Email Deliverability: the Ultimate Guide

Why does email deliverability matter?

According to the "2015 Email Data Quality Trends Report" by Experian, a majority (73%) of companies experienced email deliverability issues in the past 12 months. Return Path has reported that over 20% of legitimate email are missing.

Undoubtedly, marketers have problems with deliverability, and that negatively affects their business. "The most common consequences of poor email deliverability are the inability to communicate with subscribers (41%), poor customer service (24%), unnecessary costs (22%), and lost revenue (15%)" - the Experian's "2015 Email Data Quality Trends Report."

How to deliver emails to the recipient's Inbox?

This simplest question might have the most complicated answer. As an email marketer, you have to make people engage with your emails in a positive way: open, click, forward or reply. Recipient engagement is a powerful factor that mailbox providers rely on when filtering inbound messages.

Keeping recipients engaged is not just about sending beautiful, optimized emails. It's also about positioning yourself as a reputable sender, avoiding spam filters and getting to the user's Inbox. That's where email deliverability comes in.

In this article, we'll touch the most important factors that determine email deliverability and should be on the mind of every marketer:

1. Permission-Based Marketing:

- Single Opt-In vs. Confirmed Opt-In
- Pre-checked Boxes or Passive Opt-in
- Subscriber's Expectations

2. Sender Reputation:

- Branding
- Spam Traps
- Bounces and Complaints
- Monitoring Tools

3. Sending Infrastructure:

- Shared IP vs. Dedicated IP
- Blacklists
- Email Authentication
- Feedback Loops

1. Permission-Based Marketing.

Single Opt-In vs. Confirmed Opt-In

The opt-in is the process of an email recipient enrolling in a mail stream. There are three main types of the opt-in process:

- **Unconfirmed opt-in** is when a sender adds an address to their mailing list without asking for the email address owner's permission. This happens when the sender purchases or rents email lists from other marketers, or harvests emails addresses on the Internet using automatic harvester tools.

- **Single opt-in** is a process when a new subscriber is not asked to confirm their subscription. Their email address is instantly added to the email list after registration.

- **Confirmed opt-in** is a process that requires a new subscriber to confirm their subscription. Each new subscriber typically receives a confirmation email that requires them to click a link. Only after the email address is verified, the new subscriber is added to the email list.

The unconfirmed opt-in process is acknowledged as a big "no-no" in email marketing and prohibited by law in many countries, notably in France, Germany, Belgium, Italy and others.

Thus, best email marketing practices teach senders to get the subscriber's permission prior to sending emails to them. There is a debate about what opt-in method is better.

Let's consider the pros and cons of the single opt-in and confirmed opt-in method so that you can decide.

Pros of a single opt-in process:

- **Simplicity**. It's a one-step action.

- **Speed**. The subscription is instant.

- **High list growth**. Because of the simplicity and speed of in the registration process, the single opt-in approach typically produces higher numbers of email subscribers.

Cons of a single opt-in:

- **Fake emails**. Some people will try entering a fake email address to only gain access to content.

- **Malicious subscriptions**. Sometimes, people may sign up someone else to a list to get back at them.

- **Typos**. Human errors are inevitable during registration.

- **List hygiene**. You have to spend time for validating your list before starting your email campaign and clean it from fake, bogus and invalid addresses. Mailing to these addresses will negatively impact your reputation.

What about the confirmed opt-in approach?

Pros of a confirmed opt-in:

- **Engaged subscribers**. You'll come up with a list of people that actually want to be on it.

- **Valid data**. By its nature, the confirmed opt-in process yields cleaner lists by asking for the subscription confirmation.

- **Proof of permission.** It helps if you have troubles with your email service provider because of spam complaints.

Cons of using a confirmed opt-in:

- **Extra step**. Some people will not mind to confirm, others will be annoyed.

- **Smaller lists**. There will be subscribers who initiate but fail to complete the subscription process. They may not confirm for multiple reasons: did not want to wait for the confirmation email, misunderstood the confirmation email instructions, confirmation email did not arrive or arrived to a different tab and was missed, and so on.

According to Top 500, this year's analysis revealed that approximately 9% of retailers used a double opt-in, or confirmed opt-in, process with subscribers. Compared to 2015, we observed a 3% growth in double opt-in usage versus last year.

