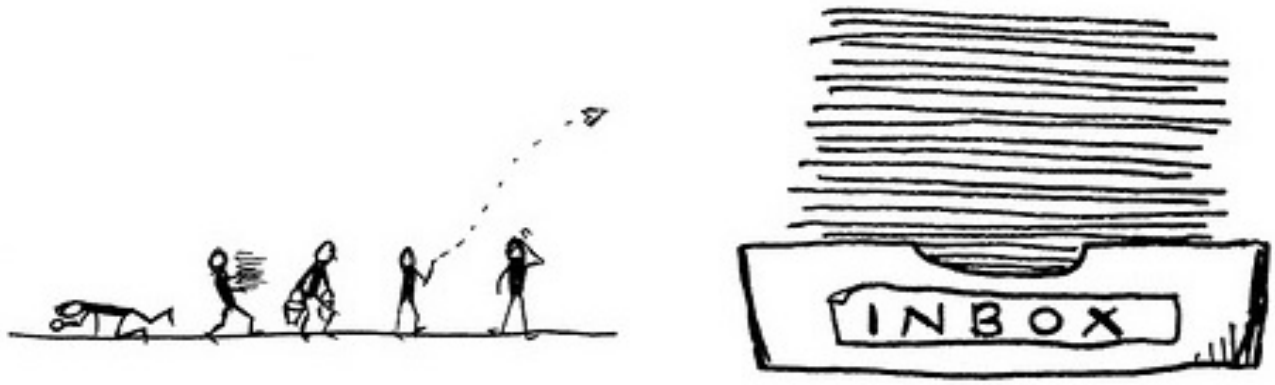
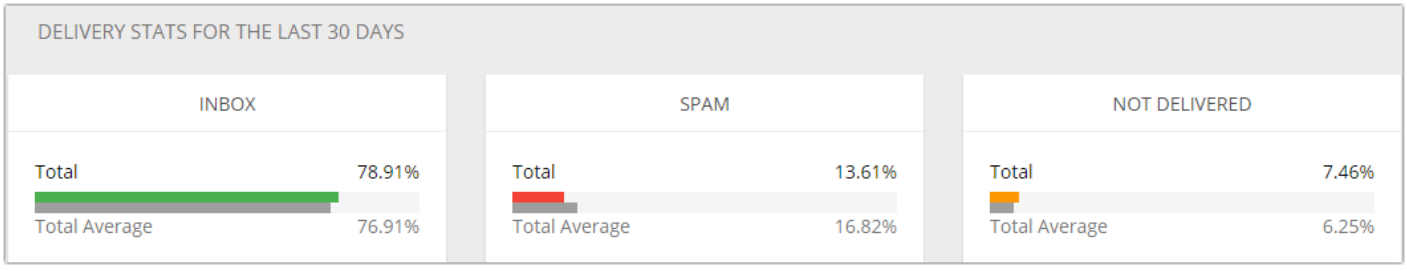
13-Point Checklist to Fix Email Deliverability



Did you know that every fifth marketing email never reaches the intended recipient?

According to the recent statistics from GlockApps, just around 77% of marketing emails land in the Inbox, worldwide.



As the volume of marketing emails skyrockets and spam tactics evolve, mailbox providers are forced to constantly advance their filtering algorithms to understand what type of messages their users want to keep unwanted mail out of their Inbox.

Thus, it's becoming harder for legitimate marketers to reach the Inbox.

So, if you want good deliverability or want to fix deliverability problems, go through this 13-point checklist.

This 13-point checklist will help you make sure you deliver your emails to the intended recipient without being filtered or blocked:

1. Check Your List Acquisition Sources.

A lot of deliverability problems come from things that many people don't even think of. When a deliverability problem happens, senders think about content, bounces, complaints, IP reputation, or email provider fault.

Of course, all these factors play a role in deliverability and they must be addressed, but all your efforts are useless if you don't fix the *root* problem.

The reality is that the root of the deliverability success and deliverability problems is the *mailing list*. How did you get those email addresses? Are those people aware that you will be sending emails to them?

Purchasing, renting or harvesting email addresses is the first step to deliverability problems. If you know or suspect that your list contains purchased or harvested addresses, it's better to throw it away and start collecting emails using an opt-in method.

Delegating email collection to a third party can cause significant issues with deliverability, too, because you do not control the process. And if you're paying per address, then the quantity beats the quality and the company collecting email addresses for you can stuff the list with invalid, fake or bogus email addresses.

