WE ARE SHAPING THE INTERNET.

Best Practices for Email Marketing

... How Marketing Emails Land in Recipients' Inboxes

eco Competence Group E-Mail

Table of Contents

Authors: Marius Bauer (Experian Marketing Services), Mathias Ullrich (optivo GmbH), Florian Vierke (Mapp Digital)

Editor: Mathias Ullrich (optivo GmbH)

Contributors: Sebastiaan de Vos (MailMike.net), Sven Krohlas (1&1 Mail & Media GmbH), Gunther Nitzsche (NetCologne Gesellschaft für Telekommunikation mbH)

Thanks to: Andre Görmer (Mapp Digital), Arne Laske (optivo GmbH), Alexander Zeh (eco - Verband der Internetwirtschaft e.V.)

Introduction

Email marketing is an efficient and inexpensive part of the online marketing mix. In a survey by the German Federal Association of the Digital Economy (BVDW), 84 % of all those questioned indicated that they use email for online orders (more information on this survey is available through the Focus Group E-Mail in the BVDW)[1]. For small and medium-sized companies without huge resources or budgets, it is easy to set up an email marketing program to inform customers and prospects about current products and services.

But it's not as simple as all that. To make sure that the advertising messages reach the recipients, it is not enough to simply "go for it". Not every email that is sent actually lands in the receiver's inbox. Some emails are directly rejected by the mail server, and others are delivered to the spam or junk folder. This guide explains how simple measures can be implemented to build your email marketing in such a way that the emails actually get to the receiver.

Risks

Properly implemented, email marketing offers great revenue potential. However, there are also risks. For one thing, mailbox providers can reject entire campaigns. So-called blocking can occur, for example, if too many non-existent email addresses or so-called spam traps (see "Data Collection – What are Spam-Traps?") are written to. Through blocking, the mailbox provider wants to protect its own infrastructure and its customers. Blocking is, as a rule, easy to detect, as the mailbox provider does not accept the emails and answers them with an error code (see "List Hygiene – Bounces").

The second risk and the corresponding consequences are difficult to detect. If a mailbox provider no longer places the emails in the inbox, but instead in the junk folder, this can only be detected through the open rate. In particular, this does not show if the target domains have a small share in a mailing.

Both risks have a strong influence on the success of email marketing. Messages that are not delivered or that land in the junk folder generate little or no revenues.

[1] http://www.bvdw.org/medien/bvdw-whitepaper-zur-wechselwirkung-von-e-mail-und-social-media?media=7575

Reputation

Reputation is an important term in the context of email deliverability. Simply put, the reputation describes the regard that the marketer enjoys from the mailbox provider. Here, it is not only the first impression that counts. Rather, a change in reputation – both positive and negative – is always a process. A single mistake can cause long-term damage. Improving it again takes disproportionately longer.

There is no specific figure for reputation that a marketer can adhere to. Every mailbox provider works with individual, differently weighted factors. In 2014, the Gmail Product Manager Sri Harsha Somanchi commented in an interview[2] that Gmail uses several hundred factors, the weighting of which changes constantly.

One of the most important factors is the engagement of the receiver: How does the receiver interact with the email campaigns? This can be positive (opens, clicks, forwarding, etc.) or negative (deleted unread, marked as spam, etc.).

The reputation helps the mailbox provider to decide whether and to which folder a newsletter should be delivered.

Email providers or legal regulations: Who makes the rules?

Every marketer is exposed to legal risk. In Europe, email marketing is only permissible with the prior consent of the receiver. As an exception, under certain conditions, it is permissible to send advertising for similar products and services to one's own customers.

When a mailbox provider assesses incoming emails, decisions are made not only in relation to the legal situation, but also according to what the user has done with the newsletters in the past. The focus of the mailbox provider is always on their users and the protection of their infrastructure. The provider has no particular obligation to deliver an email. Given that many services are financed through advertising, it is, of course, in their interests to make the users happy.

