

# How to make sure more emails reach your subscribers

GraphicMail White Paper 2011

GRAPHIC MAIL 

email & mobile marketing solutions

# Contents

1. Email and delivery challenge	2
2. Delivery or deliverability?	3
3. Getting email delivered	3
4. Getting into inboxes	5
5. Content filtering	6
6. Reputation filtering	7
7. Authentication and domain-based reputation	8
8. How is sender reputation defined?	9
9. Tracking spam complaints	10
10. Avoiding spam complaints	11
11. How an ESP can help with deliverability	12

# The email delivery challenge

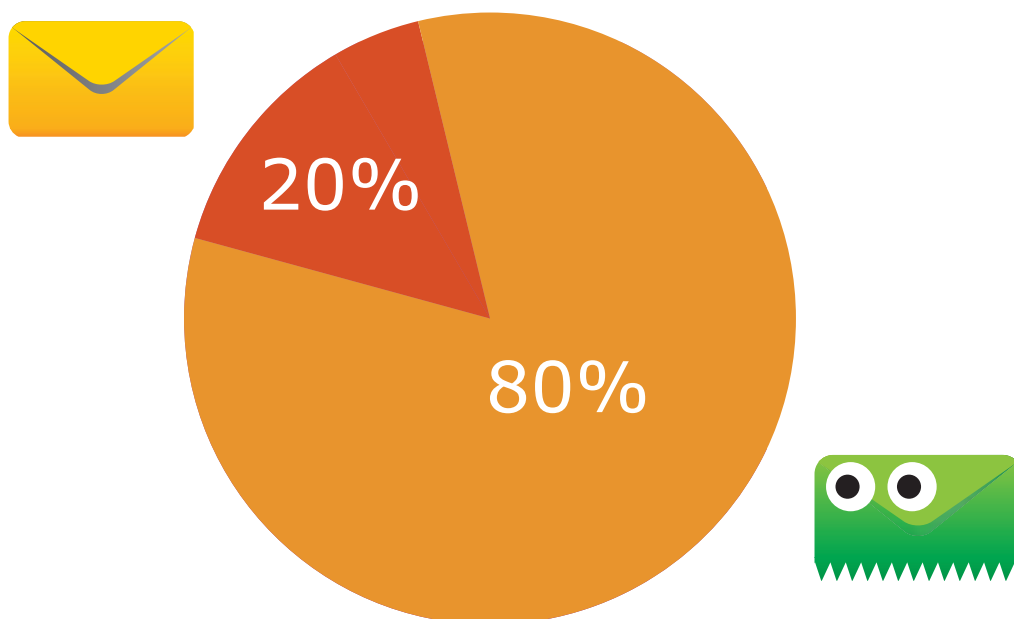
Email is simple. Once you press the send button, a little bit of electronic magic takes place and your message arrives in the inbox of the recipient. At least that's how it looks.

Unfortunately, there are various hurdles each email must overcome before it reaches its intended destination. As a result, not every email makes it through to the inbox. That's actually good news, when you consider that some 80% of all sent email is spam.

The bad news, though, is that it's not just spam that gets tripped up by delivery hurdles. Some email that people have asked for (opt-in email) gets caught, too.

The most recent benchmark reports issued by Return Path, for example, found 17.8% of legitimate marketing emails failed to reach subscriber inboxes in Europe and 19.9% failed to do so in the USA and Canada .

**In this white paper we'll take you through the terminology, techniques and tactics you need to know about to help ensure your mail does get through to your subscribers.**



# Delivery or deliverability?

There's a lot going on when email travels between the sender and recipient, but it's helpful to think of two basic kinds of issues.

The first concerns email delivery, the process of transferring the email from the sending to the receiving organization. A successful email delivery is one where the message is not rejected by the latter.

The second concerns email deliverability, which refers to getting email delivered to the recipient's actual inbox.

It's important to realize that once apparently accepted for delivery, your marketing email can still be blocked from reaching the destination email account. It might be deleted beforehand, and even if it is "delivered" to the account, it can still be rerouted away from the inbox and into the spam, junk or some other folder.

