Email Deliverability Explained

How To Get Email Into The Inbox

Second Edition

SAMPLE CHAPTER

https://emaildeliverabilityexplained.com/

Chapter 3
Message Filters and Message Streams

This chapter covers message filters and streams. It explains the different types and purposes of filters. It also explains what message streams are and how they can be used to work with filters.

Message filters are specialist pieces of software designed to classify messages and decide if they reach their intended destination, for example a recipient's inbox, or not. A filter can be a software application which is installed on an email server, a dedicated hardware appliance, or built-in to an email client. To learn more about email servers and clients, see Chapter 2. Message filters can also be hosted on the internet and provided as a service.

Filter Actions

Message filters can perform several actions on email messages.

1. Move the message somewhere other than the inbox, such as the "spam" folder or a quarantine area.

2. Modify the subject of the message. For example, by prefixing "SPAM" or "EXTERNAL" to the original subject.

3. Add a special message header, such as the results of email authentication checks. For more information on email authentication, see Chapter 11.

4. Refuse to deliver the message. This typically causes a bounce message to be generated. For more information on bounces, see Chapter 7.

5. Silently delete the message.

The action a filter takes is determined by the individual filter configuration. The default settings of most filters will not silently delete messages; the filter must be specifically configured to do so by the user.

Filter Purposes

Message filters have four main purposes - security, spam, authentication and compliance.

Security

Security filters look for attachments and other message content which may pose a risk to the recipient. These filters often look for computer viruses and malicious software (malware). Sometimes, security filters will follow the links in messages and scan the websites they are pointing to. Following links can cause issues with “open rate” metrics, this is explained in Chapter 4.

Spam

Spam filters look for signals which indicate that the message is potentially spam. These filters are often based on a scoring system. Each spam signal increases the score until the threshold is reached, and the message is presumed to be spam. Of course, some signals can increase the score such that their presence alone can cause a message to be marked as spam.

The many different types of spam filtering technologies are explained in the coming chapters.

Blocklists	Chapter 5
Domain and IP Reputation	Chapter 8
Content	Chapter 9
Engagement (recipient behaviour)	Chapter 10

Spam Filter False Positives

Sometimes, a spam filter makes a mistake and marks a non-spam message as spam. This is called a false positive. False positives can occur for many reasons from poorly maintained filtering software to a message having too many similarities to previously detected spam. For more information on false positives related to similar looking messages, see

Checksum Based Filtering in Chapter 9. Information on contacting providers to report false positives is provided later in this chapter.

When a spam filter does not detect a spam message and lets it through, it is known as a false negative. For spam filter software to be considered reliable, it must have consistently low false positive and false negative rates. Not every organisation operates reliable spam filters. For this reason, false positives are a possibility that must be kept in mind when diagnosing deliverability problems.

Authentication / Policy

Authentication filters investigate whether a message conforms to certain email authentication technical standards. Email authentication is covered in Chapter 11.

Compliance

Compliance filters look for specific message content, or other properties related to the compliance rule they are tasked with enforcing. For example, a compliance filter may be set to block customers from emailing credit card numbers to the billing department. These filters are usually used to enforce regulatory compliance. The specific filtering rules are determined by the organisation using the filter. Such filters are common in financial, pharmaceutical, and other regulated industries. Resolving problems caused by compliance filters typically involves removing the offending content from your messages or contacting the organisation directly to respectfully request that your messages bee allowed through.

Outbound message filtering

When dealing with email deliverability it is common to think that only the recipient's email system has message filters. After all, it is typically the recipient who will claim they never received a message, or it was received but landed in the spam folder. While it is true that many deliverability issues relate to the recipient's email system, that is not always the case.

Message filters also exist on the sender's email system to scan their outbound messages. It is common for mailbox providers and corporations to do their best to block their users from sending messages with viruses attached. Corporate email systems will often additionally use compliance filters to scan outbound messages. For example, some

compliance filters restrict what type of files can be attached to outbound messages.

When diagnosing a deliverability issue, always ensure that the message left the sender's email system first. This can usually be achieved by looking at the logs on the sending email server.

Mail Streams

A typical organisation may send out many different types of messages. For example, they may send out a newsletter to all their customers, replies to customer support tickets, and send general correspondence. Many message filters divide these different types of messages into categories, often referred to as mail streams. The most common mail streams are:

Regular / one-to-one

Regular messages are typically personal, or business messages sent over a day or series of days. They are not sent in bulk and only to a single or small number of recipients. They are also sent from an address associated with a person, and not a role account such as sales@example.com. Regular messages typically receive replies and are sent to recipients who may have the sender address stored in their contact lists.

Transactional

Transactional messages are associated with fulfilling a service. Examples of transactional messages include electronic invoices, support ticket updates, and password reset instructions. They are typically sent from an address associated with a role, and not an individual. Many transactional messages are time sensitive and need to be delivered as soon as possible.