In Europe, there is very strong awareness of data protection issues. There are often complaints from receivers of advertising, and many demand information from the sender regarding the use and collection of their data. A lawyer is only a phone call away. So there is no way around legally well- constructed email marketing. Details on this can be found in "eco Directive for Permissible Email Marketing[3]" and, of course, can be obtained from company lawyers.

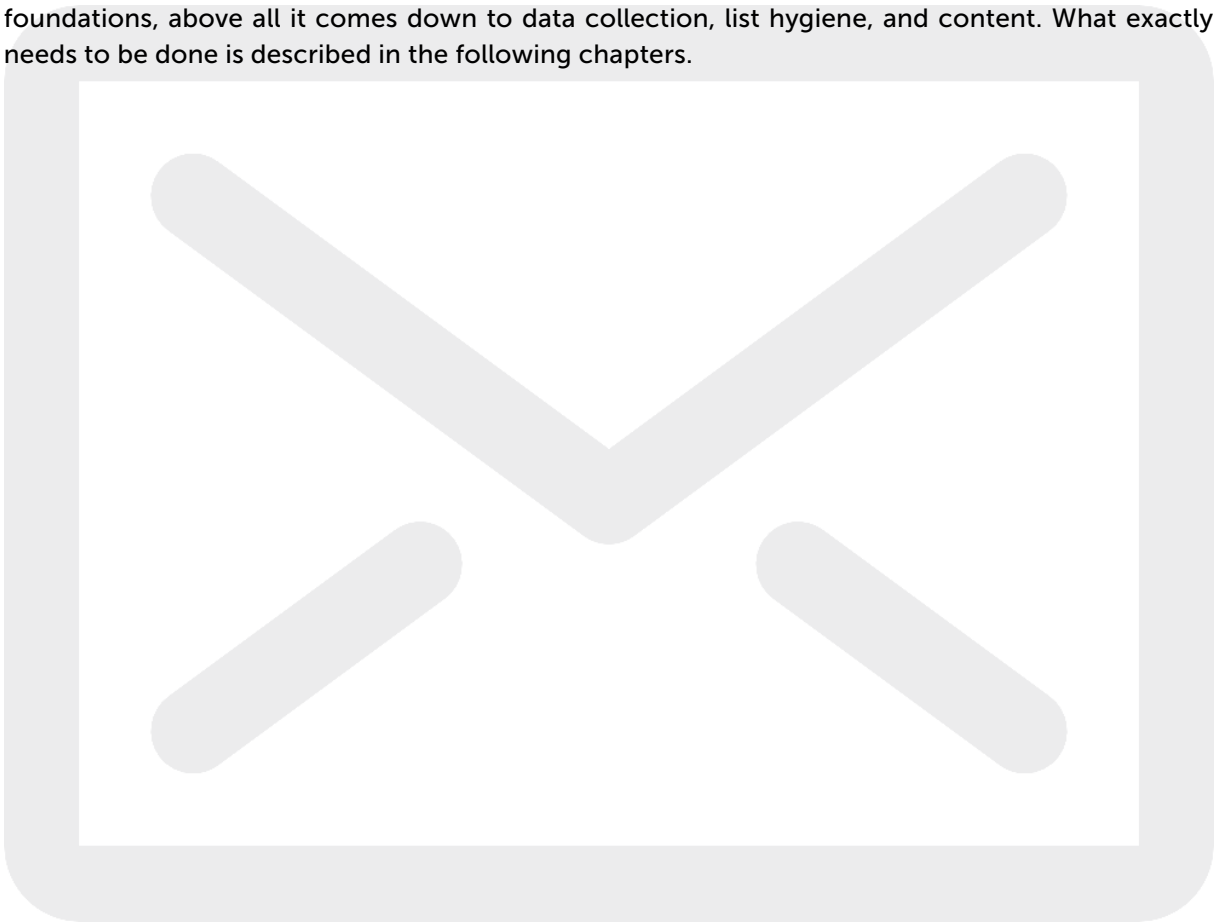
[2] http://emailexpert.org/9-gmail-fbl-myths/

[3] https://certified-senders.eu/wp-content/uploads/2016/09/Marketing-Directive.pdf

My next steps as a marketer?

