
Sean Duffy

is Lead Consultant for UK email service provider Emailcenter, who provide email marketing solutions, services and consultancy to UK blue-chip organisations such as P&O Cruises, talkSPORT, National Savings & Investments and Saga. Sean has been working within the email marketing industry since 2002 and is responsible for providing strategic and tactical advice to the Emailcenter client base.

New Technology Briefing

A guide to email deliverability for B2C email marketers

Sean Duffy

Received: 4 June 2007

Abstract

Getting your email campaigns past spam filters has been a key concern for email marketers for some time. If your email campaign gets classified as spam, the response rate will be a fraction of the potential. On average, around 20 per cent of commercial email is blocked or filtered by Internet Service Providers, which therefore equates to millions in potential revenue lost per annum. The most common question asked by marketers is what do I need to do to ensure that all my emails avoid the junk mail filters. Unfortunately, there is no magic single tool or answer but a whole host of different factors that need to be understood. As the difference between sending email to consumers compared to businesses is significant this paper aims to highlight the key factors ensuring that consumer email marketing campaigns get delivered into the inbox.

Journal of Direct, Data and Digital Marketing Practice (2007) **9**, 156–167.
doi:10.1057/palgrave.dddmp.4350081

Keywords: email marketing, email broadcasting, email deliverability, junk mail

Introduction

For UK consumer marketers, there are typically only a handful of Internet Service Providers (ISPs) that make up a typical newsletter list. This simplifies the amount of filters the marketer needs to understand.

Figure 1 gives an overview of the top ISPs that appear in a UK list.

This shows, that nearly half of a typical B2C list is made up of three ISPs. Other ISPs and consumer work addresses are likely to account for no more than 5 per cent of a list each. If a marketer has a list of 1 million email addresses and 30 per cent are Hotmail accounts, if Hotmail blocks the email or considers the email to be junk, the loss of revenue could hit tens of thousands of pounds. Therefore, this paper focuses on deliverability issues relating specifically to these ISPs although by applying this best practice it will ensure optimum deliverability at other ISPs.

The ISPs focused upon tend to have the most sophisticated filtering technologies as they have to process much more email than others. Smaller ISPs are generally much easier to achieve good delivery rates with.

Sean Duffy
Lead Consultant
Emailcenter UK Limited
Kingthorn Park
Greens Norton
Towcester
Northants
NN12 8BS, UK
Tel: +44 (0)1327 350921
Fax: +44 (0)1327 359502
E-mail: sean.duffy@emailcenteruk.com

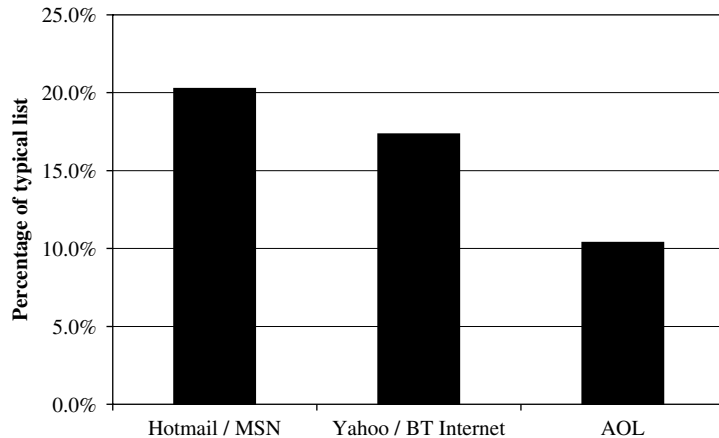


Figure 1: Top ISPs as % of typical list

The areas on which a consumer email marketer needs to focus on include:

Areas of focus

- Image and URL Blocking
- Server-level whitelists
- Content Filters
- Blacklists and Spam Traps
- Client Whitelists/Safelists
- Complaint Rates
- Bounce Rates
- Server Configuration
- Accreditation Schemes
- Email Authentication

Each of these will now be looked at in turn.

Image and URL blocking

A tactic that spammers use to capture valid email addresses is to include a unique image or URL within each email message that they send. If the image is downloaded or the link is clicked upon by the recipient, the spammer knows the address is valid and will send them more spam messages and possibly sell the address on.

