Optimize the deliverability

of your email campaigns

WHITE PAPER

Mailify

Mathieu Tarnus,
CEO of Mailify

Prologue

"Designing and sending newsletters has evolved greatly since the early 2000s. What was once viewed as just a mass marketing communication tool, has now become something far more sophisticated. Over recent years, email marketing has adapted to a new marketing landscape, shaped by an overwhelming amount of email traffic, stricter anti-spam regulations and the challenges surrounding the bad reputation that unwanted commercial emails have racked up... Nowadays, simply hitting the «send» button is no longer enough for your message to succeed. In fact, deliverability is the number one challenge digital marketing professionals face when communicating with their target audience via email. When it comes to deliverability of an email campaign, the process starts with reflection. In practice that means: accurately targeting campaigns, cleaning up the database, skillfully managing opt-outs, creating messages based on certain templates and testing before sending. But most importantly, you need to know your audience and understand how they would perceive your message. So it's safe to say that there is more to email marketing than meets the eye. It has turned into a highly effective and professional channel for direct communication. Email marketing tools, like Mailify, need to take all current needs and challenges of their users into consideration when developing the software's various features. In this white paper we'll explore the entire journey of a marketing message, from creation to inbox, as well as provide insight into the tools and techniques for optimizing your campaigns.

Email marketing has a bright future ahead, and armed with the best practices outlined in this paper you'll be able to get the most out of this effective communication and marketing tool."

Summary

EMAIL MARKETING TODAY

Email marketing is a direct communication tool characterized by its low cost and simplicity in use. Also referred to as 'bulk mailing', it suits both commercial and informative communication, and is a popular channel with small, medium-sized and large businesses alike.

Whether you're looking to acquire new customers, increase loyalty or boost sales, email marketing is increasingly attracting interest. But nowadays, this area of marketing deals with some new and technical challenges that go beyond simply creating a message: email rendering, social media networks, the increased use of smart phones... Effective email marketing requires a specialized skillset to ensure your message reaches its destination. The playing field in email marketing is an interesting one: internet providers have an important role in maintaining anti-spam protection on behalf of their users. But at the same time, companies using email marketing have one goal: delivering their message to the recipient's inbox. In this context, where the amount of spam continues to grow, yet where email advertising has become so powerful, a new challenge is at the heart of it all: deliverability!

This white paper will help you get to grips with the key issues of deliverability and the solutions for successfully delivering your email marketing campaigns.

Understand the challenges of deliverability

WHAT IS DELIVERABILITY?

It's the ability to send email marketing campaigns to recipients' inboxes.

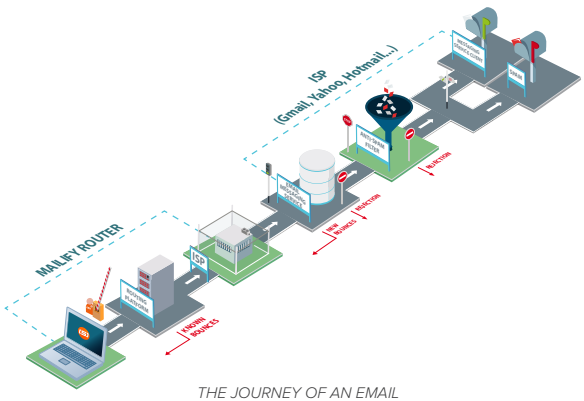
Originally, deliverability meant ensuring that messages were successfully accepted by messaging providers. Back then deliverability was only measured by analyzing bounces, which are error messages due to incorrect or invalid email addresses or domains.

Faced with an increasing amount of spam messages, the providers intensified their anti-spam regulations in addition to enforcing new codes of conduct to define «good behavior». As a result, companies are forced to optimize their campaigns by implementing best practices and using a professional infrastructure to ensure their message ends up in the recipient's inbox.

GOALS AND CHALLENGES

Sending bulk emails has become a valuable form of communication due to its cost effectiveness and high speed. But stricter anti-spam regulations have made this channel a complex one to manage. Deliverability can impact several key aspects of a business, such as turnover, profitability and customer satisfaction. Therefore ensuring a good deliverability rate is a topic high on the agenda for providers of email marketing solutions. The term 'deliverability' relates to a range of other subjects as well, such as e-reputation. This is the online reputation of an organization that sends emails.

