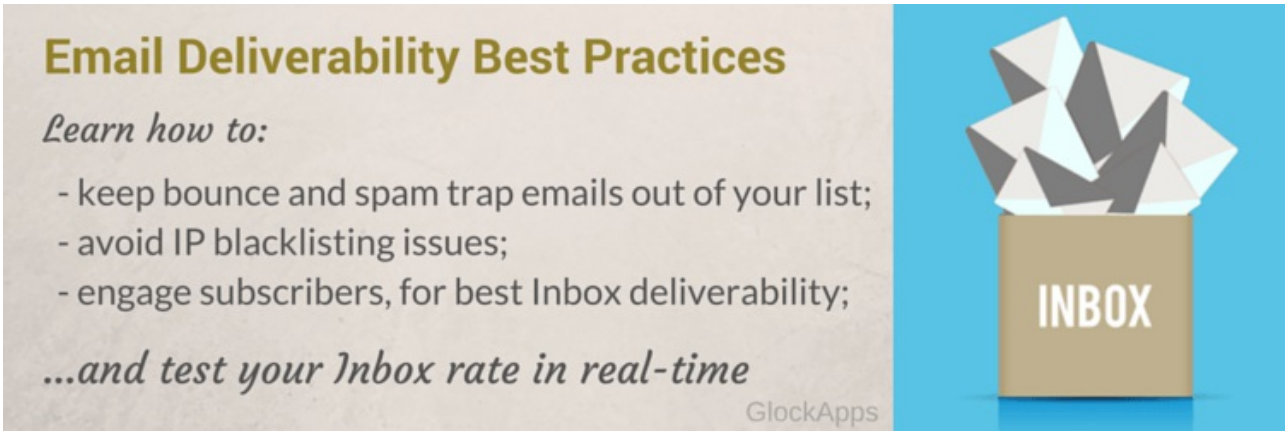
Email Deliverability Best Practices

Posted by Derek A. Lackey, Editor / September 11, 2017



Let's be honest: email marketing is nothing without deliverability. Don't believe anyone telling you otherwise. If your email is delivered, it can be seen, read, and clicked on. And if you can increase your email deliverability by even just 2-3%, it can significantly increase your ROI.

But considering smart filtering systems employed by mailbox and Internet service providers, achieving high deliverability rates is not easy.

Using thisemail spam checker toolyou can test each email you are about to send to your list and see how it is treated by different mailbox providers and where it is delivered: Inbox or Spam.

In the modern world, email deliverability is determined by sender reputation, bounce and complaint rates, and recipient engagement.

To keep all these factors in order, you need to follow these four email marketing practices:
1.Use Good List Acquisition and Management Methods
2.Set up Good Sending Infrastructure
3.Keep Your Recipients Engaged, for Best Deliverability
4.Test Deliverability Before Sending to the Whole List

Ideally, your email list must contain exclusively the email addresses of the recipients who are engaged with your brand and want to receive your messages. In the reality, email marketers often use poor list building and management methods.

However, it's important to strive for the "ideal" list because the quality of the email list impacts deliverability tremendously. Mailbox providers monitor the email addresses to which you are sending emails and will filter or block your messages altogether if a poor list quality is determined.

Thus, to be on the safe side, consider the following best practices when it comes to list building and management:

#1. Do Not Buy or Harvest Email Addresses.

Buying or harvesting email addresses from public sources seems to be the easiest and quickest way to populate the email database.

But it's a bad practice for these four reasons:

Unsolicited emails.If your recipients don't know who you are or never subscribed to receive your mailings, your emails could look like spam to them.

After enough of spam complaints, your sender reputation will go down, and ISPs will start filtering your emails. Even worse, you could have your IP landed on a blacklist, ultimately making it harder for your future campaigns to be delivered to people who actually want to hear from you.

Needless to say, sending to email recipients who haven't opted in is illegal in many countries and violates the CAN-SPAM Act.

Hard bounce addresses.You can't always trust the quality of a purchased list. You don't know where those addresses came from, whether or not they are correctly formatted and valid. The mailbox might have never existed, or has been terminated by the mailbox provider, or abandoned by the end user.

Thus, purchased or harvested email lists are likely to generate a high hard bounce rate. Mailbox providers ask senders to have low hard bounce rates because it shows that you manage your email lists and keep them up-to-date.

Bounce rates above 10% will likely cause deliverability issues. Ideally, you should keep your bounce rate below 2% to achieve a high Inbox placement.