Pre-Checked Boxes or Passive Opt-in

Some companies use a passive opt-in process when a user who registers a free trial or creates a free account with them is automatically subscribed and must check an empty box if he doesn't want to subscribe to mailings.

As a rule, people fill the form on auto-pilot and get subscribed without giving an explicit consent. Thus, in some countries, for example, in Netherlands, pre-checked boxes are not allowed on the opt-in form.

In other countries, a passive opt-in process may be legal, but it is still not recommended because in the future it can result in a high complaint rate.

Final thoughts:

If you want to protect from spam traps and minimize your risk of being blacklisted, use a confirmed opt-in method.

If you want more engaged users, use a confirmed opt-in.

If you want more opens and clicks and higher ROI, use a confirmed opt-in.

If your primary goal is to build a huge list fast, use a single opt-in or passive opt-in.

But don't take your decision based on email marketing tips only. Test with your audience, your content and offers. Test, analyze, and choose.

One more thing:

Your clients and buyers are *not* your email subscribers. While you can send them an onboarding email, transactional email or registration email, you do not have permission to send them marketing emails until they subscribe.

If people bought your product, downloaded a free trial or signed up for a free account on your website, send them an onboarding email following the event.

In the email, you can thank them for buying or trying your product or service, include links to useful resources like tutorials and FAQ and invite them to join your mailing list by going to the subscription page.

However, in the US, Canada, and Australia where laws are far tougher than Europe by virtue of being your customer the person is deemed to have provided implied consent and can therefore be sent email marketing messages.

And in almost all of Europe this is currently the case but the law is due to change. So it may be considered a good idea to try and start emailing your customers in Europe now to gain express permission and informed consent. Otherwise, you might lose the opportunity to market to what could well be the highest performing portion of your list, pre-existing customers.

Subscriber's Expectations

Before you start communicating with your subscribers, remember that everything you do as a marketer is creating an impression and impacting what they think about your brand.

Your opt-in page is the place where you set the subscriber's expectations, i.e. formulate the promise of what you will deliver to people who give you permission.

You have multiple channels to set the expectations when it comes to your email program:

- **Landing pages and opt-in forms**. This is the place where you explain the benefit of being subscribed. Tell about the type of content you'll deliver and the frequency at which they can expect to receive messages from you.

- **Confirmation emails and thank you pages**. This is the opportunity to reconfirm everything that you mentioned on the landing page.

- **Welcome emails**. Another chance to hit them with a re-cap of your mailing program and show them how to update their preferences if it's available.

- **Preference center**. Giving subscribers the option to update their preferences will help you reduce unsubscribes and complaints. If you manage multiple email lists, it's recommended that you allow users to choose between opting-out of a single email list or opting-out of all mailings you send.

- **Unsubscribe page**. Make the opt-out process a breeze, and a two-click at the most. If you offer the preference center to update contact information, frequency or mail streams, show it here.

- **Privacy Policy and Terms of Use**. Both are important places where you set expectations. Link to them from every email you send.

An important note about expectations is that they never end. You have to stick to what you promised throughout your entire email campaign. Send the content you promised to send. Don't send more or less frequently than the expectation you set. If you promised a 20% off deal once a month, deliver it. Failing to do so will compromise the integrity of your email program.

You can analyze successful email programs from the competitive brands. See what other brands use (single opt-in or confirmed opt-in), what they promise, what subscriber's data they collect and how they use it, what content they send and what mail frequency options they provide, and so on. You'll learn from their experience to start email marketing.

2. Sender Reputation.

Your reputation matters. Just like in business, your reputation as an email sender matters when it comes to email deliverability. The better your sender reputation, the more emails are delivered to the Inboxes of your subscribers.

Let's consider the things that create your sender reputation and have a direct impact on it during the entire mailing program.

Branding.

Your domain is your representation. In email marketing, the sender's domain is what creates the identity that your subscribers, the recipients of your marketing and transactional messages trust or not. If they trust, you get more opens and clicks and higher ROI. If they don't trust, you guess what. So, your goal is to build that trust and guard it as your business depends on it.

In an effort to get your sender's identity in order, we are going to focus on the From Name, From Address, and the links used within the email.

Considering that the average email user receives 200 emails per day, clearly identifying yourself helps you wade through the Inbox jungle.

From Address.