Email address collection is the key to high deliverability, but many companies and marketers just don't care about how they're collecting email leads and entering into the relationship with them. It can be OK for the time the list is small. But as far as the list grows in size, it comes under a closer examination at the mailbox providers and what used to work before doesn't anymore.

With that said, the first step to finding the cause of any delivery problem is to *look at the list*. If your email collection methods are not good, changing email templates, content, IPs or domains doesn't change the reason email are being filtered out.

So, want good deliverability? Look at how you're collecting email addresses.

Want to fix deliverability problems? Check how you've collected email addresses and how you're managing them.

If everything is in order with your email collection method and you're sending only to people who gave you permission to email them, continue reading to learn about other things that affect deliverability and should be addressed, too.

2. Watch Your Content.

There were the days when certain words or phrases in the email content caused messages to be filtered to the junk folder. While it's not the case anymore (i.e. using the words "free", "money", "loans" in your message doesn't mean it will be absolutely end up in spam), content still does play a significant role in the deliverability, especially as it relates to reputation over time.

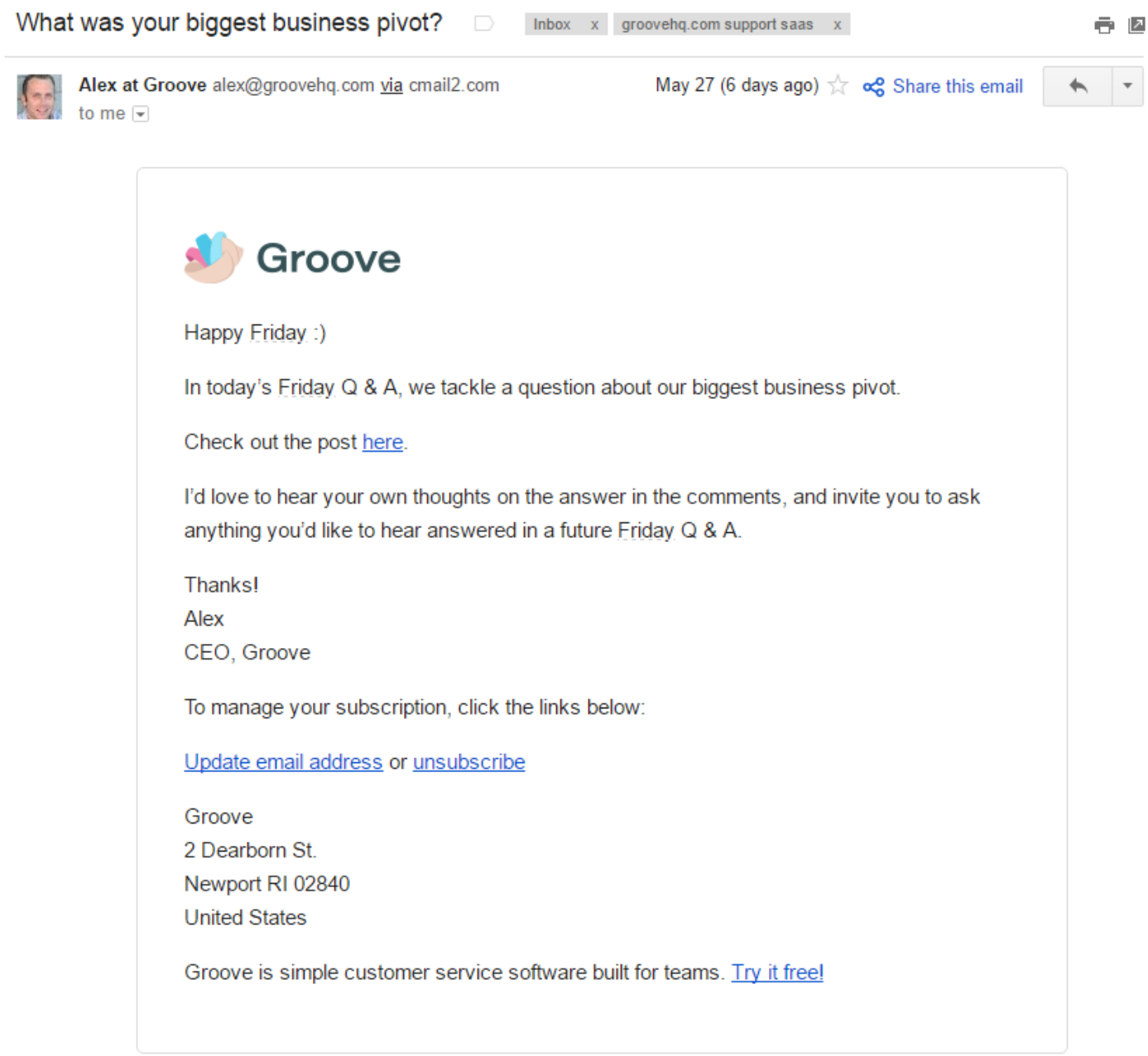
Nowadays, content-based delivery problems are not limited to a keyword here or there. Spam filters now look at any and all URLs in the message, patterns of content (whether or not it looks like other content that's been flagged as spam, whether it's yours or not), HTML code, plain-text version (whether or not it exists), image vs. text ratio, etc.