To counteract spammers capturing addresses through images and URLs many ISPs and email clients block these when viewed by the user (Figure 2). This of course means that this impacts upon genuine emails. The problems that hit marketers as a result of this are:

Problems for marketers

- Email creative loses its impact as images are either greyed out or entirely stripped.
- The reader may not understand what is in the message if images are used to write text.
- Open rates cannot be tracked as the tracking image is blocked.
- Click-thru rates are likely to drop as users have to take other actions in their email client before being able to click on any links.

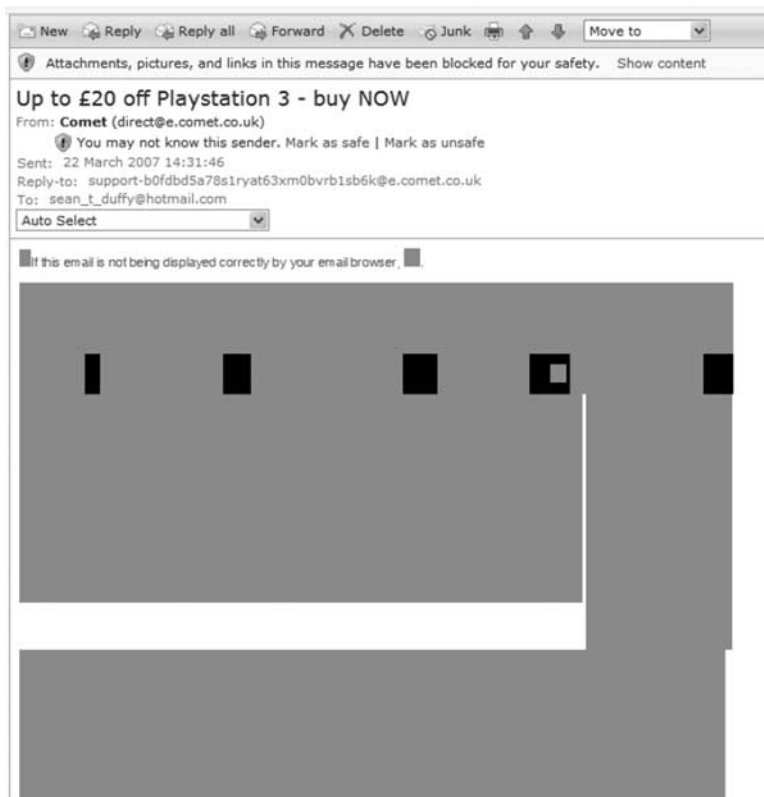


Figure 2: Example of an email with image and link blocking enabled

Table 1: Text and terminology used by ISPs

ISP	Term used
AOL	Adding the address to the recipient's address book makes the address safe.
Hotmail	Hotmail calls it a 'Safelist'
Yahoo	Yahoo informs users to add the address to their address book.

All this sounds very much like doom and gloom and people have stated that it is the end of email marketing. What still makes it viable to send graphical emails, however, is that users can easily choose to display the images either on a one-time basis or for all emails you ever send them at a click of a button. This is usually by adding your from address to their address book or a form of allowed senders or safe list.

You can encourage your recipients to add the address. For the correct terminology utilised for this, see Table 1 within the Client Whitelist/Safelist section of this paper.

The other action a marketer should take is crafting the creative so that a user can still see the main elements of your message without having to turn images on.

Whitelist

Server-level whitelists

A server-level whitelist is where an ISP or third party holds a set of IP addresses (this is a unique numeric address such as 194.154.181.116 that identifies the server and cannot be masked) or domains (I.E. www.theidm.com) that they know are legitimate senders. This helps reduce the number of opt-in emails that are classified as spam as the email is often routed around the content filters.

In addition, if you hold whitelist status with an ISP you are less likely to be placed on a blacklist.

All the major ISPs have at least one level of whitelist that is free to join, with the major exception of Hotmail, that requires the emailer to be part of the 'Sender Score Certified' scheme run by Return Path. More about this scheme is detailed in the Accreditation section.

Getting whitelisted is a relatively simple process if you are a legitimate permission-based sender. If you are using a reputable email service provider they almost certainly would have gone through this process for all of their servers. If you need to whitelist your own in-house systems, however, refer to the links below, which detail this process.

This is not the sort of paper to go into technical specifics but generally you will need:

- a secure and correctly configured sending server
- a reverse DNS set-up on the servers
- a low complaint rate (normally below 1 per cent) and
- bounce rates under 10 per cent.