Symantec (2011) State of Spam & Phishing: February 2011

Return Path (2010) European Email Deliverability Benchmark Report

Return Path (2010) Email Deliverability Benchmark Report

## Getting email delivered

When email is not accepted by the receiving organization, it's usually down to some technical issue.

Such rejections typically trigger an automatic notification - a bounce message - which you can think of as the email equivalent of the "return to sender" message. A bounce tells the sender or sending system that the email could not be delivered and why.

Bounces are commonly (if not always accurately) categorized as "hard" or "soft".

A hard bounce represents a permanent problem with delivery, such as when you send mail to an email address that doesn't exist.

A soft bounce refers to a (hopefully) temporary problem, such as when the recipient's email account is full.

The email delivery rate you find in email campaign reports is simply the number of emails sent out minus those reported as bounced.

## Why bounces are important

Email addresses with a permanent delivery problem should be taken off the mailing list. Otherwise you're consuming resources to send an email that can't be delivered. Sending email to dead addresses is also one measure used to identify a "bad" sender, as we'll see later.

Bounces indicating a temporary issue are less clear cut, but your sending system should react automatically and appropriately, dependent on the nature of the problem. Often a message is simply delayed until the problem resolves.

## SPECIAL CASES: "Blocked" bounces and "throttling"

Some systems send a bounce message when the email is blocked (rejected) as spam. Most, however, don't do this for fear of the insight it might give spammers. Most "spam" is simply deleted or sent to "junk" folders.

You may also come across the term "throttling". This is where a receiving organization restricts the amount of email that can be accepted over a set period of time from a particular source. The term is also applied when sending organizations manage the volume of outgoing email to respect these limits. This usually only impacts those sending very large volumes of email.

### ACTION SUMMARY (Getting email delivered)

- Monitor bounce messages to gain insight into why emails are not being delivered.
- Keep bounces low using an ESP or software tool that reviews and processes bounces appropriately.
- Ensure email addresses with permanent delivery problems are suppressed from future deliveries.

# Getting into inboxes

Receiving systems at Internet service providers (like the big webmail and broadband companies) and corporate IT departments don't want to send all email into the inbox, because much of it is likely to be spam. So they run a series of checks, often referred to as spam filtering, to decide how to categorize incoming messages: reject as spam, delete as spam, send to inbox or send to some other folder.

Even if your email passes through these system checks/filters positively, it may face further examination from the software (the email client) used by end users to read their email.

## How can I tell if I have an inbox delivery problem?

Receiving organizations don't provide data on exactly where they put a sender's emails.

So most marketers rely on other clues to help identify an inbox delivery problem. For example:

1. Look for unusual and unexpected dips in response rates.
2. Look for unusual increases in spam block messages.
3. Check response rates by address domain. If nobody with a yahoo.com email address is opening or clicking on your emails, you likely have a deliverability problem at Yahoo! Mail.
4. Use a seedlisting service. These monitor dozens of test accounts at major ISPs to see if your emails arrive in the inbox, in the junk folder or don't arrive at all. Your ESP may feature this or there are standalone services offered by EmailReach, Delivery Watch, Return Path and others.

Email systems and software use various combinations of public and/or proprietary filtering techniques and products to process email, but the two dominant forms of spam filtering are content- and reputation-based.

# Content filtering

As the name suggests, content filters look at the content, code and structure of the email to see if it has any characteristics that indicate spam.

A popular spam filter is SpamAssassin. It runs hundreds of individual tests on each incoming message, many of which are content checks.

Each check is given a points weighting, and the points scored with each failed check are added up to get an overall spam score. If that score exceeds a certain threshold, the email is tagged as spam and treated accordingly.

The tests run by SpamAssassin are well documented , and here are some example content checks:

- Message talks about a replica watch
- Subject is all capitals
- From: domain has series of non-vowel letters
- HTML font color similar to background

Many ISPs and anti-spam technologies have reduced the emphasis given to content filters or to individual content checks, with more focus going on reputation checks. One reason is problems with “false positives”, where, for example, email actively requested by subscribers is blocked along with spam because it happens to share a similar vocabulary or layout.

A few years ago, marketers dared not use words like FREE in subject lines for fear of triggering content filters. However, this risk is much lower now: a few content issues alone are unlikely to see an email trashed as spam.