So you'll want to pay close attention to your message content and run a spam filtering test before sending the message if you want to eliminate potential content-based deliverability problems.

3. Use Light HTML.

The more rich HTML an email has, there is more likelihood for it to be seen by mailbox providers as commercial email and filtered out of the recipient's Inbox.

Smart email marketers are now switching to a light HTML format for their marketing emails and tend to avoid using images in their emails altogether for two reasons.



Firstly, certain types of formatting such as bright colors, too many symbols, too many links or too many images make a difference as to where the email is delivered, Inbox or spam box.

Secondly, there is the problem with displaying images correctly on a mobile device. And because 65% of emails are opened first on a mobile device, it's now imperative that you create a mobile friendly version of your marketing email.

It's also a good practice to not embed video in your emails. It's better to include the link to the video instead of embedding it.

But if you still want to use an HTML-rich template, make sure your design has two things: a properly coded HTML and a plain text version.

It's also recommended that you avoid links from unknown and crappy sites as these links are used in phishing emails and can be already blacklisted.

Ensure that your links are transparent and avoid using link shorteners in your emails.

4. Include an Unsubscribe Link.

A missing unsubscribe link is the first sigh that you're a spammer. If you don't give people an opportunity to unsubscribe when they want to, you're pushing them to hit the spam button instead.

Do not hide or disguise the unsubscribe link. Some email marketers do it because they are afraid of losing email subscribers. But remember that unsubscribes do less harm to your reputation than complaints.

However, a lot of unsubscribers is the sign that something is wrong with the content you're sending to your list. You could send a quick survey and ask your subscribers whether or not they like your emails and what kind of emails they are looking for.

To make your emails fully CAM-SPAM compliant, you also need to include your physical mailing address and contact information in your email footer.

5. Increase Your Email Open Rate.

Top mailbox providers such as Gmail, AOL, and Outlook have turned towards the recipient's engagement in their filtering decisions.

They now look at how many emails are opened, how many are deleted without being opened, how many are reported as spam, and how many are moved to the spam folder as a factor that determines the email placement.

The easiest way to increase your open rate is to write an attention-grabbing subject line that makes your subscribers want to open your email.

However, do not overdo and never use misleading subject lines, just to boost open rates, as disappointed recipients can mark your email as spam.

You can look through these articles for tips and best practices to write email subject lines and increase open rates:

- Five Tips For Creating Subject Lines That Improve Open Rates
- 10 Easy Ways to Improve Your Email Open and Click Rate
- Before Hitting "Send", Craft Emails Your Customers Will Want to Read

6. Minimize Your Complaint Rate.

Every time a recipient hits the "this is spam" button, a complaint is recorded by the mailbox provider spam filters.

If the complaint rate exceeds a certain percentage (0.1% complaint rate is considered acceptable), all future campaigns from that particular sender are sent directly to Spam bypassing the Inbox.

The only way to reduce spam complaints that really works is to send emails to those people who have requested it.

Use a confirmed opt-in process to capture email subscribers and send relevant messages.

Ask your subscribers to add your sender email address to their address books or whitelists immediately after they subscribe. It can help their servers recognize your emails as desired, increasing the potential that it will pass through the filters.

Here is an exhaustive article about spam complaints where you can learn about all possible reasons people send complaints, how complaints impact deliverability and how to address them.

7. Brand Your “From” Field.

It's always better to have a friendly text in the "From" field rather than an email address alone. But do not use a generic text like "Customer Service" or "Sales Department."

Include your brand name instead: "Julia from GlockApps", "GlockApps Customer Service", "GlockApps Sales Department." A "From" name without your brand is automatically suspicious.

