RETARUS WHITEPAPER

Reputation management, a key factor in your company's success:

How your emails are placed exactly where you want them to be

Contents

Whether you're dealing with orders and invoices, or registration and order confirmations: For crucial business processes you need to be able to rely on your emails safely reaching their recipients' inboxes. Along with newsletters, customer service requests and other interactions, however, a huge volume of email which needs to be sent in a short space of time is soon generated. Email providers often misconstrue such messages as spam, meaning that legitimate, sometimes business-critical, emails are not delivered. How can you ensure that your emails are found in the inbox, and not hidden in the junk-mail folder?

Successful reputation management allows your messages to get through

More than **50%** of email is **spam**

Your sender reputation plays a crucial role in maintaining a consistently high delivery rate for your emails. Across the globe, more than half of all emails sent are spam[1] , which email and Internet service providers already filter out in advance with a high degree of accuracy. This generally happens on the basis of comprehensible attributes such as content (key words that suggest spam), composition of the message (ratio of text to pictures) or the technical set-up – for instance SPF/DKIM.

Poor reputation
leads to blocking und blacklisting

Especially for large volumes of email, however, providers also have a tendency to classify legitimate emails as spam. You can counteract this with effective reputation management, which has one main aim – making it evident to the receiving provider that the inbound email is not spam, but in fact a legitimate message. Especially relevant in this regard is the public reputation of the send-

1 Symantec email spam rate, available at: https://www.symantec.com/security-center/publications/monthlythreatreport (May 2, 2019).

ing IP address and the sender domain. If emails from a specific sender have frequently been classified as spam, then the sender reputation falls – as a result the probability increases that future emails may end up in the spam folder. A poor reputation can lead to temporary blocking or even permanent blacklisting of the IP. Emails from senders or IP addresses that wind up on such "blacklists" may even be rejected directly by email providers. To avoid this occurring and to ensure that your reputation remains consistently high, effective and active reputation management is essential. Many businesses rely on experienced specialists to implement the necessary reputation management measures – and to guarantee that their business processes keep functioning.

1. Email authentication is an essential building block for a good reputation

SPF,DKIM, DMARC-
authenticated gets better received

An important component in effective reputation management is the authentication of the technical and organizational sender. In this way, it can be made certain that sender addresses are not being faked and that only authorized servers can send emails. Of particular relevance are the use of SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting and Conformance). While SPF utilizes an entry in the DNS to stipulate who is allowed to send emails from a specific domain, DKIM makes it possible to check whether an email has actually really been sent from the declared sender domain. DMARC builds on these two approaches, additionally providing the opportunity to include rules for dealing with non-compliant messages. Authentication quickly fails if these methods are not set up correctly. Emails coming from the sender address are then automatically identified as an attempted scam by the receiving provider and classified as spam.

2. List-Unsubscribe Header supports recipients in unsubscribing from unwanted newsletters

In July 2019
CSA has made
One-Click-Post-Headers mandatory

What may at first seem to go against any marketer's intuition is, on closer inspection, an important factor in successful reputation management – the option of immediately unsubscribing from distribution lists. The very worst thing that could happen to your corporate email is for the recipient to mark your message as spam. This has grave repercussions on your reputation with the provider concerned. In addition to the mandatory inclusion of unsubcribe links at the end

of each message, it is thus also highly recommendable to already include the option of unsubscribing technically in the header of the email. This List-Unsubscribe option is already supported by well-established email clients and webmail services. In this way, recipients can immediately deregister from mailing lists for messages they no longer wish to receive. The option reduces the probability that the message will be marked as spam, helping you to safeguard your reputation. An extension to List-Unsubscribe is becoming obligatory for all those sending marketing emails using CSA-certified IP addresses as of 1 July 2019. Then an additional "One-Click-Post-Header" will make it possible to unsubscribe with just one click. It is generally advisable to make use of this function.

3. Bounce management and suppression lists prevent the reputation from deteriorating

Managing bounces effectively is a key element in reputation management

When sending emails, it often occurs that messages can temporarily or permanently not be delivered. In such cases, ISPs and ESPs send a notification message known as either a soft or hard bounce back to the sender. Although this may hardly seem significant to the sender at first glance, the receiving providers perceive recurring events of this kind as illegitimate sending behavior – meaning it has a negative impact on an assessment of the sender's reputation.

While soft bounces require repeated attempts to deliver the message, hard bounces must be recognized as permanent failures and any renewed attempts at delivery should be discontinued to avoid a negative impact on the sender's reputation.

Non-existent email addresses are automatically placed on a "suppression list", which prevents multiple attempts at sending messages to recipient addresses that have already been rejected, giving you the opportunity to clean up your distribution list.

The suppression list can also prevent the transmission of emails to so-called "spam traps" or "honey pots". Email providers are interested in filtering spam out of the regular email traffic as accurately as possible. They use special email addresses (e.g. deleted email accounts) to collect spam emails and analyze the behavior of senders. State-of-the-art email delivery services recognize these kinds of email addresses and domains, filter them out from amongst genuine recipients and automatically add them to the suppression list. As a key element in reputation management, effective bounce management makes sure that instead of stumbling into traps, you keep your slate clean.

4. Use various IP addresses and domains for bulk transmissions

IP routing can prevent blacklisting und blocking

Especially when dealing with large volumes of email messages, keeping different sorts of communication separate from each other, not only in terms of their content but also technically, has proven to be a good strategy at numerous companies. One option in this regard is IP routing, in which emails from differing domains/campaigns are sent using different IP addresses. The email address communicated to the recipient can still remain identical, allowing the authenticity of the email to be verified on the recipient's end. Email communication then still reaches its recipients, even if the employed IP addresses partly end up on a blacklist.

5. CSA Certification guarantees quality standards in email transmission

Better inbox placement through CSA-certified delivery

Your sender reputation is boosted by certifications. The Certified Senders Alliance (CSA), a project set up by eco – Association of the Internet Industry in cooperation with the German Dialog Marketing Association (Deutschen Dialogmarketing Verband), certifies senders, email service providers and other businesses. The alliance regularly informs its members of technical and regulatory innovations or changes, keeping them up to date with the latest developments and protecting them from legal and financial risks by allowing them to remain compliant with regulatory guidelines. The members commit themselves to complying with strict legal and technical quality standards when sending commercial emails. In return they are added to a centralized whitelist. Sending emails via a CSA-certified service increases the delivery rate of your emails with providers that are also signed up to CSA – including Microsoft (Office 365 and outlook.com), AOL, Yahoo!, Yandex, Web.de, 1und1 and GMX. These major ISPs refrain from server-side filtering for emails from CSA-certified senders. Another benefit of the certification is an efficient early warning system, which alerts senders of existing problems prior to them having a detrimental impact.

Reputation management plays an integral role in the success of your business

These five elements constitute the core of an effective approach to reputation management, enabling you to keep your email delivery rates consistently high. Even so, the protective measures that email service providers employ against the high volumes of spam messages are constantly evolving. In line with these changes, the measures for effective reputation management also need to be adapted accordingly. A professional partner can support you effectively in this process and ensure that your reputation remains positive – so that your emails end up exactly where you would like them to.