Reaching the Inbox - Monitoring and Managing Email Deliverability.

Transactional documents such as invoices, contracts and pay slips are the lifeblood of any company. Today, more than 50% of these documents are delivered via email around the world. Ensuring these emails reach their intended audience should be the driving force behind engaging a third-party to deliver transactional emails on behalf of your business.

While it is reasonably easy to measure your deliverability, the metric to be used needs to be agreed at the outset and constantly monitored to ensure it is met. Changes to the email delivery landscape should be addressed as a matter of urgency to maintain your sender reputation and rate of delivery.

Financial Benefits

The most obvious reason to monitor and maintain the highest rate of delivery possible is financial. Every rejected email is a missed communication and could result in the need to place the message into a "print and post" stream for delivery, with all the associated costs. To see just how much of an impact this can have on your business' bottom line, simply insert your transactional message details into our handy Cumulo9 Deliverability Calculator.

An equally strong benefit of increased delivery of these essential messages by email is the impact on day's sales outstanding (DSO). Our BOC case study shows that while BOC has always had a good DSO record, since the introduction of Mailpost they are achieving less than 38 days DSO.

Deliverability Steps

The science behind getting email delivered is complex, however there are a few simple steps organisations can take, in collaboration with their transactional email provider, to ensure their messages get through – all of which ensure recipient servers recognise your emails as the genuine article, from a trusted source.

Step One - Sender Policy Framework

The first of these steps is ensuring your domain's SPF (Sender Policy Framework) record is up-to-date and reflects the IP addresses of all servers which deliver emails on behalf of your domain. Strict enforcement of your SPF record is encouraged, once you have determined all sources of company email are correctly represented in the record.

If your domain does not have an SPF record in place, or if your SPF is incorrect, the likelihood of your messages being rejected as suspected spam is high, and rising every day, as more and more ISPs enact SPF validation as the basis of their spam profiling.

SPF ensures recipients that the message is authorised by your organisation. Once in place, the next step to ensure deliverability is to implement Transport Layer Security (TLS) for the delivery of messages. TLS provides a cryptographical secured channel for the delivery of your messages. This provides recipients with the surety of both privacy and data integrity.

Step Two - DomainKey Identifed Mail

The next step in improving your domain's reputation for genuine, secure email delivery is to implement DomainKey Identified Mail (DKIM). DKIM lets your transactional email provider take responsibility for messages in transit, providing the recipient with a method for validating your domain name identity with the message received. In short, DKIM is an authentication method design to detect email spoofing using end-to-end digital signatures to guarantee the some parts of the email have not been modified since the signature was affixed.

Step Three - Domain Based Message Authentication, Reporting and Conformance

Once you have SPF and DKIM in place, it is possible to implement Domain-based Message Authentication, Reporting and Conformance (DMARC) as the top-most level of authentication for your domain's emails. DMARC allows your organisation to indicate that your messages are protected by SPF and/or DKIM and to instruct the receiver what to do if one or both of those methods fails – such as to place the message in a junk folder or to reject it outright. DMARC protects against direct domain spoofing and provides a way for the recipient to report back to the sender if messages pass or fail DMARC evaluation.

Email Placement Influencers

Even with all these protocols in place, it is still possible to have messages rejected or placed in the junk mailbox. Several other factors can influence placement, primary amongst these being your email reputation score with the receiver ISP. Email reputation is built over time and through careful management of the emails you send. Every email sent to an invalid address at a recipient domain, could potentially impact your reputation, so it is important to cleanse bounced emails with urgency and replace or remove out-of-date email addresses from the systems used to generate your essential documents.

Equally, the content of the email itself can have an impact on message placement and a good service provider should be able to assist you with modifying the content, including templates and graphic elements, to achieve the best delivery possible.

Deal With SPAM

Once an email is accepted by a recipient server, it is not guaranteed to reach the user's inbox. ISPs seek to protect their mailbox users and have a variety of restrictions in place on what is accepted and if it is delivered to the inbox or another folder, or quarantined. The major ISPs (Gmail, Hotmail and Yahoo, for example) provide feedback loops to email service providers and it is important that any messages which are reported as spam by their users to your email service provider should be dealt with as a matter of urgency.

According to ReturnPath, globally, one in five messages does not reach the inbox. By way of comparison, Cumulo9's Mailpost has a world class measured deliverability of 99.5%.

Email Delivery Levels Vary Considerably

Delivery to the recipient's server, however, is not the end of the road. In their latest annual benchmark report, ReturnPath's analysis shows that, of the emails which do get through, inbox placement in the US is only 77 percent, while Canadian and Australian marketers achieve 90 percent, with Brazil, France, Germany, Spain and the UK falling between those two points.

As more mailbox providers begin to utilise recipient engagement in their email placement decisions, it is important to monitor customer behaviour with regards your communications and to encourage receivers to interact with your messages correctly, beyond simply asking them to add your sender address to their contact list (though that is a good idea, too). To this end, if a recipient reports that an email has been placed in the junk, promotions or another folder, they should be advised to move the message to the inbox before opening it. They should also be advised not to delete it from the spam folder under any circumstances, even if it has been viewed or clicked on, as that action can be misinterpreted as confirmation that the user believes the message is spam.

In view of these considerations, it is also recommended that organisations utilising a transactional email service, put in place a seed list of email address across the major ISPs. Once the list is in place, it is important to ensure that not only are emails regularly sent to the seed addresses, but that they are also opened and clicked on. In the unfortunate event that a message does end up in a folder other than the inbox, you can move it to the inbox and interact it with to ensure future emails are labelled correctly.

For More Information

For further information on how to maximise your transactional email ROI, visit our Mailpost product listing or get in touch with the team at Cumulo9.