cost of any time needed to explain the issue to senior management and resolve if necessary. We will represent this as U . There are also costs that are much harder to quantify surrounding the damage to the brand resulting from your recipients not getting an email that they had requested. We are going to leave that element out as it would be almost impossible to calculate on a case by case basis. The final formula therefore looks like:

$$T_{CB} = (R_E + ((C_{OH} + C_{CH}) / T_{ES})) \times B + U$$

To look at this another way, the total cost of a block is calculated by adding the per email amounts for:

- the lost revenue
- the additional expense of servicing the customer through an alternate channel
- the wasted marketing and corporate overheads

This sum is then multiplied by the number of emails blocked. You then need to add in an amount to cover the time and hassle of explaining this to management.

Unblock or Not?

It turns out that it is the relationship between U and R_E that is critical in determining the marketer's response to a block. The rest of the equation is a sunk cost because the money has already been spent and cannot be recovered. Additionally, if R_E is not greater than $(C_{OH} + C_{CH}) / T_{ES}$ or the expected return per email does not exceed the costs of sending that email, then the campaign was a loser from the off. Consequently, the cost of sending the email has no bearing on the future decision.

Only if $R_E \times B$ is greater than U should the marketer work to resolve the block. In other words, the expected return per email times the number of emails blocked must be greater than the cost to explain the block to senior management and more importantly to resolve with the ISPs before the marketer lifts a finger to remove this block.

That said if the block remains we would have to look at the expected return across all future campaigns, which could dramatically change the equation. This discussion

⁴ Total emails sent is equal to the number of emails delivered plus the number of emails blocked.

Email Deliverability: How We Got Here and What Marketer's Should do About It

however, does highlight two important points. First, emails will get blocked and marketers need to take a deep breath and do some analysis before making an ultimately fruitless attempt to get all of their emails delivered.

Second, Spammers don't worry about getting blocked. They know that their U is going to be ridiculously high and they can mail to different addresses at other domains. Spammers need infinitesimal conversion rates to have a positive ROI. The unfortunate reality is that Spam works.

Methods for Blocking & Filtering Emails

So we know that emails are getting blocked and filtered but how do they do it? The most important thing to remember is that there is a hierarchy in how these methods and tools develop. The mail receivers will implement a new tool or technique and the spammers will quickly find another way around, which the receivers will work to head off. At the same time the average email marketer is months if not years behind this development curve.

Initially the receivers were trying everything they could think of and each developed their own processes. At the same time they also did not see any incentive to working with legitimate marketers to make sure opt-in emails were delivered to the consumers who had requested them.

In January 2003, a group of email service providers in the US came together forming the Email Service Providers Coalition with a view of putting a sensible plan forward as a starting point for discussions with the ISPs and IEPs. This plan was called Project Lumos and is built on four fundamentals:

- Authentication – Ensuring that the email is from who it appears to be from
- Reputation – Identifying whether the email sender follows recognised standards of behaviour
- Education – Changing consumer behaviour and attitudes towards email security
- Legal Reform – Changing the law to cover 21st century issues

It was never the intention of the ESPCC that Project Lumos would be adopted as proposed but they hoped that it would form a basis for dialogue with the ISPs and IEPs.

In this, Project Lumos was an unqualified success. The outcome was two different methods for authenticating senders and at least two major reputation services. It also positioned the ESPCC to have a big voice in lobbying the United States Congress for the Can-Spam Act of 2003.

DomainKeys

DomainKeys is one of the authentication systems developed and was originally designed by Mark Delaney of Yahoo! with high levels of collaboration from many other experts in the field. It adds a header to each email message called a domainkey-signature, which includes an encrypted code. It also includes a plain text code around the message body. The receiver uses information in the header to

Email Deliverability: How We Got Here and What Marketer's Should do About It

perform a DNS lookup⁵. From the DNS lookup the receiver gets the public key needed to decrypt the code in the header. If the decrypted header code matches the plain text code then the message is actually from the sender and has not been tampered with since leaving the sending server.

The benefits of this system include:

- The positive identification of the sending domain reduces the chance of false positives on both black lists and white lists. This positive identification of the sending domain virtually eliminates domain spoofing which is a key to Phishing attacks.
- Forged emails can be blocked before they enter the ISP, IEP or corporate domain, thereby reducing both the drain on bandwidth and the risk posed by the email.