Just because you are on a whitelist also does not guarantee your email will stay out of the junk mail folder. Indeed, Hotmail do not even guarantee those who pay for their whitelist status inbox placement of all emails.

Useful links:

AOL Postmaster site — Details options for whitelisting:
<http://postmaster.aol.com/whitelist/>

Content filters

Content filters work by scoring your email against a set of rules. If your email is above a certain score then it will be rejected as spam.

Typically, this would be looking at text to see whether there was mention of words such as 'Free' or 'Viagra' and any other words that you would expect to see in a spam email message.

Filtering

Over time, however, these filters can also learn what words and phrases are used by spammers. They do this by analysing the content of emails that recipients are reporting as spam. This is not a perfect science as if the spammer has utilised a harmless-looking phrase that also appears in your email, it can on occasions trigger the filters to classify your email as spam.

Content filters also look at a whole host of other factors including:

Ratio of text to images

As content filters can easily pick out spam emails selling viagra, spammers retaliated by hiding keyword text within an image. As a

result, spam emails would generally come through as just images. Therefore, filters look at emails that are purely images or have limited text with suspicion.

Email campaigns that your designer has built should not be built as just images. If you do get stuck with a design like this, try adding text at the bottom such as terms and conditions to balance it out. You may see spam messages come through with reams of poetry and other random text. This is because spammers are now learning that to beat this filter they need to add text to balance the image ratios out.

HTML Coding

If your HTML email has coding mistakes or uses certain tags then this is picked up. For example if the <TITLE> tag in the page is left as 'Untitled' this can give you a spam score.

Anything other than standard HTML code such as JavaScript and Flash will also cause issues.

Formatting of MIME emails

If you send HTML emails, it is always best practice to send a text version as well. All email marketing applications can do this by default but failure to include the text version may result in the filter giving you a spam score.

In order to make sure your email does not get tripped by these rules used by content filters, you should always test the email beforehand. There are a number of ways of doing this.

Testing tools

First, there are several free testing tools you can run that are based upon a filter called 'Spam Assassin' (Figure 3). This is the most widely used filter in corporate environments and will show you the areas it thinks could be spam.

The issue with this test is that although Spam Assassin is widely used in corporate filters, the major consumer ISPs including Hotmail, AOL and Yahoo do not utilise it because they have their own filtering tools. Spam Assassin may show you a low spam score but this bears little resemblance to whether the consumer ISPs will classify your email as junk or not.

You could therefore set up some test accounts at each ISP and send to these to see whether it is classified as junk but this is a time-consuming process. An alternative would be to utilise a specialist tool provided by your email service provider or a specialist email deliverability company that holds a series of seed addresses at all major

Points	Description	Rule Name
0.4	BODY: Eliminate Bad Credit	BAD_CREDIT
0.1	BODY: Image tag with an ID code to identify you	HTML_WEB_BUGS
0.5	BODY: Message is 80% to 90% HTML	HTML_80_90
0.1	BODY: HTML included in message	HTML_MESSAGE
0.3	BODY: FONT Size +2 and up or 3 and up	HTML_FONT_BIG
2.9	BODY: HTML has very strong "shouting" markup	HTML_SHOUTING6
0.1	BODY: HTML has "tbody" tag	HTML_TAG_EXISTS_TBODY
0.1	BODY: HTML font color is blue	HTML_FONT_COLOR_BLUE
0.1	Message only has text/html MIME parts	MIME_HTML_ONLY

Figure 3: Spam Assassin example report

Service (ISP)	Delivery
AOL (Filter level 1)	JUNK
AOL (Filter level 2)	DELIVERED
AOL (Filter level 3)	DELIVERED
Gmail (GoogleMail)	DELIVERED
Hotmail (Filter level 1)	DELIVERED
Hotmail (Filter level 2)	JUNK
Lycos	WAITING...
Orange / Wanadoo	DELIVERED
Tiscali	DELIVERED
Virgin	DELIVERED
Yahoo / BT Internet	JUNK

Figure 4: Example deliverability testing report from an email service provider

ISPs. You simply send to these addresses and results come back in the interface detailing how each ISP treated the email (Figure 4).

If you do find that your email is being classified as junk at any ISP it could be for a number of factors. Unlike the Spam Assassin report, none of these ISPs provide information on why. Therefore, the only way to ensure deliverability is through trial and error.