One of the main contributing factors to a company's e-reputation is the proportion of emails that are marked as spam by automatic filters or the recipient's inbox settings. The lower the proportion, the better the reputation. Essentially e-reputation indicates the level of trust a company sending emails has gained, and is a fundamental building block in establishing a high level of deliverability. Improving and maintaining good deliverability has therefore become a major component of successful email marketing. To optimize your deliverability, it's important to take into account the fact that it comes in two forms: on the one hand you have the kind that you can improve yourself by working on your campaigns. And on the other hand there's the kind of deliverability that depends on rules and regulations that apply to the routing infrastructure.



THE JOURNEY OF AN EMAIL

The factors of deliverability

There are many factors influencing the deliverability of a campaign and affecting the reputation of a sender. This reputation will be crucial for the arrival of emails inbox.

In fact, the deliverability can be altered depending on:

- The method of collecting email addresses
- Whether there is a double opt-in confirmation or not
- The maintenance of databases
- Targeting when sending
- Possible complaints from recipients
- The number of bounces
- The authentication of the sender
- Whether a professional sending server is used
- The use of dedicated domains and IP addresses
- The content of the email
- The frequency of sending

Throughout this white paper we'll explore how to improve the chances of arriving in the inbox and what best practices you can start applying to avoid damaging your e-reputation as a sender.

BOUNCES

Managing bounces (addresses that don't exist or are no longer in use) is an important part of deliverability. Each invalid email address that is sent to the receiving server generates an error, also known as a 'bounce'. When the number of invalid email addresses in the database becomes too high it can cause occasional slowdowns in dispatches. It may also even result in the sender being blocked in some ISPs and webmails: this is called blacklisting. The higher the rate of bounces, the greater the risk of being blacklisted. To avoid this you should clean up your database after each sending.

There are two types of errors:

1/ **Hard bounces:** definitive error messages that indicate that the user of the domain name does not exist or does not exist anymore. We recommend to remove these kinds of addresses directly from your database.

2/ **Soft bounces:** temporary error messages that prevent an email from reaching the inbox. There are several possible reasons for this type of error: full inbox, sender's IP address is blacklisted, communication error with the receiving server, and so on.

These errors usually resolve themselves, although you may need to send the email again to make sure it arrives.

Sometimes soft bounces are the result of a sender being blacklisted due to complaints from users. To avoid such errors, the quality of the database must be regularly monitored and optimized.

It's important to note that the delivery of a message to the 'spam' folder is not considered a bounce. A certain number of bounces is fairly common when sending out email campaigns. In fact, it's very rare not to generate any bounces at all when sending out a batch of emails. You can minimize errors though, and it's important to take a proactive approach. The double opt-in, when collecting new email addresses, is a good way to avoid hard bounces. You can also try to identify common typos in order to correct erroneous email addresses. Besides the obvious presence of @ and . in the email address, it may be beneficial to correct the domain names as well (for example: yaho.com becomes yahoo.com). Following the launch of your campaign, it is necessary to update the email addresses as soon as you receive an error message.

SPAMTRAPS

Spamtraps (or recycled addresses) are email addresses that were once in use, but have since been abandoned by their owners and transformed into spamtraps several months later. These inboxes are owned by email providers or anti-spam groups and are intended to trap spam senders. Since these addresses have never been registered to mailing lists, all messages received are consequently spam, and their senders are reported as unwanted.

HONEYPOTS

Honeypots are e-mail addresses that are discreetly broadcasted on the web in order to be found by spambots (systems automatically collecting emails on the web). The latters retrieve them without suspecting the trap and when emails arrive in the inbox of the honeypot, antispam solutions analyze their number and trigger a process to blacklist the sender.

Using a professional routing service

AUTHENTICATION OF MESSAGES

The term authentication groups together several methods used by messaging providers to verify and identify the sender of an email. Authentication allows ISPs and webmails to tackle spam and phishing activities, and also enables senders to prove that they are who they claim to be. There are different authentication systems: SPF, DKIM and DMARC. More and more messaging providers, particularly webmails such as Yahoo, Hotmail and Gmail, ask senders to authenticate their mailings via these means. By using authentication, your emails have a better chance of successfully reaching your recipients. In addition, some providers such as Yahoo or Hotmail append a small icon in your message showing the recipient that you are an authenticated sender. This improves confidence and can influence the opening rates of your messages.

It is important to clarify that authentication does not influence the deliverability of your messages. It contributes to its improvement, but does not replace other essential optimizations described in this white paper.

Messaging providers offer three main authentication techniques: the IP solution used by the SPF (Sender Policy Framework) technology, the cryptographic signature used by the DKIM (DomainKeys Identified Mail) technology, and the DMARC (Domain-based Message Authentication, Reporting and Conformance) protocol.