Clearly this system will not eliminate spam or other abuse but it does allow the perpetrators to be tracked more easily. The other problem is that the plain text code can be corrupted by some email forwarding mechanisms.

Sender Id/Sender Policy Framework (SPF)

While the SPF concept was being presented in a 2002 paper titled "Repudiating Mail-From," written by Paul Vixie, and development had been started by Meng Weng Wong working with a large community of developers, another authentication system was developed. Sender ID was created by an industry working group that controversially added the third authentication framework, developed by Microsoft, called "Caller-Id". Because of the similarities in these systems and the politics surrounding these issues, they were combined.

This system allows a domain owner to identify which machines are authorized to send email with a return address to that domain in a special DNS record. For example should the DMA decide to implement SPF, they would use the special DNS record to identify which servers (using their IP addresses) are allowed to send emails with a DMA.org.uk reply address. If some other machine sends an email with a DMA.org.uk reply address, these messages can be blocked by receivers who check these SPF records.

Bonded Sender[®] and Sender Score Certified[®]

Both DomainKeys and Sender ID/SPF are forms of authentication; they allow the receiving domain to positively identify both the sending IP address and in the case of Sender ID/SPF ensure that the sending machine is authorised to send emails for that domain. What it does not do is give the recipient any idea of the reputation of the sender. Bonded Sender[®] was a program that was originally developed by IronPort[®] who signed a partnership with Return Path[®] in April 2005 to develop, operate and market the program.

⁵ DNS or domain naming service is the system that allows users to type in a URL and for their browser to direct them to the somewhat more cryptic IP address. Other information can also be stored in the DNS record which is used by a receiving email server to authenticate the sending server.

Email Deliverability: How We Got Here and What Marketer's Should do About It

The Bonded Sender® program was made up of two main elements: certification and a financial bond. The certification process is managed by TRUSTe® which describes itself on its website as an:

'independent, non-profit enabling trust based on privacy for personal information on the Internet. We certify and monitor web site privacy and email policies, monitor practices, and resolve thousands of consumer privacy problems every year.'

This certification ensures that the sender has a history of following good email practice and independently establishes their reputation.

The second element of the Bonded Sender® program was the financial bond. The size of the bond was linked to the volume of email sent by the sender and is a significant sum designed to weed out only but the most reputable senders. This bond was then debited based on consumer complaints received by the program.

This program had a number of benefits. Firstly, this self regulation model promoted the adoption of best practices for all reputable senders. Secondly, by using a recognised independent third party to complete the sender certification, consumers had faith the program was not used by spammers.

In April of 2006, Return Path® re-launched the Bonded Sender program as Sender Score Certified®. Other than the name, there were two major changes to the program. First, the bond element was dropped. The second change is that Return Path® have raised the compliance standards based on the data they have collected since the Bonded Sender® program was launched.

This new program also provides greater reporting to let participants know how they are performing against the standards of the program. Failure to keep within the complaint thresholds will cause your sending IP to get blocked. Return Path® also advocates the use of feedback loops from their users including MSN/Hotmail which is their biggest.

Goodmail CertifiedEmail

The CertifiedEmail program is also an authentication and certification system, which was launched in early 2006. This initial launch was in a pilot mode limited to the US and Canada only. Both AOL and Yahoo! were early adopters of the program with AOL using it for all emails and Yahoo! limiting their participation to transactional emails only.

Goodmail launched in the UK in May 2007. Like the Sender Score Certified program there is a sender certification process, but this is limited to the client companies. Email Service Providers, on the other hand, are limited to partner status only. While Goodmail partners with TRUSTe, they manage the certification process in house.

Email Deliverability: How We Got Here and What Marketer's Should do About It

After accreditation email senders pay a nominal per email fee to ensure that their emails bypass the filtering systems of partner ISPs. In return for the fee, the sender gets guaranteed delivery as well as a special icon denoting the certified email in the inbox, full functionality of all links and no image blocking.

Goodmail launched in the UK in May 2007, creating a premium class of email for the first time. For some types of email, such as order confirmations and regulatory notifications, paying the premium to ensure deliverability may make good business sense. As of the date of publication, however, it is too early to see the impact that this two tier system will have on the email market in the UK.

White Lists

Not all delivery programs, however, are managed by third parties. ISPs and other email receivers use white lists to fast track deliverability for emails from reputable senders. While being on an ISP's white list is not a foolproof way to get your email delivered, they do significantly reduce the rate of false positives.