There is a technique to minimise the time spent changing your message and re-testing. After determining that your server is not blocked by the ISP, send a text-only version without any URLs. If this still gets junked then it is very likely that it is an issue with words and phrases in your message or header information such as the subject line. After removing any obvious phrases such as ‘free’ or even ‘unsubscribe’ then remove a paragraph at a time until you find the offending words.

If it does get delivered when sent just as text, then this suggests it is either an issue with your domain, image links and filenames, the ratio of images to text or anything else that is different in the text version.

Utilising this logical method should enable you to identify issues quickly.

Free Spam Checkers:

Mailtester — requires you to send an email and a response is emailed back.

<http://www.emailcenteruk.com/free-spam-content-checker.php>

Spamcheck — an online form where you paste in your email message

<http://spamcheck.sitesell.com/>

Blacklists and spam traps

Blacklists are lists of server’s unique numeric addresses known as IP addresses (I.E. 194.154.168.112) and domains that are considered spam.

If your IP address or domain is placed on a major blacklist, you could find that a large percentage of your emails are filtered. Some ISPs you send to will reply to each message with the details whereas others will simply filter your email into a black hole so that your subscribers do not see the message.

Blacklists

There are different types of blacklist. Many deal with the type of spam that is sent from machines that have been hijacked by a virus or if there is what is called an open relay. These should not be a concern to most marketers.

There are two types of blacklists marketers need to be aware of:

- (1) Blacklists generated as a result of complaints from people receiving emails and
- (2) Blacklists automatically generated when emails are sent to 'Spam trap' addresses.

Email harvesting

Only spammers should have spam trap addresses in their list as they use automated software to scan websites for email addresses. The blacklist owner has placed these trap addresses on websites where this software will collect them. This is known as email harvesting.

User complaints are not necessarily a sign that your email list is not opt-in. People will always get out of bed the wrong way and some will forget they signed up at all. Blacklist owners tend to understand this and so one complaint can cause a blocking for a short period of time but as long as there are no other complaints, the blocking is normally automatically removed.

Major ISPs tend to look at an average complaint rate rather than individual complaints when deciding upon blacklisting and so you are unlikely to get blocked based upon user complaints; however, they do utilise independent blacklists to determine filtering rules.

To check whether you are blocked, there are some free tools at the end of this section to test your sending servers and domains.

Not all blocking is temporary but all blacklist owners will quickly remove the blocking if you explain the nature of your messages and how you collected your list. Every blacklist website has removal instructions or at the very least contact details for removal.

Of course if you have sent email that is not permission based you will get blocked and it is difficult to remove the blocking as the number of complaints will be very high.

Useful website:

This site provides a real-time check of numerous blacklists against your IP address:

<http://www.robtext.com/rbls/>

SpamCop — the most widely used blacklist:

<http://www.spamcop.net>

Client whitelists/safelists

As well as an ISP such as AOL having a global white-listing that applies to all emails sent to AOL users, ISP users can have their own whitelists or safelists that apply just to their email account.

If you are on one of these, your email will always go to the inbox of the person's account and never the junk mail folder. Many will also show the images even if the recipient has image blocking enabled.

Getting on safelists improves results of email campaigns

When a person adds you to this local whitelist, it is the 'From' address that gets recorded. Therefore, ensure that you standardise on the address you are going to use as if you keep changing the address each time your recipients receive an email, they have to whitelist it again.

Getting on these safelists will improve the results of your email campaigns as images and links will be active on opening and there is never the danger of being lost in the junk mail folder. Therefore, it is worth dedicating some copy towards encouraging your recipients to whitelist you.

Users generally get the option to mark your emails as safe when opening the email. Table 1 shows the text and terminology used by each ISP:

By personalising these instructions according to the recipient's email provider, you will increase the numbers of people adding you as they will be more likely to understand what to do.

Complaint rates

Spam complaints made at major consumer email providers get treated differently than if your email was reported to a blacklist such as SpamCop.

These email providers actively encourage their users to use the spam button rather than the unsubscribe option in your email. This is because a true spammer uses the unsubscribe link to validate whether the address actually exists.

As a result, a vast number of genuine permission-based newsletters are reported as spam everyday.