A branded and appropriate From Address is important for making your subscriber open the email. If you have multiple mail streams, create a related From Address for each mail stream (e.g., newsletter, support, sales,

marketing) and stick to it. Mailbox providers like to see stability in the From Address, too.

If you use an email address from a free domain, DMARC authentication policies implemented by some free email services like Gmail, Yahoo!, and AOL can affect the deliverability of your emails sent by various email service providers. According to the DMARC policy, if you are using a From Address from a free domain, you must also use the related free SMTP server to send your message. Thus, we highly recommend registering and using your own domain tagged to your brand.

Important note:

Do not use a "no-reply@" email address in your email marketing. Some ISPs, spam filters, and customers' personal email security settings are set up to automatically filter messages coming from "no-reply" addresses to the junk folder. Then, it's about trust. Would you trust someone who does not want to hear back from you?

From Name.

A good From Name should:

- reinforce the subscriber's trust in your brand;

- provide insight as to the type of the message you're sending;

- increase the chances of a message being found by a subscriber in the Inbox or other folder (i.e., Promotions tab, Social tab, junk);

- make it easy for the subscriber to add your email address to their address book;

With that said, avoid using a generic friendly From Name like "Weekly Newsletter", "Account Verification", "Monday Tips". Brand your From Name like "GlockApps Weekly Newsletter", "GlockApps Account Verification", "GlockApps Monday Tips". A "From" name without your brand is automatically suspicious.

You can even be more creative about your From Name and set it to show your name and company name like "Julia from GlockApps". After all, there is nothing wrong with testing different From Names.

From the legislative side, if you are mailing to U.S. subscribers, you must use a From Address and Reply-To Address that are "accurate and identify the person or business who initiated the message."

For Canadian subscribers, you must identify yourself and the person on whose behalf a commercial electronic email message is sent.

For E.U. subscribers, disguising or hiding the identity of the sender is strictly prohibited.

Links.

Branded links also help your recipients feel comfortable with your email. When your subscribers hover over a link or image in the content, ensure that the link leads to your domain, or a subdomain, and not to a shared domain provided by a third party.

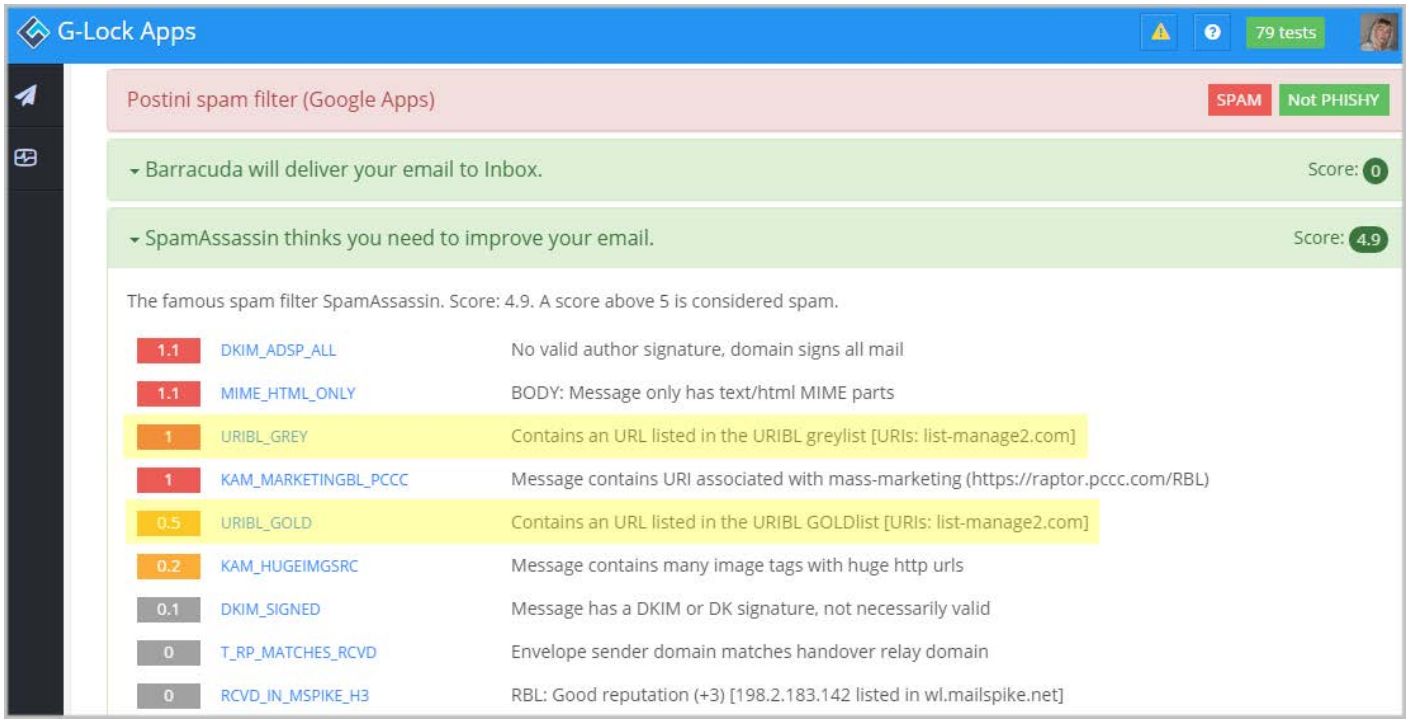
Most ESP and email tracking services, for example, G-Lock Analytics, have the ability to brand tracking links with your domain which reinforces trust.