The SPF technology requires that the servers, which are allowed to send emails using a given domain, are declared part of the DNS zone. No digital or private key signature is required on your infrastructure, just a simple TXT DNS declaration allows a machine to send emails in the name of your sender domain. DKIM technology works by cryptographic signature, enabling a domain to authenticate the beginning of the message in the email flow. As the name suggests, these are keys attached to sending domains. One key corresponds to one sending domain. When the mail server sends an email, it signs its message with the private key referring to the sender domain. A public key is available (DNS declaration) and verifies that the private key is correct. So essentially there are two keys: a private one on the sender's server, and a public one which is accessible to all. One cannot function without the other. This sending process ensures that the mail server is allowed to send emails for the signed domain in question. And vice versa, if someone tries to send campaigns with a domain that does not belong to them, their access will be refused by the recipient's infrastructure, resulting in a very low deliverability.

DMARC stands for «Domain Based Message Authentication, Reporting & Conformance», a protocol designed to strengthen the fight against phishing and spam. To be able to function properly, the DMARC requires the implementation of the SPF and DKIM. Its role is to indicate to the ISP managing the DMARC what to do if the sender's authentication fails.

DMARC plays a dual role:

- It sends reports in XML format to the email address used when configuring the DMARC. Reports allow you to view the email authentication failure rate of the domain protected by the DMARC and their origin.
- It allows you to tell the ISP what policy to apply if the SPF or DKIM authentication fails.

Currently very few internet service providers take this new technology into account. Only the main ISPs including AOL, Yahoo, Gmail and Hotmail are know to support DMARC.

What is the DNS?

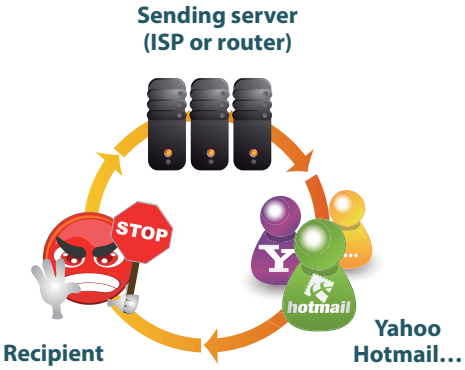
The DNS is a naming system that identifies and governs different aspects of domain names. Just like a real identity card, it defines all the information attached to a domain, such as the IP address of its website(s), IP addresses of mail servers, possible decryption keys (DKIM) etc.

The information in the DNS is public and managed hierarchically by servers all over the world that each have a time-limited cache. When querying a domain, the server nearest to the requester (usually that of the access provider of the requesting party) verifies if it has the information in its cache. If not, it solicits a hierarchically superior server and so on, until this information is known. Once the information is obtained, each requested server saves it in its own cache. This structure guarantees that the internet network maintains a certain level of continuity in the search for the domains, no matter the location of the websurfer or the hosting service of the domain.

FEEDBACK LOOPS

Messaging providers have empowered their users with a button to report a received message as spam.

This allows providers to analyze and store complaints in order to improve their filtering service. Some providers, including Yahoo and Hotmail, have set up feedback loops to send complaints to the sender to remove the addresses from future dispatches. The feedback loops give senders the opportunity to improve the quality of their content and help to identify potential problems with the content being sent, which is a source of dissatisfaction. Also, recipients are more and more used to click directly on this type of button instead of searching for the unsubscribe link. It is essential to take these feedback loops into account in order to avoid blacklisting. The role of the routing infrastructure is to manage these different feedback loops, either by taking initiatives by itself or by forwarding the information to the sender.



HOW THE FEEDBACK LOOP WORKS

MANAGE YOUR E-REPUTATION

E-reputation is a key element in deliverability. Messaging providers analyze the reputation of the servers used for all sendings to their service and assign a score to each of these servers identified by their IP address.

Thanks to this score, they can judge the nature of the message: legitimate email or spam. Therefore it's important to use a good routing infrastructure service with reputable mail servers. Recognized routers usually maintain and exchange relationships with email providers that identify them as legitimate.

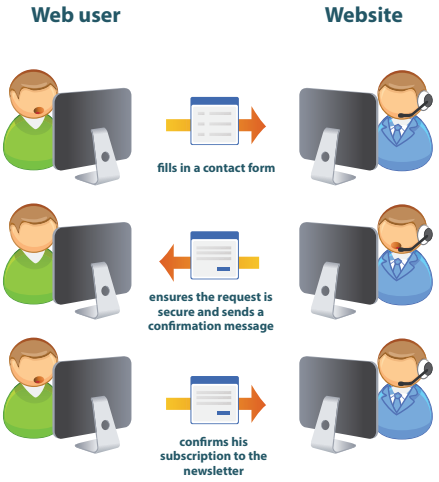
Moreover, the links present in the email are also an element of e-reputation. The tracked links are in fact identical for all the senders of the same router.

