Table of Contents

What is Email Deliverability? 3
The Importance of Email Deliverability 4
The 4 Stages of Email Deliverability 4
  1. Network Level 5
  2. Server Level 5
  3. Recipient PC Level 5
  4. Recipient Level 5
A Very Important Consideration – List Cleanliness 5
The 4 Stages of Email Deliverability 6
  1. Network Level 7
      Sender ID and SPF 7
      Domain Keys 8
      Feedback Loops 8
      Whitelisted Agreements 9
      Dedicated IPs 9
  2. Server Level 10
      Black List Check 10
      Sender ID , SPF and Domain Key Check 11
      Spam Filter Check 11
  3. Recipient PC Level 12
      Secondary Spam Filters 12
      Custom Rules 12
  4. Recipient Level 13
      Sender Recognition 13
      Appealing Subject Line 13
Glossary 14
Appendix A: Deliverability Rates 15
Appendix B
  Subject Lines to Avoid Using 16
  Words & Phrases to Avoid Using 17
About Vision6 18
What is Email Deliverability?

In simple terms, email deliverability refers to the likelihood of an email arriving in an intended recipient’s inbox. Deliverability is typically reported as a percentage. A deliverability rate of 90% would be considered exceptional and is measured by dividing the number of emails that did not bounce by the total number of emails sent (see Appendix A – Deliverability Rates).

This whitepaper is focused on understanding what email deliverability is and helping you improve your deliverability rates. The first section provides a brief overview of the 4 key levels an email must navigate from the initial send to a recipient’s inbox.

The second section goes into more detail and provides methods and tips on how to gain greater deliverability.

The 4 key levels are:

1. Network
2. Server
3. Recipient PC
4. Recipient

Finally, this whitepaper provides an example campaign and the formula used to determine the deliverability (See Appendix A) as well as a list of common words and phrases to avoid when creating your next email campaign.
The Importance of Email Deliverability

The intention of any email marketer is to reach as many recipients as possible. The more people reached, the more effective marketing efforts are considered to be, and as such increases the potential return on investment. Therefore, deliverability is of the utmost importance.

Whilst the goal is simple, the process is quite complex. Deliverability does not have a magic solution! It is important to understand the various components within the deliverability process, particularly the elements you have control over, to ensure you achieve the maximum possible deliverability rates.

Why is it so difficult?

Deliverability is a challenge because Spammers share your main goal – to reach the inbox without being filtered! Spammers are constantly re-designing their messages to maximize their own deliverability, leaving genuine email marketers in the position where they need to be smarter, more informed and more prepared than Spammers to reach the recipient’s inbox. Understanding the steps your email takes on its journey to your recipient’s inbox is the first big step in beating them at the game.

The 4 Stages of Email Deliverability

It is important to understand that every email you send goes through a number of filtering levels before it reaches the recipient. Some of this filtering is out of your control and some of this filtering can be controlled by your actions and the actions of the recipient.

The following diagram illustrates the journey that an email will go through to reach its intended recipient:

1. Network Level
2. Server Level
3. Recipient PC
4. Recipient
The Importance of Email Deliverability

1. Network Level:
At the Network Level, your ESP (Email Service Provider) can put a number of different technologies and techniques into place, that will prepare your email for its long quest to inbox delivery.

Many different techniques have come into use over the years to ensure that the ‘good’ emails get through and the ‘bad’ ones do not. However, it is important to remember that none of these techniques are 100% effective and sometimes legitimate emails will be lost.

2. Server Level:
The success of your email passing through the server level is controlled by the owner of the infrastructure receiving the email. For example, hotmail.com is governed by Microsoft, whereas a corporate email address is generally owned by a company entity.

When the email arrives at the server managing the recipient’s domain, there will be another set of rules that must be passed to allow the mail to reach the targeted inbox. These rules are set by, and can only be changed by the server administrators.

3. Recipient PC Level:
The success of your email passing through the recipient PC level is determined mainly by the content of your email.

At this level, Spam filter software and specific user filter rules come into play. For instance your email may have a high Spam score and be blocked, or the recipient may have their mail client set to only receive emails from people who are in their address book.