Do not host images and links on fishy sites that may be blacklisted. Links and images from blacklisted domains often cause message blocking and filtering.

It's recommended to run your message through a content checker to determine potential issues.

For example, GlockApps spam testing tools support content-based filters such as Postini, Barracuda and SpamAssassin that will report anything that might cause your email to be sent straight to the spam folder. You can identify and fix spam triggers before deploying your campaign.

SpamAssassin report from GlockApps



Spam Traps.

Spam traps are email addresses that are used not for email communication, but for identifying senders with poor quality email lists, i.e. spammers.

You might be lucky and not kill your sender reputation completely if you hit a spam trap address, but often times the consequences are serious.

It's important to differentiate two main types of spam traps:

- **Recycled spam traps**.

They are email addresses that were used by a person and then abandoned. The common practice of ISPs is to turn an abandoned email address into a spam trap after a 6-month period. If you send an email to a recycled spam trap, it shows that you are not managing your list properly and you are not actively removing your unengaged users. The good news is that if you show the ISP a proof that the person who used that email address before subscribed to receive your emails, then it's rather easy for you to get unblocked.

- **Pristine spam traps**.

These are true traditional spam traps when an ISP or anti-spam organization deliberately setups an email account and uses it to catch spammers. No one should be sending emails to those addresses. If you do, it typically means that you scraped the list online and you will be penalized for that. It will cause you a lot of trouble and a lot of harm to your sender reputation.

In the case of Microsoft (Hotmail/Outlook.com) they only operate pristine spam traps, the same is true of Yahoo, and one hit rarely if ever gets you immediately blacklisted.

What about role accounts?

A role address is not a spam trap. It is generally foolish for most to send marketing emails to these email addresses because they are not associated with a particular person, but rather with a company, department, position or group. Role accounts begin with admin@, webmaster@, hostmaster@, sales@, support@, postmaster@, etc. and are not generally intended for personal use.

The most common ways you can acquire spam traps on your list are:

1. **By purchasing and/or harvesting email addresses**. Firstly, such lists are collected without permission and do not contain opt-in records. Secondly, when you buy or harvest email addresses, you cannot tell how old the email address is and if it's still valid or not.

2. **By using an old list that has not been emailed for years**. If you do not contact your subscribers during a year or more, you cannot be sure that all those emails are still active and are being monitored by their owners.

3. **By using a single opt-in method**. The user can simply enter his email address with a typo and the mistyped address can turn to be a SPAM trap. And sometimes people do not want to subscribe with their real email and use a fake email address. Fake email addresses may be used as spam traps as well.

The penalties for hitting a spam trap account depend on the type of the spam trap you hit, number of hits, and how the spam trap owner handles things at their end.

Of the two types, pristine spam traps represent the greatest danger for your reputation. Hitting a pristine spam trap account will almost always result in an immediate block on your sending IP address. If a spam trap is maintained by an ISP, such as Yahoo! or AOL, that ISP could permanently blacklist your whole "From" domain.

