

# **Avoiding the Spam Trap**

---

**Understanding why your email gets filtered and what you can do to avoid it**

**Emailcenter UK  
October 2005**

**[www.emailcenteruk.com](http://www.emailcenteruk.com)**

## Introduction

---

According to leading Internet security and anti-spam company Messagelabs, 1 in every 1.54 emails is a spam message. As a result ISP's and IT Managers have implemented many tools and technologies to filter out this email.

As this is still not an exact science it does mean perfectly valid, permission-based email can get filtered, blocked or quarantined.

This guide provides marketers with a guide to how your email might get filtered and provides a checklist of activities to ensure you maximise your delivery rate.

# What causes your email to be blocked?

---

## > Invalid header information & a dodgy IP address

ISP's and filtering software will often look at the hidden parts of the email to determine its 'spamminess'.

This might be:

### **The IP address the email was sent from**

Each server has a number known as an IP address. This is difficult to fake and is totally unique. If this IP number has been reported on a number of occasions for sending spam it is likely to appear in a blacklist. The ISP or receiving email server may choose to filter this email or bounce it back to the sender.

It is a common myth that a single spam complaint will cause your IP address to be blacklisted. In most cases it takes many spam complaints for this to happen. In addition there are hundreds of different blacklists used on the Internet with less than half-a-dozen being established enough to impact on your email campaigns.

These blacklists also tend to be temporary blocks for 24-48 hours. Usually filling in a simple contact form on the website is enough to remove your IP address from blocking immediately and in some cases prevent it happening again.

### **The IP address is not matching the 'From' address**

Due to a rise in 'phising', the type of spam sent proclaiming it is from your bank or other supplier and usually asking for credit card details or other sensitive information, certain ISP's and organisations have developed a method of identifying these fraudulent emails.

This is achieved by looking at the 'From' address used and the IP address the email was sent from to see if they match up. If they don't match then there is a doubt about who the real email sender is.

This approach has many problems as organisations often have perfectly valid reasons for sending email from external servers. This could include the sending of order confirmations, statements or of course email newsletters.

Microsoft is one of many technology providers to start implementing solutions around this. They have developed Sender ID, a way for organisations to publish a list of IP addresses they send email from. This means when the ISP now checks the domain name against this list of IP addresses, as opposed to simply the IP address the domain is registered to. This is a much more comprehensive and accurate way of validating the source of an email.

In the near future Hotmail, the web-based email offered by Microsoft will start putting non-sender ID compatible emails into the junk mail folder.

### **No reverse DNS look-up**

This is the process of your server being able to look-up a domain name from an IP address. Servers without this set-up are likely to appear on many blacklists.

### **Blank headers**

If various headers are blank then these can get your email rejected. For example this might be a blank reply-to address.

## > **HTML source code & multi-part build**

IF your HTML or text versions contain errors or attributes that spammers have used then this can get filtered out.

For example:

- You have sent in MIME format but without a text version
- Certain HTML tags such as 'font size=1' have been used
- Your HTML contains errors
- The 'created by Frontpage' tag is still within the Emailcenter UK Limited

## > **Trigger phrases**

Content filters will analyse your email and give it a score. The higher the score the more likely it is to be a spam email.

These filters look for characteristics such as:

- Excessive spacing, capitalisation & exclamation marks
- "If you no longer..." and other ways of stating your opt-out message
- Claims such as free, no obligation and trial
- Links or image references on .biz or .info sites

These are just some examples of the characteristics a content filter might look for. To understand how your email will fare against the filters you can register for our free spam content checker at [www.emailcenteruk.com/free-spam-content-checker.php](http://www.emailcenteruk.com/free-spam-content-checker.php)

This will produce a report detailing every potential spam phrase and an overall spam score.

## 5 easy steps to take to improve email deliverability

---

### 1. Check and test each of your email messages

Each email campaign you send should be tested against a content filter before the final send. This will enable you to identify any major issues and take corrective action.