This does become a problem when complaint rates become too high and during a large send this can lead to your emails being delivered to the junk folder.

The other problem is reporting your email as spam does not remove them from your list. Next time you send to your list the person reports your email as spam again, causing your complaint rate to become ever higher. This could lead to a more serious blocking issue in the longer term.

As a reaction to this AOL and Hotmail have introduced feedback loops. This is where every email you send that gets reported as spam gets sent back to you so that you can ensure that you remove the person from the list. This might sound like a laborious task but a number of email service providers will have this as a standard automated feature.

By having this feedback loop in place it provides you with a guaranteed way of ensuring that someone does not report your email as spam multiple times. You can also get a better understanding of how trustworthy your recipients are of your emails.

Useful websites:

Smart Network Data Services — See your complaint rate at Hotmail:
<https://postmaster.live.com/snds/>

Senderscore.org — A free reputation monitoring service from Return Path:
<http://www.senderscore.org>

Bounce rates

Many marketers think that if an email message is returned because the recipient's address is no longer valid then the only problem is the hassle in removing them from your list.

ISPs, however, do not see it the same way. Their argument is that if you keep ignoring the bounce messages then you cannot be a genuine permission marketer and will block you from sending further messages.

The threshold most ISPs work to is that less than 10 per cent of the emails you send must not be invalid. It should be noted that ISPs will only look at hard bounces, permanent errors such as where the user has closed the email account rather than soft bounces, which is where the ISP might request you to try re-sending later.

This is a major benefit of using a specialist email marketing solution to manage your email sends as they will have tools to automatically remove or suppress hard bounces from your ongoing email campaigns. Other solutions like bulk email sending tools or CRM systems do not always have the capabilities for managing bounce backs.

As part of your ongoing analysis of your email campaigns, it is important to monitor your bounce rate not just for each campaign but also per ISP to ensure that you do not exceed any thresholds.

**Important to monitor
bounce rate**

Server configuration

ISPs expect your mail servers to be configured correctly; otherwise, they will block your emails. Without going into detail as many of these issues are technical, here are some examples of what to look at with your infrastructure:

- Servers should not send via a dynamic IP address (as opposed to a static IP address that never changes) or from a residential IP address such as from a BT Broadband connection.
- The server should be secure and not accept connections from unsecured systems as spammers hijack these servers.
- Reverse DNS should be set up on the sending IP address, which enables the receiver to look up the domain that has sent the email.
- Excessive numbers of concurrent connections made between the sending and receiving servers at the ISPs should be avoided. Fifty concurrent connections is an advisable limit to place on your server.

Useful websites

Microsoft guide to getting better delivery rates at Hotmail, Includes useful information on server configuration:

http://download.microsoft.com/download/e/3/3/e3397e7c-17a6-497d-9693-78f80be272fb/enhance_deliver.pdf

AOL Postmaster Site:

<http://postmaster.aol.com/>

Accreditation

Accreditation schemes

ISPs and email service providers have tried to find ways of working together to ensure that valid permission email sent by an email service provider is not incorrectly flagged as spam.

One of the methods is for independent third parties to assess, evaluate and monitor the emailing practices of an email service provider and their customers. If they pass tests such as having low complaint rates, bounce rates and meeting the technical requirements, then for a fee accreditation can be completed.

If your email is sent via an accredited server, then ISPs can see that it is legitimate email and so may not route messages through the same number of content filters.

Different schemes

Different ISPs use different schemes and many do not guarantee delivery into the inbox.

Goodmail

Goodmail is utilised by AOL and Yahoo and does guarantee that your email will not only avoid the junk folder but also all images and links will be working when the person opens the email.

In addition to Goodmail ensuring you meet the requirements relating to mailing practices, they also imprint your email so AOL and Yahoo can confirm the email is from an accredited source. Each imprint of an email costs a small fee and may require an extension to your sending infrastructure.

This scheme is likely to be more popular for people wishing to send important transactional emails such as order confirmations, delivery notes and invoices as there is a high value on getting this type of email delivered. It is unclear, however, whether marketers will value their newsletters highly enough in order to pay again for sending these.

Sender Score Certified

This accreditation scheme used to be known as Bonded Sender and is run by Return Path. It is basically a list of IP addresses that have been accredited by Return Path in exchange for an application fee and licence fee. Hotmail utilises this scheme and is the only method of becoming whitelisted with Hotmail. Hotmail have recently moved their position on emails from a Sender Score-Certified IP address to say that they will be delivered into the inbox with all images and links working.