Customizing links is a good solution to avoid seeing your campaign unredeemed because of bad reputation links. (Topic discussed on page 23).

OPTIMIZE THE WAY OF COLLECTING EMAIL ADDRESSES

The method of collecting email addresses that form the basis of the recipients is crucial for deliverability. It is therefore essential to control the sources through which you gather the email addresses.

To optimize your deliverability, choose to collect exclusively opt-in addresses. We speak of an opt-in email address when its owner has given explicit consent to an organization to send them commercial offers or information to that address.



PRINCIPLE OF DOUBLE OPT-IN

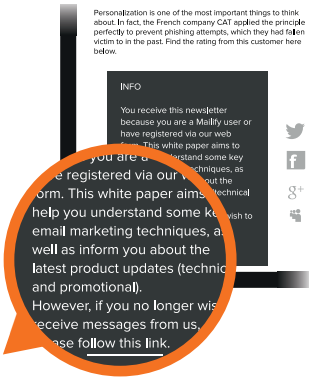
When collecting email addresses, it is important to ensure your future recipients give their consent by, for example, ticking a checkbox in your form. Furthermore, do not forget to set up some sort of input control. In most cases forms contain internal settings that check if an email address contains certain characters suchs as '@' and '.'. This will prevent you from importing erroneous addresses. But to be sure to only collect correct email addresses, there is a collection method called «double opt-in».

This is a technique that ensures the email addresses are real and they are provided by the actual owners of these addresses. The double opt-in consists of asking the user to confirm their subscription by email after they entered their email address on a web page. So the user receives an automatic message containing an activation link which must be clicked in order to make the registration valid. This method guarantees a very low bounce rate, but sending a confirmation email has another effect too: the message may be drowned in the mass of emails received every day and therefore deleted, overlooked or just forgotten... As a result you will have fewer registrations on your list but a better quality in return.

From a legal point of view, it should be noted that communicating to individuals by email requires their consent. Furthermore, whatever the context, the law imposes the right of opposition for recipients using an automated method, usually this is done by adding an opt-out link in the footer of the message.

Some providers sell so-called opt-in email files. We do not recommended to buy them because they are often sourced from suspicious or out-of-date sources, and many of these emails will no longer be valid, or even used as spamtraps or honeypots (subject treated on page 17). Your performance will be very low because they never explicitly asked to receive messages from your organization. Campaigns will be disastrous s a result of the poor quality of the email addresses. It is important to remember that the quality of a contact database is much more important than the quantity alone. Sending unsolicited messages can be very negative for your brand image and the reader be likely to consider you as a spammer.

MANAGE OPT-OUTS AND COMPLAINTS



Managing unsubscriptions is essential to increase the deliverability of your campaigns, for several reasons. Firstly, to avoid complaints: if the unsubscription process is tedious or broken, the recipients wishing to unsubscribe will seek other ways to stop receiving your emails. In that case the use of the «This is spam» button is very common if unsubscribing is not easy.

Chances are that your message will automatically arrive in the junk folder. If clicks on the «This is spam» button exceed a certain threshold, the sender's domain can be considered a spammer by the messaging provider.

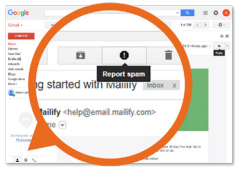
There are several reasons that may justify why recipients wish to unsubscribe. It is very important to give them the liberty to do so through a simple and effective opt-out process.

Readers sometimes tend to forget why they receive your messages. Add one or two sentences at the beginning of your content to tell subscribers why they are subscribed to your mailing list. Do not hesitate to place your unsubscribe link at the beginning of your message in order to make it sufficiently visible. For example, it is a good idea to place a sentence of this type at the beginning of the message: «You receive this message because you have subscribed to ...

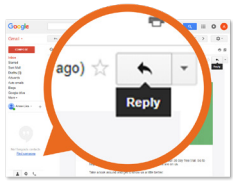
If you wish to unsubscribe follow this link». If the recipient no longer wants to receive information from you, he can easily cancel his registration instead of clicking on the SPAM button. The unsubscribe link should be easy to use. They should be able to unsubscribe in just two clicks. As it is a good opportunity, take advantage of it by collecting the reasons for unsubscribing via a multiple choice list on the confirmation page. You can also offer to reduce the sending frequency if you are able to handle this preference. On the other hand, always check that the unsubscribe link works and blacklist those recipients who do unsubscribe.