## ACTION SUMMARY (Content filtering)

- Use a spam checking tool to test how your email structure and content looks to popular spam filters and take corrective action as required based on the feedback.
- ESPs like GraphicMail have such tools built into their systems. Standalone versions are available from specialist deliverability services, such as those mentioned earlier. See <http://spamassassin.apache.org/tests.html>

# Reputation filtering

Reputation filtering looks less at the individual email and more at the origin of the message. Its importance has grown rapidly and “sender reputation” is now probably the most important factor determining the fate of delivered email, particularly at major webmail services and other ISPs.

## What is a sender?

Sender reputation is typically associated with the network connection point of the email source, the so-called IP address from which the email is sent. Email marketing services, for example, manage a range of IP addresses from which they send out their clients’ emails.

## Shared/dedicated IP address

A dedicated IP address is one for the exclusive use of a single sender. Your sender reputation is based entirely on your own emails and sending practices.

A shared IP address is one also used by other senders (perhaps fellow ESP clients). Your sender reputation is influenced by your own practices, but also by those of these other senders.

It seems sensible then to always use a dedicated IP address (or insist on one from your ESP). However, there are two problems with this:

1. You need to send a significant amount of email to build up a reputation. Little-used sender IP addresses tend to be viewed negatively by ISPs.
2. New IP addresses need to be handled with care, with outgoing email volumes building gently with time. This “warming up” process needs expert management.

As a result, smaller email senders are usually better off with a shared IP address at an ESP, who are experts at managing such addresses to ensure they maintain a good reputation.

The better ESPs also reward “good” senders by putting them together on the same high-reputation IP address. This removes the risk of associating with bad apples who might bring down your reputation.

# Authentication and domain-based reputation

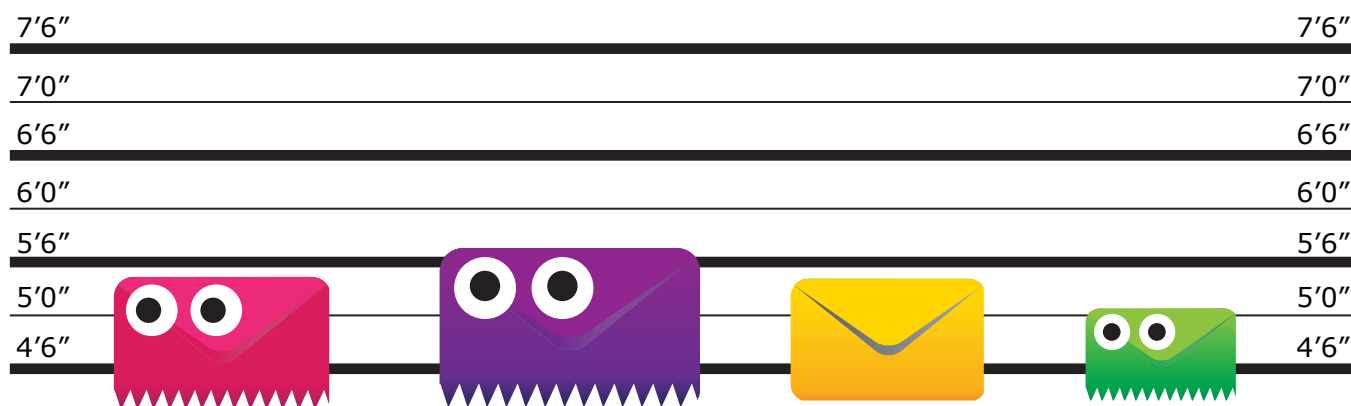
Obviously, it would be better if ISPs could associate emails with the “real” sender, like the domain name behind the email, rather than the IP address used to send it out. This accountability would allow legitimate senders to build their own reputation and carry it around with them across different sending systems.

As part of a broader move to more accountability in the email ecosystem, ISPs and others are implementing email authentication: a set of standards that allows receivers to confirm the true identity of the sender of an email.

The role of authentication and domain-based reputation continues to grow, so it’s a recommended practice to ensure outgoing emails support the authentication process. This is done through changes to domain name records and the information accompanying the email message.