The first step should always be the choice of a professional email service provider (ESP). The ESP makes the technical infrastructure available, which is essential to successfully deliver emails. The ESP also supports customers in relation to authentication measures (see "Technical Foundations – Authentication").

However, it is a fallacy to believe that the ESP alone is responsible for delivery or is capable of solving all problems. Certainly, the service provider can support, but alongside the technical foundations, above all it comes down to data collection, list hygiene, and content. What exactly needs to be done is described in the following chapters.



Data collection

A fundamental component of email marketing is, of course, the acquisition of new recepients. How this process would be set up in order to minimize the risks as much as possible is described in this chapter.

Consent

The central starting point must always be the active and informed consent of the affected party. This legal expression describes the subscription via a newsletter subscription page on the homepage or in the shop.

Active in this context means that the future subscriber needs to "do something" in order to receive the newsletter. Normally, this activity is represented by the clicking of the button for the newsletter subscription.

But a checkbox that the customer needs to actively tick in the order or registration process can also be such an activity. Here it is important that the checkbox must not already be checked (this would be a so-called "Opt-Out"). Through this method, the new customer may overlook the option and, as a result, may not become a subscriber. However, this would be a better result than if the customer overlooks the need to be active in order to avoid subscribing to the newsletter, and is then negatively surprised when the newsletter arrives.

The second aspect is the so-called verification, which is designed to ensure that the owner of the email address is also the person providing consent. If the consent is not verified, then it is possible for third parties to create subscriptions with any email addresses. The most common and most reliable method is the Double-Opt-In process, in which the recipient receives a confirmation email after giving consent, in order to actively confirm the consent. Through this, spam traps (see "Data Collection – What are spam traps?") and false subscriptions (regardless of whether they were accidental or malicious) can be avoided, and the mailing list becomes all the more valuable. Legally, you are also on the safe side using the Double-Opt-In process – this process is recommended on many websites, such as the Düsseldorfer Kreis[4] Conference of the German Federal and State Data Protection Officers.

Transparency

A very important aspect of data collection is to inform the future subscriber – as transparently as possible – what can be expected. This starts with an indication that the Double-Opt-In email will be sent and which must be confirmed.

[4] https://www.lda.bayern.de/media/ah_werbung.pdf , Seite 11

It is important that the receiver knows what can be expected and how often. The better the receiver is informed about content, frequency, and sender, but also about the possibility to unsubscribe, the lower the probability of complaints.

What are spam traps?

Spam traps are email addresses that are used by the providers of anti-spam software or mailbox providers to improve spam-filter algorithms or to punish senders that do not adhere to the rules. There are two main types of spam traps:

- "pristine traps": Email addresses that have not been actively used
- "recycled traps": Email addresses that have previously been used normally, and after deactivation have been turned into a spam trap

If you write to a spam trap, this either suggests a lack of verification (such as Double-Opt-In) or flawed bounce management. In both cases, problems can arise for the marketer that could result in damage to the reputation of the sender, and, as a result, advertising messages will not reach the recipients. If sending is carried out via an ESP, the ESP can also end up with problems like blocking.

Direct Customers

In Germany, and throughout all of Europe, it is legally possible to send advertising to one's own direct customers for similar products or services. However, especially in Germany, creating a legally permissible design is very involved, as several issues need to be taken into account for the deliverability. The legal requirements can be found in the "eco Directive for Permissible Email Marketing".[5]

Spam traps again pose the first risk, because online shops do not, as a rule, verify the email addresses of their customers. As a result, spam traps can find their way into the mailing list if customers, deliberately or by mistake, input an invalid email address. The activities in the shop offer no evidence of such a false email address, as it does not always prevent shopping.