If you do not have an automatic churn system, consider cleaning your base regularly following these requests. Otherwise, the SPAM button will be used as a last resort to stop receiving your messages. And then, you may have already experienced it, nothing is more annoying than a link of unsubscribing that does not work. In addition, recipients can complain in various ways if they feel spammed. For example:

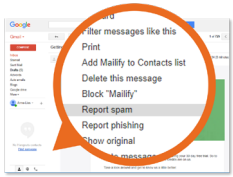
- By clicking on the spam button. In this case, it is necessary to be able to collect the complaints via the feedback loops (subject treated on page 15),



- By sending a message to the reply-to address. This address must be checked in order to be able to unsubscribe the complainants.



- A message sent to anti-abuse addresses «abuse@mailify.com» or «abuse@gmail.com» for example. Here, it is the router or the webmail that will conduct actions with the sender.



Proper handling of complaints allows you to have a return on your dispatches. If you see peaks in complaints, you will need to analyze the reasons for the discontent: increased sending frequency, inappropriate content to the target, importing new contacts into the database, and so on.

FILTERING

This is probably the most important good practice nowadays. Indeed, American ISPs are increasingly looking at the behavior of users and analyzing how they react to a particular sender.

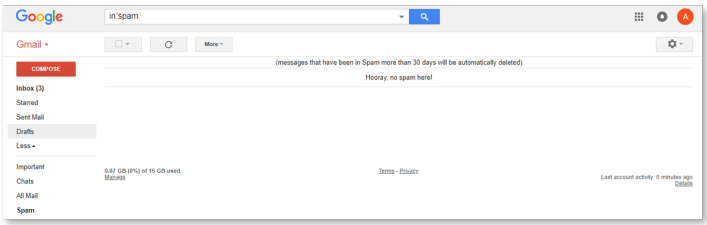
In other words, if your email is never read or regularly deleted before it is opened, your reputation as a sender may be impaired and your emails will arrive less and less often in the inbox at this ISP.

This is why targeted emails, in addition to a healthy and respectful collection, is crucial. Sending mass emails is less and less practiced and leaves room for sending targeted emails.

The accuracy of targeting has a significant impact on recipient behavior. The better an email is targeted, the more it gets opened, and the better the reputation of the sender is.

CHOOSE YOUR SUBJECT LINE

The choice of subject lines is not only important for good marketing performance, but it is also crucial for deliverability because spam filters are very demanding when it comes to the contents of subject lines and do not forgive any mistake. Let's look at some best practices to bypass these filters without a risk.



- Never send a campaign without a subject line
- Do not write whole words in capital letters (example: INCREDIBLE OFFER!)
- Do not abuse puctuation and especially question and exclamation marks. Filters are getting more and more strict with their rules and might send you to spam for just one single exclamation mark in your subject line.
- Do not repeat the same word several times in the subject line
- Do not unreasonably space out the words of the subject line
- Avoid the use of special characters such as% or .
- Avoid spam words such as: FREE, CREDIT, CLICK HERE ... Campaigns with the theme of money, sex, drugs or games are the most sensitive. Be vigilant about the terms used with these topics.

You need to keep in mind that choosing a subject line is not an exact science. The best way to ensure that the subject will not cause any problems is to test your message on the main messaging softwares and webmails before hitting «Send».

FORMATS

There are two formats to create a newsletter: plain text or HTML. The HTML format gives the possibility to customize the message using styles (colors, fonts...) and inserting images and animations. The plain text is a simplified format that lacks any formatting or creativity.

Most commercial newsletters are nowadays created in HTML. But the plain text format is still used when it is not necessary to embellish the message. It is more often used by the BtoB sector. The raw text offers an optimal rate of deliverability: as they are very light, these messages are easier for anti-spam filters to analyze and display correctly on all the messaging systems, unlike the HTML format that sometimes poses problems. But there is a solution to this dilemma: the multipart. This technique involves creating a message in both HTML and also in plain text. It is then the recipient's mailbox that determines which format to display. In most cases, the HTML format will be readable. But some email softwares used in the workplace or on mobile phones do not support HTML and that's where the plain text format comes in.

However, it's important to realize that the opening rate of a message is usually measured in terms of the loading of a small invisible image. As images are not supported by the plain text format, information about the opening of the email cannot be collected. Only the HTML format is used to determine the opening rate of a campaign.

PERSONALIZING LINKS AND CONTENT

The personalization of emails is a major component for good deliverability.