4. Recipient Level:
The success of your email finally being read by the recipient is, once again, mainly determined by the content of your email.

At this level you need to consider the sender details of your message and the relevance of the subject line as these factors will be paramount in enticing the recipient to open the message.

AN IMPORTANT CONSIDERATION

List Cleanliness

The content of this whitepaper makes the assumption that your database is clean and you have the correct email addresses for the recipients you are trying to reach. If your database is ‘dirty’, it will inevitably reduce your deliverability success. It is highly recommended that you regularly clean and maintain your list to remove these invalid addresses and improve your deliverability rates.

Elements of a dirty email list include, but are not limited to:
- Incorrectly formatted email addresses
- Addresses that have previously “hard bounced”
- Addresses that have previously unsubscribed but are still active in the list
- Addresses from expired, invalid domains
The 4 Stages of Email Deliverability

This next section of the whitepaper covers the stages your email goes through to reach your recipients inbox in more detail. It also provides useful methods and tips to help you improve your deliverability.
1. Network Level

What happens at the Network Level?

At the Network Level, your ESP can put a number of different technologies and techniques into place that will prepare your email for its long quest to Inbox delivery.

Sender ID and SPF (Sender Policy Framework)

Both Sender ID and SPF have been developed as an attempt to control forged email. That is they aim to stop Spammers sending emails that look like they are coming from email addresses that are not really their own.

Sender ID and SPF aim to give mail server owners a way to say which mail sources are legitimate and which ones are not. A key consideration being that while not all Spam is forged, many forgeries are Spam.

Tips on Sender ID and SPF

Although SPF and Sender ID are not yet uniformly adopted they are becoming increasingly common as a tool in the fight against Spam. It is recommended that you check your ESP has these tools configured in their suite of deliverability tools.

Furthermore, it is also recommended that you contact the person/company who manages your domain and ask them to add SPF and Sender ID records to your emails to further assist with delivery.
1. Network Level

Domain Keys

‘Domain Keys’ is another pivotal tool in the fight against email forgery. Domain Keys helps to verify that the message really is coming from the person who claims to be sending it and that it hasn’t been altered during the sending process.

Essentially, ‘Domain Keys’ adds a digital signature to your email. The receiving mail server verifies this signature against a central system to validate authenticity.

Tip on Domain Keys
As with Sender ID and SPF, it is recommended that you contact the person/company who manages your domain and ask them to add Domain Keys to your emails to further assist with delivery.

Feedback Loops

Many ISPs (Internet Service Providers) and web based email programs now offer recipients the chance to report email they receive as ‘junk’. When a recipient chooses to flag a message as junk, if a Feedback Loop is in place, the ESP will be informed that this has happened and should normally convey this information to the sender of the email via a reporting function. These ‘junk’ reports are often referred to as ‘complaints’.

Tips on Feedback Loops
It is advisable to treat these notifications as unsubscribe requests and as such remove these addresses from your database prior to any future sends. ISPs monitor these types of complaints very closely and generally take the attitude that if the recipient doesn’t want an email then it can be counted as Spam – regardless of how legitimate you consider your email. If an ISP notices excessive amount of complaints from users, they may end up throttling back your delivery or worse still, blacklisting you.
1. Network Level

**Whitelist Agreements**

A whitelist is one component of an ISP's filtering infrastructure. Whilst whitelisting does not guarantee delivery, it can be very helpful. Generally the whitelist consists of a list of networks or email addresses, typically IP addresses or email domains that will be given preferential treatment by the ISP in the delivery process.

Your ESP may have a Whitelist Agreement with some ISPs, yet it is important to understand that this can only be achieved with some ISPs and some simply do not offer whitelisting as an option, e.g. Hotmail and Gmail.

**Dedicated IPs**

When you send an email with an ESP you may be sharing the IP address with numerous other companies who are also clients of the ESP. Therefore, the reputation of the IP address you send your mail from can be affected adversely by other companies who may not be using good practice.