Each ISP has different rules and procedures for getting on their white list but in general they are:

- Only send opt-in email
- Always include a prominent unsubscribe link and promptly respond to all unsubscribe requests
- Use separate IP addresses for different lists
- Keep email lists clean by scrubbing invalid addresses
- Monitor and react to ISP feedback collected both on your email server logs and your abuse@ address
- Do not hide your identity by
 - Including your brand in the from address and subject line
 - Implementing SPF/Sender ID and Domain Keys

Some ISPs also maintain "Enhanced White Lists". As their name implies these are white lists with higher standards for inclusion, which further improve deliverability to that ISP.

Content Filtering

Unlike the programs listed above, which requires email marketers to take active steps to use, filtering tools used by email receivers look at the image, text content and the underlying code of the email and use heuristic or Bayesian rules to determine if the email is legitimate. The ISPs would use this as a secondary system if the sender cannot be validated using one of the authentication or reputation systems mentioned above. Users, however, also use these systems locally to filter emails that make it through the ISPs systems. There are three things to remember about these rules based systems. First, no single rule will cause an email to be blocked. They measure the email against all of the rules to give it a spam score. If the score exceeds the threshold set by the user, the email will be rejected. The second thing to remember is that emails blocked by content filters will have been reported as being delivered because they have been accepted by the mail server and are blocked at the inbox. Finally, the third thing to remember is that these rules change on a daily basis, so marketers need to monitor changes in how these rules are used.

Email Deliverability: How We Got Here and What Marketer's Should do About It

Real Time Black Lists

Real time black lists (RBLs) were the first attempts to limit the amount of Spam on the internet. A RBL is a list of IP addresses and domains that send Spam. Credited with creating the first RBL is Paul Vixie of the Mail Abuse Prevention System (MAPS).

ISPs and other email recipients can subscribe to one or more of these lists and block all incoming email from IPs and domains on the list. ISPs do not maintain their own RBLs in the sense that they do not let other use their list. ISPs do however maintain lists of IP from which they will not accept email.

RBLs have frequently been surrounded in controversy. From the email sender side, getting on an RBL is a somewhat arbitrary process and RBLs are often seen to be uncooperative toward removing legitimate senders that have been placed on the list in error and therefore a restraint of trade. At the same time consumers have also had problems with RBLs that list ranges of dynamic and dial-up IP addresses, as this can block those who run their own mail server or people connecting to the internet from home.

Increasing Deliverability

Now that we have a better idea of how emails get blocked, we will look at ways to improve email deliverability. The techniques to improve deliverability can be grouped into three categories:

- Permission
- List Hygiene
- ISP relations

Permission

Permission is the key to all deliverability. In the UK, the legal requirement is that you get the subscriber's permission by them taking a positive action, which is fully informed and freely given before sending an unsolicited commercial email. There are two exceptions to this rule:

1. Business to Business emails sent to staff of limited companies and public limited companies with content that relates to business products or services.
2. Business to Consumer emails sent to individuals when all the following conditions are met.
 - (i) email address collected in the course of negotiations for the sale of or the sale of a product or service;
 - (ii) consumer told email address would be used for marketing purposes and offered an unsubscribe facility (easy to use and free of charge other than the cost of transmission) at the time of data collection and on every subsequent message sent;

Email Deliverability: How We Got Here and What Marketer's Should do About It

- (iii) the marketing relates to similar products and services of the organisation which collected the data; and
- (iv) the identity of the sender not disguised.

Staff of sole traders and partnerships should be treated as individuals above under Business to Consumer regardless of whether the marketing relates to consumer or business products.

Following guidelines on opt-in and opt-out are vital components of permission.

For example, a marketing director at a stationery supply company wants to send an email to businesses that may benefit from stationery products. There is no need to have prior consent as long as the recipients work for a limited company. On the other hand, a marketer for a clothing company cannot send an email to the same population promoting their products, because, while it is important to be dressed at work, clothing does not relate to the recipient's job in most cases.

For the business to consumer exclusion to the opt-in rule, the email address must have been collected as part of a negotiation or sale and advertises a similar product or service. In the UK a negotiation is defined as beginning when the seller quotes a price to the consumer.

For example, if a consumer places a number of items of clothing in a shopping basket and provides their email address as part of this process, it is permissible to email these consumers clothing related offers in the future. It would not be permissible to mail this consumer offers for furniture, even if these items are sold by the same company.