Never use an email like noreply@yourdomain.com in your reply email field. It's not illegal, but it's a bad email marketing practice that hurts your deliverability.

Some ISPs, network spam filters, and customers' personal email security settings are set up to move messages with "no-reply" addresses to the junk folder.

It's also a question of ethic. By not allowing the recipients to reply to your email campaigns, it makes you look like you don't care about them. It's a one gate play when you can blast them with emails and they can not communicate back. And it increases the likelihood they will report your email as spam.

Here you can read more about 7 Reasons Why You Should Not Send from a "No-Reply" Email Address

8. Maintain List Hygiene.

Mailing to a large number of addresses that appear to be invalid or abandoned is a negative signal to mailbox providers and plays against your reputation.

Thus, it's imperative that you clean out your list by removing hard bounce email addresses and email addresses of the recipients who complained. It's a good idea to sign up for feedback loops with ISPs to get notifications when a complaint is recorded.

You should also remove unsubscribed users from your list immediately.

And to reduce your costs and increase your open rate, you'll want to clean out unengaged subscribers who are not interested in your emails anymore but did not unsubscribe for some reason.

You can send a re-subscribe link to see if your subscribers still want to be included on your list. Then separate the subscribers who have not responded from your mail list, to keep your main list active and clean.

And if you have not emailed to your list for 6-12 months, it's a good idea to check it for validity before you start sending. The easiest way to check the list is by using an online verification service like BriteVerify or DataValidation.

If you are an advanced user and know how to configure a Windows VPS to emulate the SMTP server, you can consider a cheaper alternative – desktop software like Advanced Email Verifier.

9. Authenticate Your Emails.

Authentication helps protect your emails from forging and prove that you are the sender who you say you are. Email messages that do not pass authentication checks may be blocked or are subject to additional filters, potentially preventing them from coming to the user's Inbox.

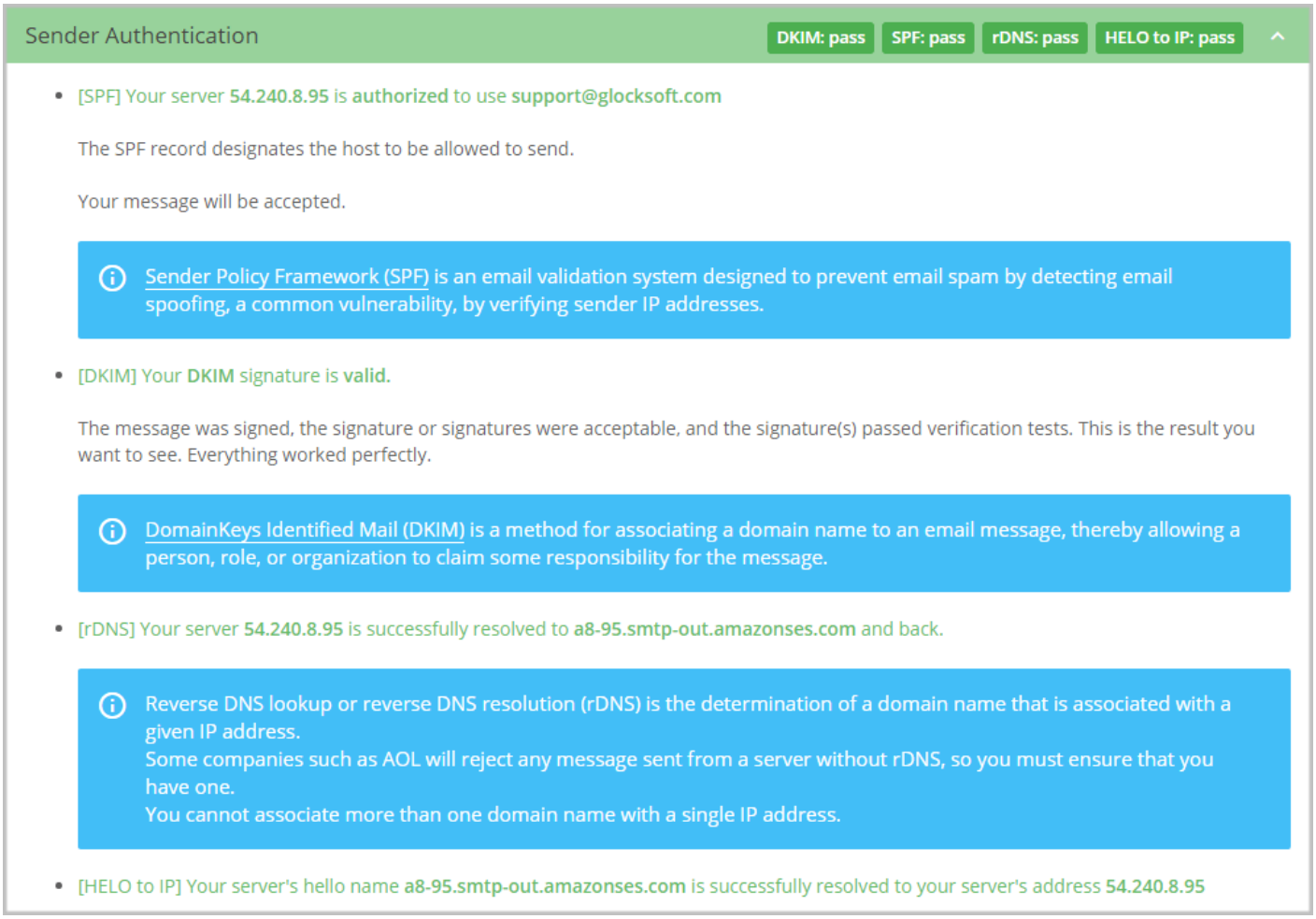
Plus, authentication is essential for protecting your brand and preventing forged messages from damaging your sender reputation. Many Internet providers use authentication, among other things, to track sender reputation.