A further problem can occur through the sending of email marketing to direct customers without their consent: Many people simply do not know the legal exception. For many receivers, then, the advertising comes as a surprise. This leads inevitably to complaints. If a receiver marks a message as "junk", this will damage the reputation of the marketer, regardless of the legal stipulations.

The safest method is always to obtain the active consent during the order process. For this, it is enough to add a non-preselected checkbox to the questions regarding customer data, which would allow customers to subscribe directly to the newsletter.

[5] https://certified-senders.eu/wp-content/uploads/2016/09/Marketing-Directive.pdf

The worst case would be to, on the one hand, offer this option, and then subsequently, regardless of the customer decision, to offer the customer “similar products and services”. This is very non-transparent for the customer and leads to complaints.

List Hygiene

Bounces

Put simply, a bounce is the indication from the receiving mail servers that the email can not be delivered. For every bulk mailing, there are bounces. These should be processed according to their categorization. It is important to note that a certain number of undeliverable messages (similar to the era of postal "returns") is acceptable.

Hard bounces

Hard bounces are cases of permanent undeliverability. The recipient does not exist (user-unknown). Sometimes the domain also no longer exists (domain-unknown).

Generally, hard bounces are seen as extremely damaging for the reputation of a sender. The condition for this is that they occur multiple times per receiver. Therefore, it should be continuously ensured that reliably-categorized hard bounces are directly removed, with the corresponding email addresses, from the mailing list.

Soft bounces

If there is even a vague possibility of reaching the receiver again in the future, then we talk about a soft bounce. Frequent examples are:

a) **Mailbox-full:** The user has no more storage capacity available to accept the email. If the mailbox is cleaned up in future so that the user has capacity again, this situation will change and emails can again be accepted. This issue varies from region to region. In Germany, the number of ISPs with small mailboxes (in the free mode) is declining, and as a result, so is the number of full mailboxes. If it comes to such bounces at German ISPs nowadays, the tendency is to exclude the affected receivers, as it is generally preceded by a long period of inactivity.
b) **Spam-Reject:** Rejection due to the suspicion of spam is based either on the reputation of the Domain/IP or on the message itself. In most cases, such rejections are comprehensively applied for all of an ISP's users. As a negative reputation is, as a rule, reversible, the willingness of the ISP to accept emails will change if there is an appropriate reaction to such an incident. As a result, such bounces should be understood more as an operating instruction rather than a recommendation for deactivation.
c) **Others:** Of course, there are also many other reasons why messages are not accepted. These should be examined as individual cases and then, if necessary, an additional automated processing routine can be added.

The automatic and prompt processing of bounces is obligatory in all cases. Some email service providers also offer automatic reactivation of soft bounces. Ideally, the ESP offers the choice of an automated de- and reactivation routine. This should be adapted to the respective sender behavior.

Unsubscribe

Unsubscription is an active form of assessment of marketing communication. A previously active receiver of newsletters from a particular brand is now no longer interested and cancels subscription for the future.

Shrinkage should be avoided. However, in contrast to soft bounces, there is no room for negotiation or interpretation here. Generally, the unsubscribe link is too small and placed too inconspicuously for the receiver to have accidentally clicked on it.

There are a range of possibilities to keep the receiver in the list under altered conditions. Senders have, in the past, had very good experiences with a so-called preference center. On this site, the receiver can set preferences and/or frequency. There is nothing wrong with offering the receiver the chance to adapt the frequency of the newsletter. Often, simply too many emails are sent in too short a time for the taste of the individual receiver.

Artificially impeding unsubscription should be avoided at all costs. Deliberately delaying unsubscription through further landing pages, Double-Opt-Out or Captcha will lead in the medium term to loss of reputation as a result of spam complaints by the user, who, after an overly long unsubscribe process, has simply given up.

Feedback Loops

Alongside unsubscriptions, complaints are a possibility for the receiver to remove from their line of sight emails with unwanted content or from unwelcome senders. As soon as a user makes a complaint about spam and marks a corresponding email as such, the mailbox provider will send all future messages from that sender to the spam folder.