Neither the B2B carve out nor the prior negotiation exclusion are considered best practice by the ISP community. They feel it is best practice to acquire a positive opt-in for all forms of email marketing. This is a higher standard than the DMA's own best practice guidelines, the DMA code and the law. Readers should refer to the DMA's Best Practice document (June 2007). When using either exception, however, it is important to remember that all marketing emails must include an opportunity to opt-out of future communications.

Collecting the Opt-in and Confirmation Emails

There are two components of permission. The first of these is the opt-in, which is simply asking potential subscribers if they want to receive marketing email communications from you and getting their email address. This can be done anywhere on your web site but a few things should be included with the registration process. First, there must be a clear link to your privacy policy, which details how you will handle the registrant's data. You should also set the recipients expectations appropriately by detailing what you intend to send and how often. Where possible you should let the recipient dictate content, message type (HTML vs. plain text) and frequency. This is also a good time to collect additional data that would be useful for your program, but remember to explain how this data will be used and how giving this data will benefit the recipient.

Email Deliverability: How We Got Here and What Marketer's Should do About It

The second part of getting permission is confirming that permission. This should always be done by sending out a non-commercial welcome (NCW) email. This email should remind the recipient of the benefits of the email program. It is also a good opportunity for marketers to get users to add their from address and domain to safe senders lists (a locally managed white list). Finally, the NCW, like all marketing emails, must include a prominent unsubscribe link to provide recipients to prevent future emails if they were registered in error.

At this point, the NCW described would be used for confirmed opt-in. What the sender has done is confirmed that the email address is valid and given the owner of that address the opportunity to unsubscribe if they registered in error. This is the minimum best practice standard.

A higher standard is called double opt-in, where the recipient has to take an additional positive action by clicking on the NCW email. The upside of this approach is that there can be little ambiguity of the intentions of the recipient and they are likely to be very engaged with the email messages. The downside to this approach is the drop off of recipients who registered but do not follow up by clicking on the email.

It is also possible to collect valid opt-ins from off-line sources such as a contact centre, product registration cards and retail outlets. Data quality is always an issue when data is collected off-line, so these addresses need to be treated differently.

First, until you have confirmed the email, it is best to segregate these addresses from the rest of your list both in your database and by sending them separately (ideally through a separate IP address). Second, as a practical matter, using double opt-in here gives you a digital audit trail for the opt-in.

Opt-out

Email marketing is all about permission and the recipient has the right to revoke their permission at any time. It is not only a legal requirement that the sender act on this revocation but this is also the best way for the sender to protect their brand.

Each email sent must include an obvious unsubscribe mechanism. It is best practice that a registrant can unsubscribe in one or two clicks and that unsubscribe requests are processed by the sender in near real-time. Some feel that putting the unsubscribe link at the top of the email and/or using the same font size as the rest of the text are also best practice.

Recipients may prefer to notify the sender of an unsubscribe request through any of the customer touch points such as contact centres, retail outlets or in the post. It is important that the sender be able to process these requests in a reasonable amount of time regardless of the channel.

List Hygiene

After opt-in/opt-out policies and practices, maintaining list hygiene is the most effective way to maintain high deliverability rates. In off-line direct marketing, the cost of producing and mailing each pack acts as a deterrent to over mailing campaigns. In email marketing, however, the marginal cost of each additional email

Email Deliverability: How We Got Here and What Marketer's Should do About It

does not hold the same disincentive. The result is that list owners have become lazy in removing invalid email addresses.

There are many reasons for email addresses becoming invalid. The first source of invalid email addresses is poor data collection. This is especially troublesome when email addresses are collected through offline means such as using the contact centre, product registration cards, etc. Using a confirmation email helps validate addresses collected offline, but only if the sender stops sending to addresses where the emails bounce.

Similarly, email addresses churn periodically and will become invalid and it is important that senders stop sending to these invalid addresses. Part of the SMTP handshake that transfers an email from the sender's server to the receiver's server is an acknowledgement of what the recipient is going to do with the email it has received. Recipient servers pass back codes letting the sender know among other things if the target email address is no longer valid. Processing this information to minimise the number of invalid email addresses on the list is not only best practice, it will also improve the sender's reputation with recipients.

In addition to codes indicating bad email addresses, recipients pass back a number of these bounce codes indicating both soft and hard message failures. In general, soft bounces occur when a message cannot be delivered for reasons that are temporary, while hard bounce failures are permanent. Ideally, senders will understand each code and act accordingly in marking addresses invalid on their email lists.