Marketing

Marketing messages are promotional in nature. Examples of marketing messages include newsletters, new product announcements, and abandoned cart notifications.

Keeping streams separate

The more advanced message filters, especially those operated by large receivers, often treat different message streams differently. For example, a spam filter may be designed to be more lenient with bulk messages that look transactional in nature while scrutinising others more closely. This is common sense as recipients are not particularly tolerant of password reset messages landing in spam, for whatever reason. Likewise, individual messages may be treated differently to bulk messages, even if they have the same content. For this reason, it is always a good idea for a sender to clearly distinguish different mail streams, both by content and sending means.

The most important way you can use content to distinguish streams, is to never mix transactional and marketing content in the same message. For example, including a special offer in a password reset notification may cause the message to be considered as marketing related. This could result in it being treated differently, such as with delayed delivery.

Traditionally, the recommended method for technically distinguishing different streams was to send them from different IP addresses. These days, while it will not do any harm, the use of dedicated IPs is not nearly as important as it was.

A good way to distinguish different streams is to use different DomainKeys Identified Mail (DKIM) signing domains on each stream. For more information on DKIM, see Chapter 11.

Another method of distinguishing streams is to use different sub-domains for each stream. For example, newsletter@email.example.com and sales@crm.example.com. Using different sub-domains will help segment domain reputation between the two domains, which can help limit deliverability problems. For more information on domain reputation, see Chapter 8.

Putting it all together – Mail Providers

Maintaining a reliable email system can be expensive and time consuming. It is for this reason that most organisations outsource some or all their email requirements to third parties. The most common third parties that manage email on behalf of organisations are Email Service Providers, Mailbox Providers, and hosted software solutions.

Email Service Providers

Email Service Providers (ESPs) have email systems which are designed to send high volumes of email messages very quickly. They typically offer additional services, such a web interface to create and track the success of email campaigns. ESPs may also record bounce messages (see Chapter 7) and complaints.

There are many different types of ESP. For example, some ESPs focus purely on marketing messages, while others include social media messaging features. There are also ESPs which specialise in sending transactional messages.

Specialist ESPs also exist to service niches. For example, some ESPs specialise in sending bulk messages for non-profit organisations.

Mailbox Providers

Originally, Internet Service Providers (ISPs) bundled email services along with connections to the internet. Over time other organisations began to offer email services too. This book uses the term Mailbox Provider (MBP) when referring to both traditional ISPs and newer providers.

They typically offer message sending, receiving, storage, and filtering services. Others may also offer hosted address book and calendar features.

MBPs typically do not intend their services to be used for sending large volumes of messages and may even suspend users who attempt to do so. To send bulk messages properly, you need an ESP.

Many MBPs use message filters which make decisions based on the volume of complaints associated with a particular sender. If enough

recipients use the “report spam” option, it can hurt deliverability by causing all your email to go straight to the spam folder.

Some MBPs provide feedback to senders on recipients that mark messages as spam. They do this via Feedback Loops (FBLs). FBLs are an automated way for mailbox providers to report information on complaints back to the sending ESP. The ESP will typically present this information to their users on a dashboard along with other metrics.

Larger MBPs, such as Yahoo! and Microsoft operate their own FBL service. Other providers offer FBLs via a third-party service operated by a company called Validity.

Google does not provide a traditional FBL service. To use Google’s FBL a sender must include a special message header in their bulk messages. Google provides aggregate data on the number of complaints via their Google Postmaster Tools service.

Larger MBPs often provide a way for senders to contact them in cases where they believe that their messages are being filtered incorrectly. This is commonly referred to as “contacting the Postmaster”.

Hosted Software

Hosted software, often referred to as Software as a Service (SaaS), is software which is delivered over the internet. For example, the Customer Relationship Management (CRM) software provided by Salesforce, the accounting software provided by Xero, and the Calendly calendar booking tool are all hosted software solutions.

Hosted software solutions can either send through an organisation’s existing MBP, use a third-party ESP, or use their own email systems.

Self-hosted email systems

Some organisations do not outsource their email and instead use commercial or open-source email systems which they install and maintain themselves. It is very difficult to diagnose deliverability problems with these email systems since it cannot be known how the message filters have been configured.

It is important to choose the right mail provider for the type of messages you intend to send. Not doing so can result in deliverability

challenges which are avoidable. For example, do not use a mailbox provider for sending bulk marketing messages.

This chapter covered message filters and mail streams. Message filters can scan, re-direct and even delete messages before they reach the inbox. Filters typically scan for security risks such as viruses, spam, and problems with email authentication. Organisation-specific filters can also scan for prohibited words and phrases specific to that organisation's policies. Filters can treat different message streams differently. Transactional messages such as password-resets may be treated more leniently than marketing messages. It is best practice not to mix transactional and marketing content in the same message. You can use different sub-domains and DKIM signing to differentiate message streams. There are different types of mail providers for different message streams. It is important to choose the right provider for your content. For example, you should use an ESP for sending bulk messages and not an MBP.