The simple concept is that if you isolate your IP address so you are the only sender, you are in control of your reputation and therefore gaining control of the deliverability of your mailings. Dedicated IPs are often considered the 'silver bullet' of deliverability and whilst they may be a good option for you to consider, they are certainly not a fail-safe solution.

**Tips to Whitelist Agreements**

The most common misconception with Whitelist Agreements is that if your ESP has a number of these in place then you are guaranteed higher deliverability rates. This is not always the case, whitelisting is only one component that will help with your email’s delivery and there are a number of further parameters that must be considered and addressed to ensure your email is delivered.

**Tips on Dedicated IPs**

It is important to consider carefully if a dedicated IP is the right solution for your business. The following points should be considered when weighing up this option:

- **Volume History:** A new IP address comes with no history. This means you need to start small and earn your reputation, as many ISPs are now throttling or limiting IP addresses with no volume history to more stringent reputation thresholds. You would need to be prepared to build your reputation up – it won’t happen overnight.

- **Spikes:** The reputation of your IP address takes factors such as volume spikes into account; therefore volume needs to be managed carefully as you don’t have the ESP smoothing out the spikes of your individual mailings with other client’s mailings.

- **Cost:** Most ESPs will charge an additional fee for having a dedicated IP which needs to be factored into your overall email marketing budget accordingly.
2. Server Level

What happens at the Server Level?

When the email arrives at the recipient’s domain, there are another set of rules that must be passed. These rules are set by, and can only be changed by, the server administrators.

Black List Check

Blacklists are used to look-up information about the source of each incoming email. The idea is that if a particular machine is seen to be sending Spam this will be reported by other users, and this will be stored in a list. If a blacklist check at the server level is in place, the email may be tested against several public blacklists that have been configured and if it is detected as being one known to send Spam the message may be rejected.

Tips on Black Lists

Be diligent with your list hygiene – unsubscribe contacts who complain via feedback loops, remove permanent bounces and respect manual unsubscribe requests.

Remember, blacklisting does happen. If it does, make sure your ESP has processes in place to be removed from blacklists.
2. Server Level

SPF, Sender ID and Domain Key Check
While these tools are configured at the Network level, where they really come in to play and the benefits are realised is here, at the Server level.

Spam Filter Check
The server level presents the first round of Spam filtering your email needs to pass through. Spam filters have varying degrees of configurability. Sometimes they make decisions based on matching patterns of text whereas other times, keywords in the message body are used, URLs or perhaps the sender’s email address.

Tips on SPF, Sender ID and Domain Keys
The importance of implementing technologies such as SPF, Sender ID and Domain Keys becomes evident as they have the potential to reward you with preferential treatment at the server level for having them in place.

Tips on Spam Filter Checking
Running your email through a spam checker such as spam assassin may help you identify potential problems which may cause a message to be marked as Spam prior to sending.

To avoid being picked up by Spam filters, key points to keep in mind when constructing an email include:

- When creating HTML emails, also create a plain text version.

- Ensure you create high quality HTML emails, avoiding tools which generate messy HTML (e.g., Microsoft Word)

- If you are using HTML emails, do not use invisible text within those emails – as this text is often identified as Spam. Also avoid using “cute” spellings, don’t S.P.A.C.E out your words, don’t put str@nge letters or characters into your emails (see Appendix B for a list of words and phrases to avoid).

- If, during testing, you find that your email is being flagged as Spam, review reports and examine closely which rules are most responsible for causing the message to be rated highly as Spam. By changing a few elements of the email, you may be able to clean up the majority of the problems.
3. Recipient PC Level

What happens at the Recipient PC Level?

Your email has now arrived at the recipient’s PC and whilst the number of checks it needs to pass through have significantly decreased, the diversity and customisation of rules at this level means your email may still be filtered against a massive set of parameters.

Secondary Spam Filters

Although an email may pass through the Spam filters at the server level, individual email clients may have secondary levels of Spam filters that your message needs to pass through. For example, Microsoft Outlook has a built in Spam filter that automatically places suspicious messages into the Junk Folder.