Spam traps.Spam traps are email addresses that don't belong to active users and

are created and used by mailbox providers, anti-spam organizations, and blacklist administrators to identify spammers and senders using poor data management practices.

When a mailbox provider sees spam traps hits from a particular sender, they question the sender's list quality. Then they place verdicts on the sender's IP address, domain, or content, which then allow them or filtering companies to take measures such as temporary or permanently blocking the sender's email.
The type and age of the spam trap often influence the severity of verdicts placed on senders who hit spam traps.

There are two types of spam traps:
Recycled spam trap:it is an email address that once belonged to a real person, but was turned into a spam trap after being abandoned. Recycled spam traps are aimed to identify legitimate senders with poor list hygiene practices.

Pristine spam trap:also called "honey pots," it is an email address set up solely to capture bad senders and was never owned by a live person. It is assumed that no one should send an email to such an address.

Many spam trap managers hide their spam trap addresses on websites, so only harvester tools can capture them. When senders harvest email addresses from websites, they get spam traps. Any email sent to such addresses is seen as spam.

Bad statistics.This is obvious. Those people didn't want to hear from you, so what's the reason for them to open and read your message. At best, very few of them will open and click your emails. Are those few email clicks worth spoiling reputation and future deliverability?

Not to mention, your sending costs are increasing as far as your email list is growing. With a bad list, you are paying more and getting less. The key is to have a list of valid and engaged subscribers who want to receive your emails and act on them positively.

How to achieve that? Read below

#2. Employ Good List Management Practices.

Following are the recommendations for keeping hard bounce emails, complaining users, and spam traps away from your email list:
1. Use confirmed opt-in.Marketers who ask people to take an action usually click a link to confirm their subscription generally generate smaller lists than those who don't ask anything, but those lists are much cleaner than non-confirmed lists. They also used to have lower complaint rates.

2. Quarantine new addresses.If you don't use a confirmed opt-in process, don't email new subscribers until you send a welcome message and do not receive a hard bounce. This protects you from adding invalid addresses to your regular subscriber base.

3. Provide easy update/unsubscribe options.People often change email addresses and may be willing to update their contact information with you. If you don't have a full preference center, offer the option to change the email address at the point of

unsubscribing.

4. Send regularly.As a rule, the less often you email your list, the more likely you are to have high bounce rates. "Frozen" email lists are also more likely to produce spam hits as old addresses may have been turned into traps since your last campaign.

5. Handle bounce, complaints and unsubscribes.Usually, these are handled by the email service provider, but if you are operating a self-managed email system, you should set up the process of handling them yourself or use a 3rd tool likeGlockApps.

GlockApps will provide you with daily reports about your bounces and complaints. You will only need to load them into your "do not send list" or suppress those addresses from your base forever. As to unsubscribes, most self-hosted email solutions offer the unsubscribe handling as a feature.

6. Monitor inactive users.According to the best email practices, a subscriber who has been inactive for more than a year and has not responded to your re-engagement campaigns should be removed from your list. Set shorter "inactivity" periods of six-nine months if you send frequently and separate passive recipients from your main list.

Note: do not delete inactive users forever. Just keep them separately and stop sending email campaigns to them. Though they do not respond to your email communications, you can always try to reach them through other channels, for example, social networks.

7. Scrub and validate your list.Regularly check your list for role accounts (admin@domain.com), obviously bogus addresses (test@test.com), and typos (john@gmal.com).

If you allowed your list to "freeze," consider checking it for validity before launching a marketing campaign. Usedesktop email verifieror online email validation services like BriteVerify or DataValidation to determine invalid users on your list.

2.Set up Good Sending Infrastructure
You can't send successful email campaigns and achieve high Inbox deliverability if you have a weak email sending infrastructure.
You must have a robust infrastructure providing accurate authentication, high sender score, clean sending IP address, and a good sender domain/email reputation if you're serious about email marketing and are going to run world-class email campaigns.

Now:
Let's consider the main components of the sending infrastructure and their impact on email deliverability.

#1. Authentication.
Authentication allows the mailbox provider to confirm that the sender is the one who he pretends to be. If the sender cannot be authenticated, then mailbox providers may block the message or run it through additional filters to determine whether it should be delivered (and where) or not.

There are four primary methods of authentication:

1.SPF (Sender Policy Framework).SPF is an open standard created to stop forgery of "From" addresses. SPF records allow the receiver's host to verify that the email is being sent from the server it asserts it's sent from. It's like the email sender is telling the receiver "I send emails from this computer only."
So, if any other machine tries to send an email from the same domain, the receiver's mail server knows the "From" email address is forged. SPF standard is being used by a number of ISPs including several large mailbox providers such as Hotmail, Yahoo, AOL, etc. and mail hosts.