There are different methods to authenticate the sender such as SPF, DKIM, rDNS, and DMARC. There is no agreed best method for authentication, and different ISPs can use different methods to check the sender's authenticity. That's why it's important to have all authentication records set up correctly.

Thus, if you use your own SMTP server with an in-house email system, implement outbound email authentication with valid PTR, DKIM, and rDNS records.

You can use the GlockApps service to test your authentication records and make sure they are in the "green" zone.

Authentication test from GlockApps



10. Watch Your Email Reputation.

Email reputation has a great impact on whether or not your emails will be sent to the Inbox and consists of two components: IP reputation and domain reputation.

Some mailbox providers look at your IP reputation while others evaluate your domain reputation.

For example, AOL has its own IP reputation monitor and rates the sender's IP reputation as "bad", "neutral", and "good". If your IP reputation is "bad" with AOL, you'll see your emails filtered out as junk mail or blocked altogether. A "neutral" reputation is generally OK.

Gmail, on the opposite, relies on the sender's *domain* reputation. If you're sending a lot of emails to invalid email addresses or receiving a lot of complaints, then Gmail will block your domain. So, you'll have to set up a new domain and build a new reputation for it to get your emails delivered to your Gmail recipients.

More and more mailbox providers are switching to the domain reputation because it's easier to change the IP than to change a domain considering all the data that needs to be set up on the new domain.

So, if your email messages are consistently ending up in the junk folder for one or more of the major mailbox providers, then it's possible the issue is in your email infrastructure.

First, look at your IP reputation.

In GlockApps, you can setup an automated process of checking your IP against blacklists and be alerted via email when the IP got listed. If a blacklisting issue happens, you should go through the removal process. The removal instructions are usually stated on the blacklist's website.

If your IP doesn't have significant issues, then you can probably keep it as you don't want to hop from IP to IP (pure spammer's tactic!).

If you have a good IP reputation, but see that your messages are still sent to the spam folder, then you will want to test your domain.

Start sending messages from a new email address on the same domain and see where they are going to.

If the issue is still there, you may consider setting up a new domain for your marketing campaigns and start building a good reputation for your new domain. It is costly and time-consuming, but possible if there is no other solution.

Stay off blacklists at all costs. There is a number of blacklists that can heavily impact your deliverability. So, you should scan your IP regularly to make sure it's not blacklisted. You'll want to avoid blacklisting issues for both your IP and your domain.

11. Choose Best Email Provider.

Using a good email provider, delivery vendor or SMTP server can considerably increase your deliverability rate.

Emails sent through large email providers are more likely to get flagged as spam simply because of the high volume of emails they send out, but they're also more likely to fix the issue quickly when it happens.