The more customized your mailings, the more they match the expectations of your recipients. By adding customization using, for example, the recipient's first and last name, you are able be more engaging and are more in personal dialogue than is the case in mass communication.

If your recipients feel considered, complaints will drop, your e-reputation will improve, and therefore your deliverability will be better!

Another important point to take into account is the customization of tracking URLs.

In a newsletter, hyperlinks are used quite often to bring the recipients of the message to a web page. When you want to track the results of your campaigns, you set up a way of tracking to detect clicks on these links. The URLs are automatically modified whenever someone comes from a message provider, in order for the URL to comprise a unique identifier. This one is then returning to a tracking server before redirecting to the landing page. This server allows you to count the number of clicks for tracking.

Customizing these links means choosing the Internet domain that you want to appear instead of those automatically assigned by the service. This makes it possible to perform tracking on clicks, while keeping the possibility to customize some of the URLs with your own web domain, such as: www.my-website.com/my-page.asp?xxxxxxxx

The customization of links has a direct influence on the good transmission of the message to the recipients. Tracking URLs can be blacklisted by email providers following a SPAM incident. In case of pooling of the tracking domain, this affects all the clients that share this URL. This is why it is important to customize these tracking links so as not to suffer the blacklisting of a shared domain because of the actions of other users. Tracking URLs associated with campaigns that have caused significant complaints rates in the past have a bad reputation, which will adversely affect your deliverability.

«Antispam filters of email providers are extremely sensitive to the use of links in emails because of the many phishing cases that have happened. Phishing aims to obtain confidential information (contact details, credit card number ...) by pretending to be a legitimate sender.

For this, they will notably simulate legitimate links. They operate with this little HTML trick: <ahref=»»http://www.phishingwebsite.com»»>www.websiteofmybank.com

With this code, recipients will read the trusted url (www.websiteofmybank.com) but will not see the true destination of the link (www.phishingwebsite.com).»

This practice is heavily monitored by email providers, which have therefore strengthened the filtering rules. Now, in your legitimate campaigns, you may be forced to use this same technique unintentionally! Imagine that you put this code in your emailing: <ahref = «http://www.mywebsite.com»> www.mywebsite.com

With URL tracking, your emailing service will edit your url like this: www.mywebsite.com

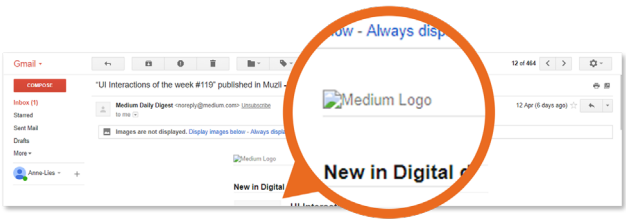
By customizing your links with your domain you are putting every chance on your side to pass the antispam barriers. This technique offers the best chances that antispam filters will consier your campaigns as legitimate, thus ensures better inbox deliverability and therefore a better opening rate. And beyond the deliverability aspects, the fact that the recipient feels reassured about the origin of the domain, substantially increases the click-through rate of the campaign.

Best practices for the HTML format

There are a number of essential good practices to designing an emailing campaign in HTML and maximizing the chances of getting it into an inbox.

MANAGE IMAGES

More and more mailboxes no longer automatically display images contained in newsletters. Users are asked to click on a link to display the images. In addition, messages consisting solely of images are more likely to be found in the «SPAM» box because the antispam filters can not analyze their content. When in doubt, they sometimes consider them SPAM. Hence the importance of not creating your message with only images.



Follow these guidelines for managing images in your designs:

- Mix images and HTML text: use images only for visuals or effects. Everything else can be in HTML text, to which you can apply formatting (font size, bold, color ...). It is still common to see legitimate senders design their emails with one or more images. When you create emails, always test your message without loading the images. If you do not see anything but disabled images, you should review the design to include text. Opt for a 60% ratio of images (preferably to be hosted on a server to lighten the weight of the message) and 40% of text. This technique will allow you to propose an attractive and light message, allowing to communicate according to your goals and without constraints! Moreover, this ratio has the advantage of having a good level of deliverability.

- Prefer the use of multiple small images instead of one big one
- Fill in the ALT tags of your images (they will be readable by some messengers at the place of your images before they are loaded, and especially if they are replaced by a cross because they are not displayed)
- Set the dimensions of your images (width and height attributes). The template of your newsletter will then be correctly displayed even if the images are not visible.

THE RESPONSIVE DESIGN

Nowadays, with more than 50% of emails worldwide read on mobile, it becomes more than imperative for marketers to worry about responsive design. Responsive design means the adaptability of an email to a mobile device such as smartphone or tablet.