Hotmail and the other main web-based email providers tend to use different filters. Indeed the strictness of these filters tends to vary according to email volumes they are receiving. Around Christmas time marketers may find it increasingly difficult to get the email into the inbox and not the junk mail folder.

Therefore it is useful to create a set of test accounts at each of these providers to see if the email gets delivered into the inbox before you send any campaign for real.

### 2. Choose a reputable, experienced email service provider partner

Your email service provider will be able to assist you and indeed manage most aspects of deliverability to ensure your email gets delivered.

This will include:

- Placing their servers on whitelists
- Preventing questionable email senders from using their servers
- Setting up feedback loops with major ISP's such as AOL to receive and action any spam complaints

There is another myth that anyone using an in-house server will suffer from deliverability problems. There is nothing to stop an email service provider from assisting someone using an in-house server from becoming whitelisted with ISP's.

Indeed as long as only genuine permission emails are delivered it is unlikely that enough spam complaints will be generated to cause the server to become blacklisted.

### 3. Exclude bounces

If you continually send emails to known bad addresses certain ISP's including AOL will take action. Therefore monitor your bounces and exclude addresses that continually bounce. Most email service providers will be able to automate this process for you.

### 4. Think whitelist, not blacklist

Many marketers and email service providers take the approach and mindset of trying to avoid blacklists. Whitelists are lists of approved legitimate senders 'from' or IP addresses. These are controlled both by ISP's and recipients who might have a personal whitelist. Any email sent through a whitelisted server is usually subjected to less filtering if any.

Getting on an ISP's whitelist is fairly simple. It is usually the case of simply stating your organisations details along with how you collect your list. Some ISP's might ask for an email address to forward spam complaints onto. Of course if you are using a reputable email service provider all of this should be done for you anyway.

For those marketers and providers that are constantly switching IP addresses to avoid becoming blacklisted, are generally doing so firstly because they are sending high-risk email from questionable list sources. These people are never identified as legitimate senders as their IP addresses are unknown – this means the ISP's put these emails through the most stringent tests increasing the likelihood that the email will be put in a junk mail folder anyway.

## 5. Encourage your organisation to register a SPF record

As more and more ISP's attempt to identify forged email addresses Sender ID will become more important in ensuring your emails are delivered.

Each IP address your organisation sends email from will need to be listed in your sender policy framework record. This is not just your email service provider IP address but any other services such as order confirmations from your website. Therefore someone in the organisation needs to carry out a mini-audit to identify all servers that emails are sent from and create a SPF record.

A wizard for this can be found at <http://spf.pobox.com/wizard.html>

## Mailtester – Your FREE Spam Content Checker

---

Mailtester is a free tool to test your email campaigns against a Spam filter to identify and correct any potential problematic phrases or characteristics within your email.

Simply register at:

[www.emailcenteruk.com/free-spam-content-checker.php](http://www.emailcenteruk.com/free-spam-content-checker.php)

Content analysis details: (4.3 points, 0.0 required)

pts	rule name	description
0.1	EXCUSE_10	BODY: 'if you do not wish to receive any more'
1.0	HTML_TAG_EXIST_TBODY	BODY: HTML has "tbody" tag
1.7	HTML_IMAGE_RATIO_02	BODY: HTML has a low ratio of text to image area
0.3	HTML_90_100	BODY: Message is 90% to 100% HTML
1.5	MIME_HTML_MAINLY	BODY: Multipart message mostly text/html MIME
0.0	HTML_MESSAGE	BODY: HTML included in message

## About Emailcenter

---

Emailcenter are one of the UK's leading email service providers. Emailcenter currently manage the email marketing for over 100 UK organisations including Saga, P&O Cruises, Thomson and National Savings & Investments.

To discuss how we can assist with your email marketing call us on 01327 350921 or visit [www.emailcenteruk.com](http://www.emailcenteruk.com)