Tips on Secondary Spam Filters

The tips for Spam Filters at the Server level also apply for these secondary Spam filters.

Custom Rules

Custom rules are put in place on an email account or client that are controlled entirely by the recipient. As the name indicates, these custom rules can vary greatly from recipient to recipient which makes them perhaps the most difficult to avoid in the deliverability process. Fred may choose to set his hotmail account to only receive emails from addresses in his address book where as Mary may have a rule that sends any message with the word ‘Free’ in the subject line straight to the ‘Junk’ folder – so even a legitimate email presenting Mary with a ‘Free’ offer will be filtered out.

Tips on Custom Rules

Although it is impossible to anticipate all the different rules that recipients may place on their email clients, one idea to help with some of these general rules is to include a request in your email for the recipient to add the sending email address to their ‘Safe Senders’ list. Emails sent from this address would then in future always be delivered directly to the recipient’s inbox, provided no other deliverability issues are encountered.
4. Recipient Level

What happens at the Recipient Level?

Your email has finally arrived in your recipient’s inbox, yet after passing through all the various filters so far, it still faces the biggest test, actually being read by the recipient.

Despite the automated filters outlined in this document, sometimes Spam does make it to the inbox and recipients have become used to having to manually filter some Spam. Therefore, at this level there are two key filters you need to consider.

Sender Recognition

One of the first details a recipient is likely to look at prior to opening an email is who the sender is. If the sender is recognised, the email is likely to be opened. However, if an email is received from a sender of whom there is no prior knowledge, it is likely that a secondary filter (subject line) will be applied before opening the message.

Tips on the Sender

Choose a regular ‘From Address’ and ‘From Name’ to use for your emails; this will usually be your name and/or your organisation’s name. This will ensure that these details become familiar to readers so they easily identify the emails relevance and ideally will add you to their address book.

Appealing Subject Line

The main purpose of a subject line is to achieve an open and it is important to remember that you only have about 45 characters to capture a reader’s attention.

In some cases a dubious subject line may be recognised as Spam and deleted by the recipient before being opened. ‘Please contact him for your..... BANK DRAFT PACKAGE!!!!’

Even if a recipient has recognised the sender, they may still refer to the subject line to help them decide whether they will open the email or not. For instance, if you subscribe to emails from Amazon.com you may not open and read 100% of the emails sent by Amazon.com. However, when you receive an email with the subject ‘Amazon.com: Top 10 Deals in Electronics’ you know immediately the relevance of the email and choose to open the email to read the full message.

Tips on the Subject Line

Ensure the subject line accurately communicates to the recipient what the email is about whilst also providing an incentive where possible to open the email and read more.

Ensure the subject line does not create friction and anxiety for the reader that might ultimately discourage the recipient from opening the email.
Glossary

**Blacklist**
This is a list of the domains or IP addresses or URLs suspected of being involved in sending spam. Many companies use blacklists to filter out unwanted inbound email.

**Dedicated IP**
An IP address which is assigned to one specific organisation, which does not change, and which is not shared amongst multiple resources.

**ESP**
Email Service Provider providing email services, an email service provider (ESP) offers email marketing or bulk email services.

**Expired Domain**
A domain name whose renewal date has passed, but which has not yet been dropped from the domain name system.

**Feedback Loop**
The process by which the email client (ISP) of the receiver forwards complaints of emails marked as Spam by recipients for removal by the sender.

**Hard Bounced**
Returned to sender email message because the recipient’s address is invalid. A hard bounce might occur because the domain name doesn’t exist or because the recipient is unknown.

**HTML Email**
A HTML email is a full-color, email message. It usually contains graphics and links to web pages, or “landing pages.” HTML (Hypertext Markup Language) is the computer programming language used to build web pages and full-color, interactive emails.

**IP**
An Internet Protocol (IP) address is a numeric identification (like a phone number) that is assigned to devices participating in a computer network utilizing the Internet for communication.

**ISP**
An Internet service provider (ISP) is a company that offers their customers access to the Internet.

**Sender ID**
Sender ID is a method major Internet service providers (ISPs) use to confirm whether emails are actually coming from the company they say they are coming from.