If you hit a spam trap operated by an anti-spam service such as Abusix, Spamhaus, or SpamCop, you'll have deliverability issues at ISP and mailbox providers who consult that service's database to filter incoming emails. Just one hit of a SPAM trap address at an anti-spam organization can reduce the Inbox deliverability to major ISP in 3-4 times.

Tip:

If you suppose your deliverability problems are caused by spam trap hits, change your list acquisition practices. Often times, the root cause of deliverability issues lays in bad list acquisition practices. Until you change them, you're doomed to failure.

Bounces and Complaints.

Next, let's talk about bounce emails and abuse reports (spam complaints) as they have an impact on your sender reputation, too.

When an email message is returned to the sender after not being accepted by the recipient's mail server, the email is called bounce.

There are different reasons why emails bounce and the reason of the bounce is explained in a "return to sender" message.

Not all bounce emails have the same impact on email deliverability. There are "innocent" bounce messages such as challenge-response or auto-reply ones.

"Mail block" bounce emails are helpful in understanding how the recipients treat your mailings. A lot of "mail block" emails is a sign that you should revise your email program and pay attention to the message content and your sending IP/domain.

Soft and transient bounce can be ignored until they turn into hard bounce ones.

The most important types of bounce emails that can't be ignored are hard bounce and abuse feedback reports.

A hard bounce happens at the result of a permanent delivery failure because the recipient's email address is invalid or no longer in use.

Spam complaints are a direct signal from a recipient to the mailbox provider that your emails are unwanted. Most ISPs have a "Report Spam" button that the email users can click on and report the ISP that the email is undesired.

To help you deal with complaints, ISP provide a feedback loop service. After you sign up, the ISP will send you FBL emails that happen from users' spam reports. FBL emails typically include the original message so you are able to extract the email address of the complaining user and suppress it from your list.

Both hard bounce and complaints indicate that the sender uses bad list acquisition and/or list management practices and sends unwanted or irrelevant messages.

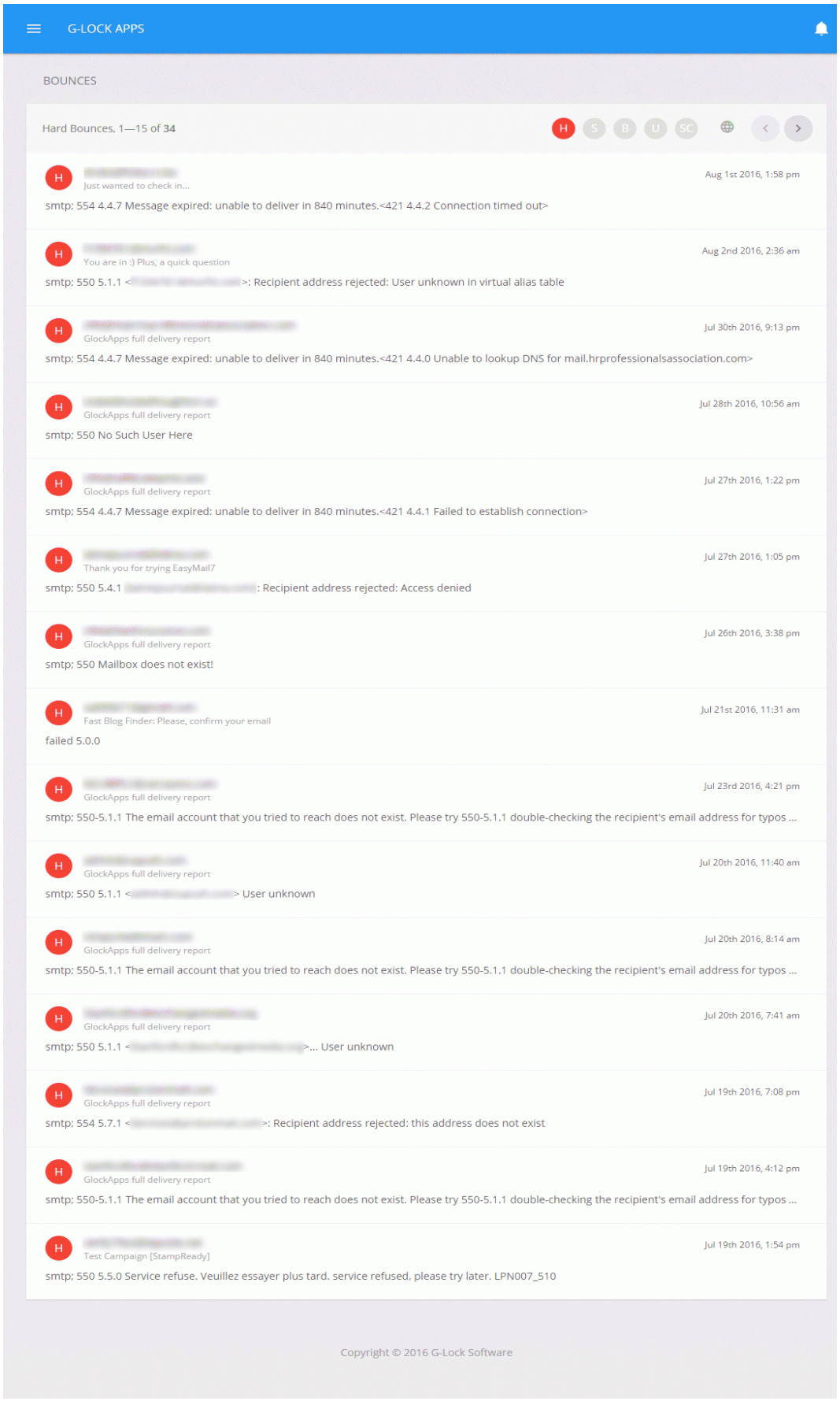
The industry's average bounce rate should be between 2-3%. The complaint rate is even lower - 0.1% is acceptable and often seen among good senders.