«If an email cannot be read on the phone, it has one chance out of two to be ignored and thrown to the trash. Given the vigilance of Gmail / Hotmail ISPs with regard to user behavior, if an email is quickly sent to the trash, it will be more likely to arrive in SPAM next time.

This is why it is necessary to take this trend into account and create adaptive content emailing. Today, professional email marketing solutions enable you to generate responsive messages in an automated way without any technical knowledge.»

IMPORTANCE OF THE PRE-HEADER

The pre-header is the first sentence in an email message. Generally located at the top, it appears entirely or partially in the preview of the inbox, just below the subject line, before the email gets openend. Only some inboxes show it before opening on a computer screen, but it almost always appears on mobile.

Its role is to make the recipient want to open the email by completing the subject. It should therefore not repeat it but provide additional information. Its importance in terms of deliverability lies in its ability to boost openings. Since American ISPs rely on user behavior to judge the quality of a sender, encouraging openings increases the likelihood that it will be appreciated by providers and thus improves deliverability in the long term.

LINK TO A WEB COPY

Systematically display a link at the top of your message to a web copy of your newsletter, which can be read in a web browser.

This online version ensures that a recipient, who cannot view the HTML content of your message or download the images, always has the possibility to read your message via their web browser.

USE INLINE CSS

CSS, which traditionally allows the formatting of texts on web pages, is not to be banished from newsletter marketing. But it must be used rarely and following certain rules:

- Position your CSS directly in the HTML elements: in <td>, , <font> tags. The use of <STYLE> tags is not supported by all messaging systems
- Do not put any CSS class between <head> </ head> because many emails remove the elements between these tags
- Do not use <LINK> tags containing an external link to a CSS sheet, this will not work.

AVOID MULTIMEDIA TAGS

You may be tempted to use multimedia elements to embellish your emailings. Forget it! Videos or the Flash format are not displayed in all the message providers at the moment. The tags to be avoided are therefore:

• <OBJECT>

• <EMBED>

• <APPLET>

Do not use Javascript or DHTML.

If you still want to insert a video clip, the best is to use a small sequence in an animated GIF that redirects to the real video hosted on your website.

In addition, it is extremely undesirable to insert attachments, especially for mass mailings. Prefer the use of links to hosted documents.

SIMPLIFY AND CLEAN HTML CODE

- Respect the W3C HTML 4 standard for HTML editing of emails.
- Do not use HTML map links on images
- Delete HTML comments
- Assemble slices of your codes using HTML tables. Avoid overlapping tables.

LINKS

- Focus on short links
- Delete links to IP addresses. These links are mostly used by spammers. It is always better to use domains.
- Verify that all links are functional

TEST RECEIVINGS

Receiving tests are essential to verify the deliverability of your emails. To do this, you must first determine the most frequently used messaging services in your database.

You can do this by analyzing the domains of emails (gmail.com, hotmail.com, etc.) in your contact list. Then, all you need to do is to create email addresses for testing purposes in different webmails in order to test the deliverability before your dispatches. Is your message arriving correctly? Did it land in the spam box? Depending on the results, it will be necessary to act on the content of the campaign and to check the reputation of the sending server.

Email rendering

One of the difficulties of email marketing is to make ones message readable on the multitude of email clients currently available in the market. Even if the HTML best practices described in this white paper make it possible to make them as homogeneous as possible, you can only be sure by using email rendering. Email rendering is a technique consisting of testing the display of emails on the main messaging terminals, be it webmails or email softwares. This technique saves you a lot of time because it is an automatic program that restores the rendering of your emails in different environments. It is through these results that you can then act on the HTML code to optimize its display. Given the importance of HTML design in deliverability, this service is essential!

MANAGING THE SENDING FREQUENCY

The frequency of sending your campaigns is a factor that can affect your deliverability. Do not harass your recipients with daily news (unless they have expressly accepted or requested). And don't wait too long as there is a risk that your recipients might forget you! The frequency also depends a lot on your market. If your list is made up of «hot prospects» who are in the pre-purchase search phase, it is in your interest to communicate quickly and at short intervals. The best is still to inform your future recipients about the frequency at the moment of registration and even better if you can allow your customers to choose from several frequencies.

Try to be consistent in the frequency of sending. This will allow you to get the subscriber to expect your messages at regular intervals. Frequency stability also improves your reputation with email providers and thus minimizes complaints and unsubscriptions.

If a recipient wishes to unsubscribe because of the number of messages, you can offer him a lower frequency, and you will avoid a significant part of unsubscriptions.