## ACTION SUMMARY (Email authentication)

- Consult with your technical staff to ensure you support the two main sets of authentication standards: SPF/Sender ID and DomainKeys/DKIM.
- If you use an ESP, they should authenticate outgoing email for you and help you make any necessary changes to your domain records.



Please identify the real spam?

# How is sender reputation defined?

As you might expect, different organizations rank, weigh and select reputation elements in different ways, but it typically derives from a combination of the following:

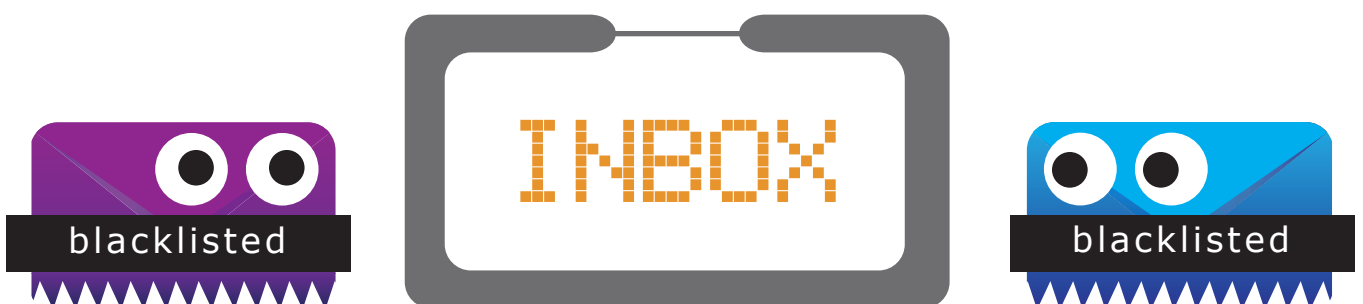
- User interaction with your messages
- List hygiene (bounce management and spam traps)
- Blacklisting
- Sending infrastructure and sending patterns

## Reputation factor: User interaction with your messages

ISPs and others look at how users interact with the messages previously delivered to email accounts from a particular source. Positive interaction contributes to a good sender reputation for future messages from that same source, negative interaction to a bad one.

Far and away the most important interaction is whether account holders are reporting emails as spam, commonly through the “report spam” buttons found on many webmail interfaces.

If the proportion of emails marked as spam by its users exceeds an acceptable threshold, then ISPs will likely throttle or block further messages from that sending source. Such blocks may be temporary or may require remedial action by the sender before they are lifted.



# Tracking spam complaints

Most of the major ISPs offer a feedback loop (FBL). An FBL is where an ISP provides a sender with information on which addresses emailed by that sender generated a spam complaint. The sender can (and should) prevent those addresses from getting any future email from them, and adjust their practices in response to complaint levels.

## ACTION SUMMARY (Tracking spam complaints)

- Sign-up for FBLs from all the major ISPs and correlate complaint levels with different email campaigns to identify problems.
- Many ESPs are already signed up to relevant FBLs, and monitor and process complaints automatically on your behalf.

# Avoiding spam complaints

It's important to understand why people mark legitimate messages as spam, so you can use this insight to keep the number who do as low as possible.

See [http://wiki.wordtothewise.com/ISP\\_Summary\\_Information](http://wiki.wordtothewise.com/ISP_Summary_Information) for a list

## 1. Permission

The classic definition of spam is unsolicited bulk email: email which the recipient never asked for.

However, even where people have signed up for an email, they may still use the "report spam" button if:

The emails they get are not what they expected. For example, if you send your newsletter subscribers another newsletter from a sister organization.

They forgot about the original opt-in.

### ACTION SUMMARY (Avoiding permission problems)

- Only send email to people who explicitly requested it.
- Don't buy email addresses, as these people are not expecting email from you.
- Don't leave too big a gap between sign up and sending out email (no more than 2-4 weeks) and make sure new subscribers always get an immediate welcome email.
- Ensure your sign-up forms and pages let subscribers make an informed and clear choice to join a list and (together with the welcome message) explain what kind of emails they can expect.
- Consider placing a reminder of where people signed up for your email in the footer of each message.
- Don't leave more than a few weeks between sends.
- Make sure the from line, subject line and the top of your email together clearly communicate the identity of the email and sender.