If your list is regularly generating higher bounce and/or complaint rates, it's important that you work out why and take steps to reduce the number of bounces.

Needless to say that you have to setup a working process of handling your bounce messages after each mailing. Most email service providers have bounce email handling as a feature, so you don't need to worry about it. But if you are managing your own SMTP server or sending through a delivery service like Amazon SES, you have to handle your bounces yourself.

There are bounce handling services out there that you can consider. For example, the GlockApps service includes the bounce and feedback loop monitor tool that processes returned emails for you in real time and provides you with daily reports. You can use this data to suppress complainers and bounce emails from your subscriber list.

Bounce email report from GlockApps



Final thoughts:

Below are 5 easy practices for building and keeping your good sender reputation from the beginning and across all your email marketing activity:

1. Use a confirmed opt-in method to grow your list.

A confirmed opt-in list of recipients who have requested your emails is the main prerequisite for a good sender reputation and high deliverability.

2. Clean your list regularly.

If your email campaigns start generating a lot of bounces, it's time to clean your list. You can use desktop software like Advanced Email Verifier or online email verification service like DataValidation, BriteVerify, or NeverBounce.

3. Setup your authentication records.

Implementing DKIM, SPF and DMARC authentication dramatically helps your deliverability by confirming that the email came from where it says it came from. We'll talk more about authentication in chapter 3.

4. Check your IP against blacklists.

Being blacklisted severely impacts your reputation and your ability to deliver emails to your subscribers. You never know whether or not your IP is blacklisted until you test it.

5. Handle bounce, FBL and unsubscribe emails.

It's all about list hygiene. It should be a part of your email program from the beginning. Unsubscribes, feedback loops, and bounce handling should go without saying.

Monitoring Tools.