MANAGEMENT OF SENDING VOLUMES

Some campaigns may be blocked if they are sent to too many subscribers. Spammers often make massive dispatches without worrying about flow control. Messaging providers control the volume of emails sent for a given IP address. A high volume of emails that are not spread over time may be a reason for a temporary blocking or even sometimes a permanent one. This can have a major impact on the deliverability of campaigns. The current campaign is not delivered on time, which can sometimes have a marketing impact and the reputation of the sender may be affected. It is therefore recommended to regulate sending flows by spreading out the quantity of messages to send. Avoid all type of practice that will negatively impact the deliverability of your messages and therefore the performance of your campaigns. To avoid these blockages, use a service provider that sends your campaign in a continuous flow, which allows better deliverability.

PRESENTATION OF MAILIFY

The group around Mailify develops and publishes softwares and services to support companies in the management of their digital marketing by offering various solutions.

All activity began in 2001 when newsletter marketing was still in its infancy. Quickly, it met a great success with the small and medium enterprises, in particular thanks to softwares that were simple to use. Mailify now has more than 140,000 users worldwide.

Mailify's software is among the pioneers of newsletter solutions and publishes new innovative features year after year, in order to offer its customers the most complete and powerful newsletter tool on the market. The interface of Mailify has been designed for great intuitiveness. The goal is that the user gets to focus on the artistic creation and marketing of his newsletter campaign.

Today, Mailify is one of the European leaders when it comes to number of clients.

A PROFESSIONAL INFRASTRUCTURE

With around 8,000 active clients of the fifth version of its emai lmarketing solution, Mailfy takes the issue of deliverability very seriously. Several million emails are sent every day via the PRS (Professional Routing Service), a totally secure infrastructure and specifically designed to accelerate and optimize the deliverability of newsletter campaigns.Our platform uses all the latest authentication techniques (SPF, Domain Keys, DKIM, DMARC). Techniques that are now required to ensure good reception at many providers.

Additionally, wrong addresses are detected before you hit «Send». When you start Mailify, all bounce addresses detected in the course of sendings made with our Professional Routing Service are automatically downloaded and added to the filters to clean up erroneous, falsified or obsolete addresses. And in parallel, a dedicated technical team, in charge of the Professional Routing Service on a daily basis, is able to intervene at any time. Each element of the platform is monitored accurately and continuously.

All these techniques and measures make Mailify enjoy a privileged status with the many Internet service providers. Close relations are maintained with most of these European and Global Internet providers, which considerably increases the level of deliverability of emails sent with our platform.

MANUAL HANDLING FOR HIGHER QUALITY

Mailify has a dedicated department that hand-moderates all campaigns 24 hours a day, even on weekends. Maiify verifies that each campaign complies with the software's user charter and ensures that the mandatory unsubscribe link for each campaign is present. This moderation is carried out in the general interest of all users. In case of abuse of one of the clients concerning the content of its message, the failure or the dysfunction of the principle of unsubscription, the method of collection or more generally any other breach of the legal and regulatory obligations applicable in the matter, Internet users are invited to contact the Abuse service of Mailify at abuse@mailify.com. All complaints addressed to this box are treated with the utmost attention and the actions are carried out quickly. Mailify has also set up feedback loops with email providers that can detect and act on non-legitimate senders.

MAILIFY'S INNOVATIONS FOR AN OPTIMAL DELIVERABILITY

Mailfy offers the possibility to customize your Behavioral Tracking URLs with your own domain, so you no longer use the one common to all users and assigned by default. This innovation has the double advantage of appearing more coherent in communications, reassuring the recipients, and of course increasing the efficiency and the deliverability of the campaigns. Moreover, faced with the multitude of messaging providers available, it is increasingly difficult to test the rendering and readability of its emails on all providers. But the proper HTML design of the message is essential for deliverability. Mailify's R&D teams have developed a new pre-delivery preview feature that is available to customers. Users can send a substitute copy of their campaign directly from the software and view the final render on Outlook 2003, Outlook 2007 SP2, Outlook Express 6, Outlook 2010, Windows Live Mail, Windows Mail, Hotmail, Thunderbird and Orange. Other software and webmails will extend this list in the coming months. This feature allows the user to correct all or part of their message before the message is sent.

Conclusion

Deliverability is a huge subject and it is an integral part of email marketing. Each person wishing to send newsletter campaigns must now take a serious interest before embarking on the adventure. We hope that this white paper has been useful to you. The Mailify team remains at your disposal to answer all your questions on email marketing.