Deactivation from the sender side on the basis of a successful spam complaint is a further possibility. To enable this, some mailbox providers offer the possibility of setting up a complaint feedback loop.

The technical solution is simple: In the case of a complaint, the receiver sends an email in a particular format back to the sender as an indication that they do not want the marketing email. This email contains the full content of the email (which is also the argument for the German mailbox providers and Google not to offer such a mechanism). With the help of this information, the sender is able to identify the receiver and to stop writing to them. Therefore, in future there will be no further advertising emails sent to this receiver.

Excepted from this rule are, of course, transactional emails, which can be triggered by the complainant, for example, in the context of an order process.

Example: max.mueller@example.com complained on Monday about an advertising email, but then ordered a product on Wednesday: the order, dispatch and payment confirmations can and must still be delivered.

Generally, ignoring complaints (from an existing feedback loop) can have an extremely negative impact on the reputation of the sender today.

Manual Answers

Email is a subcategory of dialog marketing. This means that answers from the receiver are possible. Not least because of this, it is standard today to use "no-reply@" sender addresses. Added to this, manual answers should not only be received, but also processed.

Connection to the company-internal customer care is recommended. This is also helpful if there is any lack of clarity relating to the articles offered in the newsletter.

A certain level of automation is also possible here, and is recommended from the outset. Of course, topic-related questions or issues can always be included in the answers, but often enough, the answers are limited to gruff demands to end the newsletter subscription.

Content

Engagement

As has been described in the previous chapters, the open and click rates (engagement) are some of the most important measurable criteria for a good reputation. Therefore, the goal must be to keep an eye on these KPIs and to critically analyze sinking values. They are the first indication of having chosen the wrong target group, or they indicate the sending of content with low relevance.

Relevance

Opening signals to the mailbox provider, in the first place, interest in the content of the email. Through a click, the receiver demonstrates emphatically the relevance of the email, because

a) they trust the sender enough to open the link contained in the email,
b) they have further interest in the content of the email,
c) the sender is obviously known to them and the content is expressly desired.

Today, relevance is one of the most important criteria for the successful delivery of emails. Topics or wording only play a subordinate role – as long as the content is relevant for the end customer, there are no further barriers.

Please note: Relevance is a subjective term – everyone sees different content as relevant. As a result, high relevance can only be achieved with a strong understanding of the target group.

Transparency

A further important point is transparency or the recognition value of the news. The more end customers know about,

a) what content
b) how often
c) at what time
d) from which sender and even
e) in what color/fonts

they receive, the more positive the impact on the open rate and in particular on the complaint behavior of the receiver. It is also important that the user can unsubscribe at any time, without difficulty – here also, complaints and the associated negative reputation can be avoided. A thorough legal notice with a link to the T&Cs generates trust – an important foundation for building a target group mailing list with long-term engagement.

Technical Foundations

Authentication[6]

The security of electronic post has been a controversial topic from the very beginning of the email in the 1980s – and is still so today. The success, and at the same time the weakness, of the email lies in its simplicity and its large distribution. In the early years, spam was much further from solution than it is today. There was hardly any regulation of data protection. Today, there are far-reaching possibilities to establish security and authentication.

A diverse range of technologies enable improved security and authentication for email messages. These are, in detail:

SPF (Sender Policy Framework)

Information about which IP addresses are permitted to send emails on behalf of the domain is stored in the so-called Domain Name System. SPF is quick and easy to implement, but it cannot manage forwarding or mailing lists (so-called indirect mail flows).It is therefore unsuitable for the authentication of senders as the only tool.

DKIM (Domain Keys Identified Mail)

The email is furnished with a digital signature that can be verified by the receiver using the public key in the DNS. In this way, it can be detected if the email has been falsified in transit, or if the sender has been changed. The process forms the basis of domain-based reputation measurement.