In practice, however, it is not always as straight forward. SMTP bounce codes were set in 1982 and have been in use since. While the codes are set, how they are applied is up to the network administrators managing each recipient domain. As a consequence, most senders have adopted business rules around the number of bounces needed to make an address invalid. The best practice rule of thumb is to make email addresses invalid after three consecutive bounces. It is possible, however, for senders to reverse engineer how each major ISP uses the codes and therefore adjust the rules around the number of bounces needed to invalidate and email accordingly. For example, some SMTP response codes should drive invalidation in the first instance, but other softer bounces (like mailbox full) should drive invalidation after as many as six bounces.

Another difference between off-line and on-line direct marketing surrounds recipients who could be classified as chronic non-responders or inactives. The costs associated with offline communications means that these inactives would be excluded. This is not the case in the online world where the marginal costs of each additional email are fractions of pence. Costs, however, should not be the driver for eliminating inactive recipients but rather the marketer's desire to protect their brand by sending information only to those recipients that want it.

ISP and IEP Relations

Regardless of how carefully you collect your opt-in data, process unsubscribe requests and maintain good list hygiene, you will occasionally find yourself being blocked. It is at this point you may need to contact the abuse experts at the ISP. The

Email Deliverability: How We Got Here and What Marketer's Should do About It

first place to look for information is at the ISP website. Here you will frequently find an FAQ page which will give you an idea of the source of your block. This area will also frequently give you contact details if you need to speak with somebody.

When speaking to an abuse representative, you should have all of the information to hand that they will need to help you. This includes:

- Your privacy policy
- How you collect opt-ins
- The date and time when the block started (if possible)
- A copy of the message that caused the block
- The IP address or range that is being blocked

While it is not guaranteed, frequently just the fact that you called is enough to get your first block lifted. Spammers never call to get blocks lifted, so your willingness to call gives you and your brand some legitimacy. Getting the block lifted, however, is not the only reason for the call. You should also try to establish why you were blocked in the first place, so you can take corrective action and ask for advice on how to prevent future blocks.

A quick count on the domains in your email list will tell you which ISPs are the most important to you. Depending on the impact that a block would have, it may be worthwhile to proactively begin to build relationships with these ISPs. You can begin this with an introduction of yourself and your brand that explains what you are doing and how you collected your data. This is also a good time to ask advice on how to prevent blocks.

The Future of Email Deliverability

As stated earlier, Spam exists because it works. The economics of Spam are such that an almost infinitesimal response rates becomes profitable. This gives the Spammers the economic incentive to be one step behind the ISPs in identifying new ways through the filters, if not closer. Legitimate email marketers are always going to be farther behind this development curve.

It is this gap that is being filled by companies like ReturnPath® with their Sender Score Certified® program and Goodmail® with their CertifiedEmail® offering. This intermediary space will continue to grow and will become increasingly crowded with companies that offer accreditation services.

At the same time, authentication technology will continue to develop. There have been proposals to fundamentally change the way SMTP works to make the entire email system more secure and less vulnerable to Spam and phishing techniques. This will take years to be adopted as internet standard and even more time to be implemented, assuming it can be agreed in the first place. In the meantime, there will be incremental advancements to DomainKeys and SPF/Sender ID as well as the development of new standards. It will continue to be important that senders keep up with these changes.

Email Deliverability: How We Got Here and What Marketer's Should do About It

Conclusion

Unlike marketers in other disciplines, email marketers have to worry about getting their messages to their intended recipients. Regardless of how much time you spend on getting the copy just right and the care you put into your creative, it is all wasted if your message is not delivered.

The volume of spam is driving the ISPs to block emails. Currently 80% of email traffic is spam, so there is a legitimate financial reason for the ISPs to control the amount of spam traffic on their networks.

The challenge in effectively blocking Spam, however, stems from weaknesses in the fundamental design of SMTP, which makes it hard for ISPs to decide which emails are legitimate and which are not. SPF and Domain keys are two technical solutions that allow ISPs to authenticate who the email is really from, but these do not provide into the reputation of the sender. Reputation is at the core of both the Sender Score Certified and Goodmail Certified Email programs. Aside from these technologies and programs, email marketers should follow basic data hygiene rules that will allow them onto the ISPs white lists and hopefully off real time black lists.

Going forward there will be a number of technical advances as well as other third party reputation services entering the market. Email marketers will have to keep abreast of these developments if they want to continue to receive their high rates of delivery.