**Server Administrator**
One who manages and maintains computer systems and software, as for a business or institution.

**Spam**
This is slang for junk email, also known as unsolicited email. These are emails that are sent to large numbers of recipients trying to sell them on everything from weight loss products to loans, and are often associated with scams.

**SPF**
SPF aims to stop email spammers from forging the “From” fields in an email.

**Whitelist**
This is a list of “accepted” email addresses that an ISP, a subscriber or other email service provider allows to deliver messages regardless of spam filter settings.
Appendix A

Calculating Deliverability Rates

Step 1:
Divide the number of bounced emails by your total send volume and then multiply by 100 to achieve a percentage. This will give you your percentage bounce rate.

Step 2:
Subtract the above calculated percentage bounce rate from 100% to achieve your percentage deliverability rate.

For Example
The diagram below provides actual statistics from a recent campaign.

To calculate the deliverability rate:

Step 1:
\[
\frac{140}{3689} \times 100 = 3.8\%
\]
Number of bounced emails divided by total send volume, multiplied by 100

Step 2:
100% - 3.8% = 96.2%
Subtracted the bounce rate from 100%

Thus the deliverability rate from this campaign = 96.2%
### Appendix B: Subject Lines to Avoid Using

| Contains $$$                                                                 | Free membership          |
| “100% Free”                                                                | Free offer               |
| Contains word “ad”                                                         | Home based              |
| Apply now                                                                  | Homebased business       |
| Earn $                                                                     | Income from home         |
| Earn extra cash                                                            | Increase sales           |
| Explode your business                                                      | Increase your sales      |
| Double your income                                                        | Incredible deal          |
| Eliminate debt                                                            | Info you requested       |
| Extra income                                                               | Internet market          |
| Free                                                                       | Limited time offer       |
| Fast cash                                                                  | Make $                  |
| Financial freedom                                                         | Web traffic              |
| Financially independent                                                   | Weight loss              |
| Free gift                                                                  | Online marketing         |
| Free info                                                                  | Save $                  |
Appendix B: Words & Phrases to Avoid Using

100%  access
50% Off!  Freedom
Aging  Full refund
Amazing  Great offer
Best rates  Guarantee
Big savings  Guaranteed
Breakthrough  “Hidden”
Call now  Income
Cash bonus  Increase
Checks  Incredible
Completely free  Investment
Consolidate (bills)  Limited-time only
Coupons  Loans
Credit card  Lose weight
Credit  Marketing solutions
Discounts  Million dollars
Double your income  Mobile phones
Earn $  Money back
Eliminate debt  Money order
Exercise  Mortgage information
For free  Multi level marketing
Free!  No cost
Forward to a friend  Now only
Free consultation/free  One-time mailing
Opportunity
Opt in
Please forward
Promise you
Quote (no obligation)
Refund
Remove/removed/
Removal
Risk free satisfaction
satisfaction guaranteed
Save up to
Serious cash
Special promotion
“Stop” or “stops”
This is not spam
Urgent
What are you waiting for
Win
Wrinkles
You’re a winner!
Your own
About Vision6

Vision6 is an Australian owned and run company. We were founded in 2001 by friends and colleagues Evan Fortune and Mathew Myers.

Together they identified that marketing professionals needed an easier way to create, send and track email messages; and to integrate e-messaging into the marketing mix. As a result the duo formed Vision6.

From two guys in a tin-shed (well Mat’s living room – close enough) we’ve grown to become a team of more than 30 developers and professionals.

Today, we are passionate about all things e-messaging. We empower thousands of businesses to achieve great marketing results. And we are always on the lookout for new ways to make our clients happy.

We also contribute to the marketing community by writing whitepapers, providing free training, producing the Email Marketing Metrics Report and organising Australia’s only email marketing summit (EMSA).

Contact Vision6 for a FREE 30 DAY TRIAL

ground floor 47 warner street   fortitude valley qld 4006 australia
emarketing@vision6.com.au   p+61 7 3257 3906   f+61 7 3257 3907