BIZCOMMUNITY

Pitfalls of neglecting your email delivery

By JD Engelbrecht, issued by Everlytic

24 Nov 2021

Email marketers face a myriad of challenges in sending emails at scale and ensuring that as many as possible get read, whilst avoiding the technical pitfalls that may lead to blacklisting and a complete stop of delivery. And the stakes are always high: a 10% lower delivery rate means a similar reduction in sales, people attending an event, and chances of KPIs being hit. Fortunately, by managing just a few aspects more strategically, companies and marketing teams can quickly see a meaningful and hugely positive difference in their email campaign results.

To begin with, delivery and sender reputation are the crucial differentiators. But what makes a company a 'safe' sender and what affects its classification (i.e. that could see it labelled as spam and even potentially be blacklisted by monitoring organisations)? And what makes one email service provider (ESP) better at delivering email than another?

Email delivery can be a complex undertaking. We simplify this by using the analogy of the mailman. If a mailman is trusted and delivers the mail to the right people in an apartment building, then the supervisor will always let the mailman in. But if the mailman starts slipping in too many unsolicited messages or doesn't follow the rules of the building, then eventually the supervisor could deny him entry. The same logic applies to email messages.

Gaining access: DKIM and SPF checks

At this point, we need to take the analogy a step further. Consider that the mailman works for a post office – which is comparable to an ESP such as Everlytic. Each mailman uses uniforms representing the ESPs and carries branded bags filled with the mail from various senders – clients of ESPs delivering on their behalf. The sender of the message gives authority to the post office, who sends its mailmen to deliver.

The mailman obviously needs some form of authorisation to get into the building. In the email world, this is called authentication. The building supervisor can see that the mailman is carrying a mail bag with the sender's logo and is wearing a uniform of the post office which they know and trust. He also needs an identity tag that can be scanned to confirm he is authorised by the post office and is truly acting on behalf of the sender.

Think of the mailbag as the 'from-envelope' address in the email and the mailman as the IP address belonging to the ESP across which email is delivered. The way the mail system checks the validity of that address is through SPF (sender policy framework) and DKIM (domain keys identified mail) checks. The SPF check aligns the IP addresses to the organisation that has the authority to send the email on behalf of the sender, while the DKIM does the job of the identity tag of the mailman – his integrity check.

Getting this right is critical to email delivery, as it adds an extra security layer of authentication on top of your emails which prevents them from being classified as spoofing or phishing. It is important that the sender domain reputations of both the ESP and the sender are as positive as possible, to ensure receiving email domains and servers trust and accept the content.

Protecting email recipients

Being able to authenticate and be trusted when delivering mail in our analogous apartment building, is by no means the only consideration. In addition to delivering unsolicited spam or breaking the rules of the building, if the recipient's experience is poor, the content is not relevant or harmful, or mail keeps coming to people who don't live in the building anymore, then the recipient will stop opening the mail before too long or start complaining to the building supervisor.

And if enough of the building's people do this, the supervisor will refuse entry to that specific mailman. This would mean

any mail from that mailman's other senders' bags – who never did anything wrong, as well as the legitimate messages in the branded bags of the offenders also won't make its way to its recipients.

This equates to an IP address being blocked by spam monitoring organisations from delivering mail. This will negatively impact both the delivery and sender reputation. The job of the spam monitoring organisations (building supervisors) is to monitor delivery via IP addresses and ranges and to ultimately protect people from receiving unsolicited, harmful, or irrelevant emails.

One of the ways they do this is by creating spam email boxes or converting very old domains into spam domains. These would have been out of circulation for a while. If your business sends emails to these spam email boxes or old domains, it flags on their side that either you or your service provider are not doing proper database management and are therefore spamming people – hence the term spam trap.

You hate robocalls for the wrong reasons

JD Engelbrecht, Everlytic 29 Jun 2021

Denied entry

If enough of a service provider's IP addresses (mailmen) are flagged, its entire IP range or domain (corps of mailmen) might get blacklisted along with the sender's domain causing incredibly challenging technical problems to solve.

In the past, spam mail was automatically classified. More recently, spam monitoring organisations take a more nuanced approach in addition to the measures discussed above. For example, a customer opened a clothing store account a year ago but has not been opening any marketing emails for the past 11 months. Technically, said company, can now – under the rules of the spam monitoring organisations – be seen as spamming the customer because they are no longer engaging with the content.

Spam monitoring organisations, therefore, fulfil a critically important role for customers to 'protect' them against spam or malicious emails. So, even though they are setting these spam traps, there is no malicious intent. In fact, many service providers work with spam monitoring and prevention organisations to ensure they are operating as effectively as possible. It really is an integrated ecosystem whereby most stakeholders only have the best interests of their respective customers (whether those sending the emails or those on the receiving end) in mind.

A delicate balancing act

Unfortunately, service providers and the companies themselves rarely get alerted that they have been blacklisted. Even if they are, these messages are invariably sent from a 'no-reply' address and automatically gets filed in some obscure location by the service provider or the organisation.

Being blacklisted affects both promotional and bulk messaging, as well as transactional messages like OTPs, invoices, account verification, and other business-critical correspondence. Simply put, being blacklisted can grind a business to a halt.

This is why it is so critical for a company to use an ESP that is good at what they do, and is geared to tend to all these complexities … proactively! Not only does this ensure that all email messages go through, but also that they are read by the intended recipients. Sure, companies can manage and send their own email campaigns, but there is no way of understanding all the complexities involved. Rather, work with an expert that has all the tools and systems in place, and who understands this complex ecosystem.

Ultimately, by not having to focus on the delivery of email, the company can look at creating the most engaging content that

brings the most value to the recipients – which is far more beneficial and value-adding in the long run.

ABOUT THE AUTHOR

JD Engelbrecht is the managing director of Everlytic.

- **Everlytic frees up email marketing capacity for SA businesses** 15 May 2024
- **Enter Everlytic's You Mailed It Email Marketing Awards today** 23 Apr 2024
- **Everlytic launches new playbook for email marketing success** 22 Mar 2024
- **Everlytic demystifies new email authentication protocols** 11 Mar 2024
- **Boost open rates with inspiration from top 10+ valentine email subject lines** 13 Feb 2024

Everlytic

Everlytic is the leading Cloud Marketing Software solution in South Africa. Every day hundreds of top South African and international companies use our software to send millions of messages to their customers and subscribers. With our bulk and transactional email and SMS engines you can manage all of your digital communications from one central hub. Whether it be newsletters and notifications, to statements and system generated messages, Everlytic is the leader in ensuring top delivery rates.
Profile | News | Contact | Twitter | RSS Feed