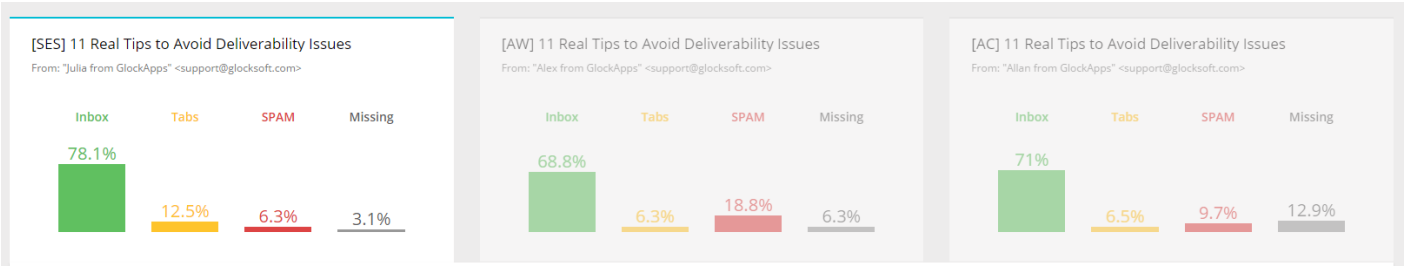
Emails sent through small vendors are less likely to be flagged as spam, but when it happens, it can be time-consuming for them to address the problem.

A lot of email providers claim that they provide almost 100% delivery rate, but they do not tell anything about their *Inbox deliverability rate*. It's better that you don't take it on trust, but test their deliverability yourself and compare their Inbox placement rates.

Set up free accounts with different delivery vendors or ESP and send tests using GlockApps. Then compare the reports and see which one provides the best deliverability.

After testing multiple tools including MailChimp, SendGrid, Mailgun, Amazon SES, AWeber, Active Campaign and others, we found out that the best Inbox placement rate is achieved with Amazon SES.

Deliverability chart from GlockApps: Amazon SES, AWeber, ActiveCampaign



To send emails through Amazon SES, you can use in-house email software like [EasyMail7] that works as a front-end to SMTP relays and delivery vendors. EasyMail7 is integrated with Amazon SES and works perfectly with Amazon SES API and SMTP settings.

12. Be Consistent at Sending.

Inconsistent senders who send large volumes of emails after a long term of inactivity can be an indicator of a spammer or compromised server.

Inconsistent sending can also provoke spam complaints if your subscribers forget they have subscribed to your list or lose interest in what you have to provide them.

They may delete your message without opening it or send a complaint by marking your message as spam. Thus, you should try to send emails regularly in order not to let your list “freeze”.

On the other hand, sending too often can lead to a negative reaction from the recipients as well.

So, there is a good reason for maintaining a steady flow of communication with your list, rather than relying on occasional, massive "blasts" or overwhelming the subscribers with a dozen of emails per day.

Ideally, you should tell the subscribers how often they will receive emails from you during the signup process and stick to the frequency that you promised.

13. Keep Your Subscribers Engaged.

Engagement is seen as a positive interaction of a recipient with email messages: opens, clicks, replies, forwards, and "not spam" markings.

Each mailbox provider has its own criteria for measuring engagement. Some are more advanced than others, but all do evaluate subscriber engagement to make Inbox/Spam placement decisions.

Microsoft, AOL, Gmail, and Yahoo are the industry leaders in their use of engagement metrics to determine email placement.

Thus, you should aim at keeping an engaged subscriber base — people who like receiving their emails, who open them regularly, and interact with the content.

Following are some best practices for keeping subscribers engaged:

1. Start building relationships from the beginning by setting clear expectations, sending a welcome message, and then following with what you've promised.

2. Send messages that look nicely on any device. Use a template that is easy to scan and capture the essence, and offer content that meets the subscribers' interests.

3. Monitor engagement metrics. Engagement-based metrics such as "deleted unread" and "marked as not spam" provide a better way to understand Inbox filtering decisions and determine whether engagement filtering is actually a problem. These metrics are available today with data providers like Return Path.

4. Re-engage inactive subscribers. Unfortunately, every email list sooner or later will contain recipients who are not actively engaged. Re-engagement campaigns can help you recapture the attention of inactive recipients and not lose the list quality.

What to Do Next...

Now it's time to put into practice what you've read in this whitepaper. You can do these 4 things right now:

1. Test your email quality and deliverability with GlockApps.
2. Check your report to find elements that failed the test and correct them.
3. Check your email list acquisition method and make sure you're not sending without permission.
4. In GlockApps IP Reputation monitor, setup an automated process of checking your IP against blacklists to be alerted via email when the IP got listed.