Habeas Safelist

Habeas claim to have the most widely used internet whitelisting service for commercial senders. As with other schemes Habeas look at a variety of areas in your email practices and sending infrastructure before allowing you to join.

Truste

Truste are known for their approval of websites that follow a range of privacy principles rather than email accreditation. They do, however, have an accreditation scheme that differs from others as it looks at how you collect, store and use your email list.

All these accreditation schemes are run by profit-making third-party organisations who have a vested interest in displaying figures that show an uplift in deliverability rates through being accredited. That is not to say that on average those who are accredited get better delivery rates than those that are not. Those that are not accredited, however, include people who do not qualify for these accreditation schemes because their mailing practices are not to the required standard. This group of people would of course struggle in achieving good deliverability and end up putting a slant on the statistics. In addition, those who have paid to become accredited take deliverability seriously and will also on the whole be more proactive in testing against junk mail filters, removing bad addresses and reducing spam complaints and so will naturally achieve better delivery rates anyway.

However, it seems as the majority of consumer lists are dominated by AOL, Yahoo and Hotmail addresses, it is likely that this will drive Goodmail and Sender Score Certified take-up upwards as the benefits are easily quantifiable.

Links to Accreditation Schemes

Goodmail

<http://www.goodmail.com/>

Sender Score Certified

<http://www.senderscorecertified.com/>

Habeas Safelist

<http://www.habeas.com/en-US/Receivers/safelist/>

Truste

http://www.truste.org/businesses/email_privacy_seal.php

Phishing

Email authentication

Phishing is where someone sends you an email claiming to be someone they are not. For example you may have received an email claiming to be from your bank asking for login or account details.

The email may even have come from the address used by your bank but if you respond by completing the online form, your bank account will be quickly drained of all funds by the con artist.

To overcome this, ISPs have come up with ideas to stop people faking the identity of the sender. Unfortunately, the big three consumer email providers have not standardised so far and so there are separate authentication schemes to consider for each provider. Each of these schemes is not compulsory in order to get delivery but each will assist in avoiding the junk mail folder.

Sender Policy Framework and Sender ID

Sender Policy Framework (SPF) and Sender ID are very similar schemes. SPF is a creation of the open-source community and looks up the IP address of the server sending the email to see whether it matches the From domain. This is not the 'From' address but the address of the server that is hidden in the headers of every message.

Sender ID is the Microsoft implementation of SPF and utilised in Hotmail and the latest versions of Outlook. Sender ID differs in that it can be configured to check the actual from address or the server address.

It is very easy to become compliant as you have to follow some simple wizards on websites. This is generally a task for your IT department as only they will have access to your DNS records that require changes. Links to some wizards are listed below:

SPF Wizard:

<http://old.openspf.org/wizard.html>

Sender ID Wizard:

<http://www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard/>

DomainKeys

Yahoo has chosen to implement a solution that signs each message leaving your server with a key as opposed to simply setting up a single record like in SPF and Sender ID.

While this is a more comprehensive solution it has the drawback of requiring compatibility from the mail transfer agent (MTA) used by your emailing solution. Currently, most MTAs are not supported apart from third-party commercial products that require a significant investment and only when domainkeys support becomes commonplace among other MTAs including open-source tools will this authentication become important for email marketers.

Email deliverability is crucial

Conclusion

Email deliverability is a crucial element that makes up the success of your email marketing campaigns. The idea that it is impossible for a marketer to deliver campaigns on their own without extensive support from experts is false. There is no need to outsource all email marketing activity to get deliverability, although doing so helps take the burden away from the marketing department.

Indeed, the perception that your email service provider will handle everything for you is also wrong. The ESP will handle whitelisting, ISP relations, monitoring of blacklists and perhaps provide you with a range of testing and list management tools to assist with everything discussed in this paper. If you are managing your own email campaigns via an ESP solution or your own in-house software, however, you still need to consider checking the content against filers, tailoring your content for image blocking and encouraging your subscribers to add you to their personal whitelists.

As long as your email marketing efforts are permission based and you follow the basics set out in this paper, you will never have any major deliverability issues. If your email is not permission based, however, there is nothing you can do to guarantee that your email will not be delivered.