## 2. Value/annoyance

People may also mark messages as spam simply because they are no longer interested in the contents or because the emails come too often.

### ACTION SUMMARY (Avoiding annoyance problems)

- Monitor spam complaints and response rates if you increase your frequency significantly.
- Work to increase the relevancy and value of your emails.
- Identify subscribers who no longer respond to your emails and consider a special campaign to win back their interest.

## 3. Lazy unsubscribes

When using webmail, some people use the spam report button instead of going through the unsubscribe process, since they both have the same outcome (no more emails from that sender appear in the inbox).

#### ACTION SUMMARY (Avoiding “lazy unsubscribes”)

- Make the unsubscribe link in your footer obvious and ensure the unsubscribe process is clear and efficient. Monitor email replies to your messages in case these include unsubscribe requests.
- If you are concerned about spam complaints, consider placing the unsubscribe link in a more prominent position...such as at the very top of your email.

## Reputation factor: List hygiene

ISPs and others expect senders to keep their email lists “clean”: clear of non-existent or defunct addresses and full of real, active email addresses. It’s a sign of a “good” sender, as bad senders - i.e. spammers - typically don’t trouble to update their lists. The higher the proportion of emails you send to “dead” addresses, the more your sender reputation suffers.

Some ISPs also take disabled addresses (for example, from closed accounts) and, after a suitable period of time has elapsed, convert them to spam traps. A spam trap is an address created such that, by definition, any email to that account is likely to be spam. In this case, a good sender would have already removed the dead email address long before it became a spam trap.

#### ACTION SUMMARY (List hygiene)

- Again, only send email to people who explicitly requested it.
- Again, don’t buy email address lists: these are likely full of dead addresses and spam traps.
- Always remove addresses that cannot (or can no longer) accept email from your list, or use an ESP that does this automatically for you.

## Reputation factor: Blacklisting

A blacklist is a list of “bad” senders whose email can then be blocked automatically. A blacklist may also list domains commonly used in spam, so that the appearance of a blacklisted domain in a message also allows blocking.

ISPs manage their own internal blacklists and/or they may use those provided by third parties. Appearance on such a list (blacklisting) results from excessive spam complaints or some other indicator of a poor sender reputation, like emailing spam trap addresses.

Such a listing may be temporary or may require remedial action and communication with the blacklist owner.

#### **ACTION SUMMARY (Blacklists)**

- All the tactics outlined to improve your sender reputation should keep you off blacklists.
- Monitor public blacklists using your ESP's own tools, using the tools provided by deliverability services or using standalone blacklist checkers like MXToolBox. If you are listed, follow the blacklist's instructions on how to get your listing removed.

## Reputation factor: Sending infrastructure and sending patterns

This concerns technical aspects of the sending process, such as the configuration of the connection and the identifying information that accompanies an email message.

This should meet standards associated with the security and transparency of the sending process.

A regular, consistent flow of emails without sudden and unusual peaks also improves your reputation.

#### **ACTION SUMMARY (Sending infrastructure and sending patterns)**

- Consult a delivery specialist to ensure your systems and sending patterns comply with typical ISP requirements.
- Alternatively, use a professional ESP who already has this infrastructure and volume management in place.

# How an ESP can help with deliverability

There is a lot of jargon in the email delivery world and a lot of potential hurdles preventing email reaching the subscriber's inbox. However, deliverability is not the huge challenge it is often made out to be, provided you follow the best practices outlined in this paper.

Deliverability is affected by what you send and how you send it. You may find it easier to meet the challenge by using a professional email service provider. A good ESP can help your deliverability through, for example:

- Automatic bounce management to help keep your list clean.
- Built-in spam testing and other deliverability monitoring and optimization tools.
- Optimized shared IP address management to ensure a higher sender reputation for smaller senders.
- Support for email authentication.
- Built-in FBL and complaint processing.
- Professional sending infrastructure meeting required standards.
- Expert understanding of ISP requirements and deliverability problem resolution.