2. Reverse DNS.This is another way to authenticate the email sender to the receiver host. Reverse DNS lookup implies determining what host and domain name belong to a given IP address. If a Reverse DNS Lookup returns a "no domain associated", then the email will likely bounce to the sender, or will be deleted or filtered.

3.DKIM.This is the next step to do after you setup your Reverse DNS records. According to Wikipedia, "DomainKeys Identified Mail (DKIM) is an email validation system designed to detect email spoofing by providing a mechanism to allow receiving mail exchangers to check that incoming mail from a domain is authorized by that domain's administrators and that the email (including attachments) has not been modified during transport."

In other words, DKIM authentication system checks if the email is actually sent from the domain it claims to be sent from.

For legitimate senders, authentication is essential because it:
Protects your brand against phishing and spoofing.
Builds your domain reputation.
Reduces the chances of the messages being filtered or blocked by major mailbox providers and increases the Inbox Placement rate.

Allows you to sign up for Yahoo feedback loops. Yahoo feedback loops are domain based and require senders sign their messages with DKIM to sign up for the program and receive complaint feedback.

4.DMARC.DMARC ensures that the legitimate email is properly authenticating against established DKIM and SPF standards, and that fraudulent activity appearing to come from domains under the organizations control (active sending domains, non-sending domains, and defensively registered domains) is blocked. Two key values of DMARC are domain alignment and reporting.
DMARCs alignment feature prevents spoofing of the header From address by:
matching the header From domain name with the envelope From domain name used during an SPF check, and
matching the header From domain name with the d= domain name in the DKIM signature.

Here you can read the complete guide aboutemail authentication.
Remember:
Authentication is not the magic formula for solving deliverability problems. While it will make it harder for your "From" domain/email to be forged, it will not compensate for poor list management and sending practices.

#2. IP Address.
An IP address is a number in the domain name system that sends email on behalf of

your domain name. Mailbox providers look at the reputation of IP addresses sending emails on the behalf of your domains when deciding whether or not to put your email in the Inbox.

There are two types of IP addresses that email marketers can use:
Dedicated IP addresswhich is used by a single sender. It means that no other marketer or company is sending email from this IP address. The IP address reputation is affected only by the sending practices of the IP owner.

Shared IP addresswhich is used by multiple marketers or companies to send emails. The overall reputation of that IP address is evaluated based on all messages sent by all the IP address users. Thus, the IP address reputation can be spoiled by one sender and then all senders sharing the IP will be negatively affected.

Best email marketing practices teach that senders should have a dedicated IP address to maintain full control over the mailing activity associated with the IP address. However, when you are using an email service provider, you are sharing the IP and reputation with other ESP users.

If you are concerned about your reputation, you can consider a hybrid email system likeEasyMail7. Hybrid email software works as a front-end to delivery services and SMTP relays. So, you can get a dedicated SMTP server with a dedicated IP address and use it with the hybrid email system. This way, only you will be responsible for your email traffic and IP reputation.

On our opinion, email marketers should look for a dedicated IP address in case they are planning to send high volumes of emails. If you are one of them, you will need to warm up your IP by starting with small mailings and increasing the volume slowly over time.

A good scenario of the IP warm up is:
Day 1 1000 relays per day and 100 per hour
Day 2 2500 relays per day and 200 per hour
Day 3 3500 relays per day and 300 per hour
Day 4 4500 relays per day and no hourly limit
Day 5 7500 relays per day and no hourly limit
Day 6 9000 relays per day and no hourly limit
Day 7+ no limits

If you are using G-Lock EasyMail7, you can set the limitations per hour and per day in the Outgoing Mail Account settings to be sure you are not exceeding the volume of sent messages each day.

Its also important to watch the bounce rate and complaint and if any of them or both are high, you should stop mailings and fix the issues causing a high bounce/complaint rate in order not to spoil your IP reputation.

When you are using an email service provider like MailChimp or delivery service like Amazon SES, Mailgun, SparkPost or others, you are sharing the IP and reputation with other ESP users. ESP and delivery vendors already have good warmed up IPs and are known to provide high deliverability to their users. At the same time, they are severe towards bounce and complaint rate and will suspend your account if your bounce and/or complaint rate exceed the allowed threshold.

It's always a good idea to...

Read The Full Article