DMARC (Domain-based Message Authentication, Reporting and Conformance)

DMARC unifies the use of SPF and DKIM and makes it possible to set up one policy for the mailbox providers. This then regulates how a message should be handled in the case of a failed test. In addition, DMARC makes reporting to the sender possible, so that the sender finds out how many messages tested positive or negative. The process serves the protection of brands, as well as the fight against phishing. Our recommendation is to use DMARC on the organizational domain in order to protect the entire brand (and not only an exchangeable sub-domain). Using the "reject-policy", a brand can actively prevent a message with failed or missing authentication from being delivered to the receiver.

[6] First published in the German original on the Teradata GmbH blog: Sicherheit & Authentifizierung – welche Technologien gibt es im E-Mail-Marketing? [F.Vierke, July 2016] http://blogs.teradata.com/teradata-applications/de/sicherheit-authenzifizierung-welche-technologien-gibt-es-im-e-mail-marketing/

TLS (Transport Layer Security)

Encryption of the transport route between sender and receiver. Emails are transported encrypted and can not be read en route (see also a blog article [7] by Florian Vierke on encryption).

What can/must I do myself, what should the ESP do?

In the choice of a sender service provider, alongside price and personal preference, the services included are paramount. As a rule, most market participants on the platform side offer everything that you need to undertake good email marketing.

Manual answers can be limited through settings in the platform. (Do I accept all emails to my answer address or only answers to messages sent by me? The difference is immense!)

Bounce handling is also standard. The fine-tuning always depends on the current mailing behavior. This means that these settings need to be adjusted if the mailing frequency increases or decreases.

DNS-based Authentication

For ESPs that use domain delegation, **SPF** is used automatically for those IPs that the sender wishes to use in future. If the ESP enables so-called domain pointing, it will make a comprehensive instruction manual available, to enable the sender to set up the necessary TXT-Record in the DNS zone of the sender domain.

DKIM (DomainKeys Identified Mail): Here also, an ESP that uses domain delegation can offer a better customer experience. The setup is undertaken when specified by the customer, and is done automatically without the customer needing to do anything themselves. If the ESP offers domain pointing, or if the sender insists on administering the domain themselves, a comprehensive instruction manual will usually also be made available.

DNS-based Reporting

DMARC (Domain-based Message Authentication, Reporting and Conformance): The setup of this standard is undertaken by the ESP in the case of a delegated sender domain. If the domain is pointed (or DMARC is set up for the organizational domain), then the ESP will, also in this case, make a comprehensive instruction manual or support available.

[7] http://blogs.teradata.com/teradata-applications/de/sicherheit-und-verschluesselung-im-e-mail-marketing/

Transport Encryption

TLS (Transport Layer Security): The ESPs are, in every case, the administrator of the sender server (Mail Transfer Agents). The establishment of a TLS-encrypted connection to the servers of the ISPs that support encryption, takes place there. As a result, regardless of how the domain is administered (delegation or pointing), this is a service provided by the ESP.

Sources and References

The newest version of this document is available online on the Competence Group E-Mail blog for download.

https://e-mail.eco.de/downloads.html

About eco – Association of the Internet Industry

eco, (international.eco.de) with more than 1,000 member organizations, is the largest Internet industry association in Europe. Since 1995, we have been instrumental in the development of the Internet in Germany, fostering new technologies, infrastructures and markets, and forming framework conditions. In the Competence Network, a range of specialists and decision makers of the Internet industry are represented, and current and future Internet themes are driven forward, together with a team of more than 60 staff.

Special eco services help to make the market more transparent for providers and users. Our seal of approval ensures quality standards; our consultations for members and our services for users provide support in questions of legality, security and youth protection.

As an association, one of our most important tasks is to represent the interests of our members in politics, and in national and international committees. As well as our headquarters in Cologne, we have our own office in the German capital Berlin, and are represented at all relevant political decision-making processes in Brussels.

More information about the eco Competence Group E-Mail can be found on the official blog at https://e-mail.eco.de/