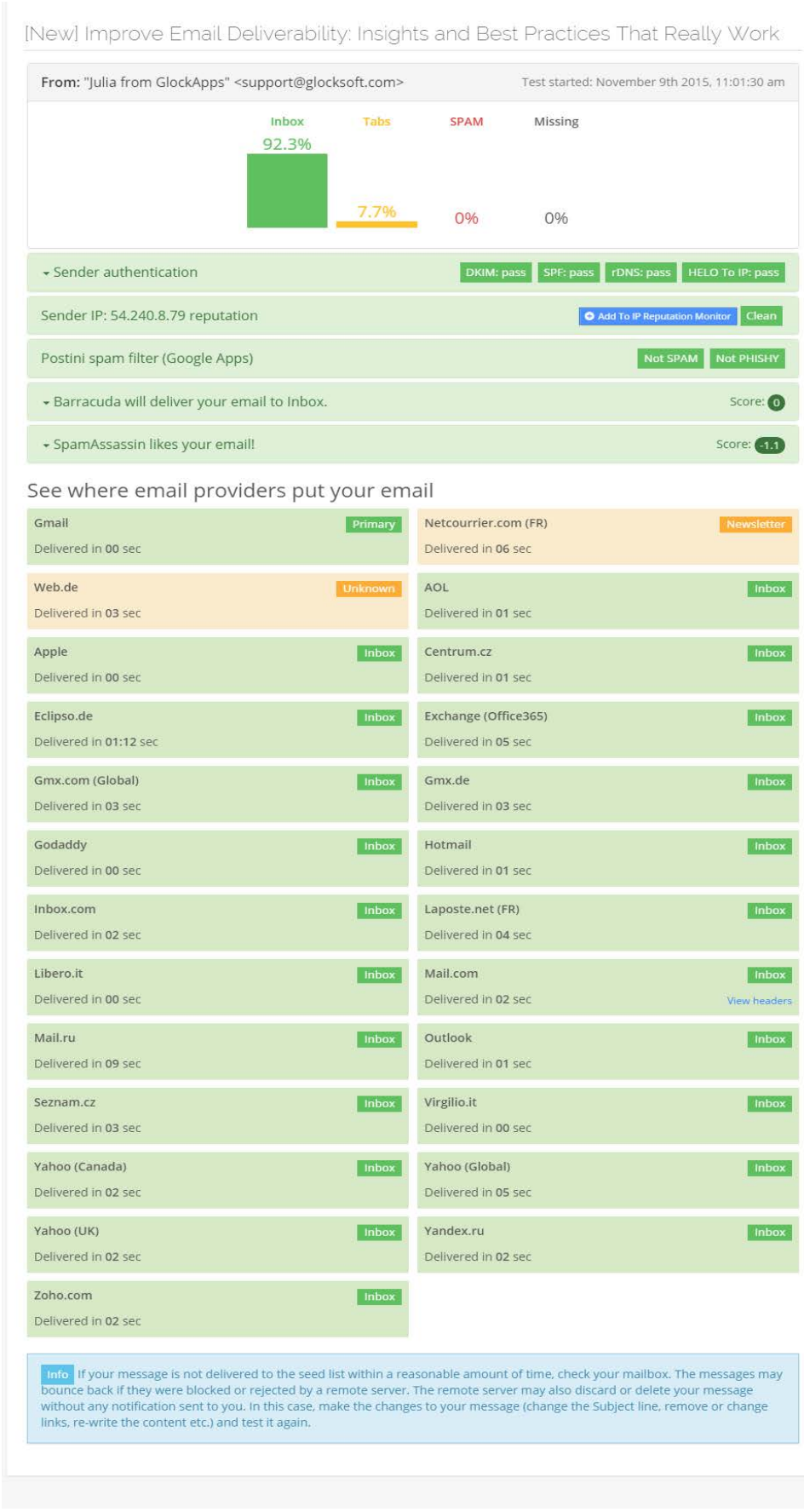
Is your sender reputation affecting your email deliverability? To find out how ISP and other email receivers rate you as a sender, you can use the following testing and monitoring tools:

– Senderscore.org run by Return Path. The score ranks from 0 to 100, 100 being the best. It tells you how you're performing. For good deliverability, you should maintain your sender score of 90 or better.

– Senderbase.com run by Cisco. It tells you how your reputation is across all the network providers Cisco manages. The reputation score is grouped into Good, Neutral, and Poor.

- GlockApps run by G-Lock Software. It tests your Inbox placement rate, spam placement rate, IP reputation, sender score and spam score and helps you determine and fix possible deliverability problems before you send the message to your subscribers.

GlockApps email deliverability and reputation report



[New] Improve Email Deliverability: Insights and Best Practices That Really Work

From: "Julia from GlockApps" <support@glocksoft.com>

Test started: November 9th 2015, 11:01:30 am

Inbox	Tabs	SPAM	Missing
92.3%	7.7%	0%	0%

- Sender authentication — DKIM: pass | SPF: pass | rDNS: pass | HELO To IP: pass
- Sender IP: 54.240.8.79 reputation — Add To IP Reputation Monitor | Clean
- Postini spam filter (Google Apps) — Not SPAM | Not PHISHY
- Barracuda will deliver your email to Inbox. — Score: 0
- SpamAssassin likes your email! — Score: -1.1

See where email providers put your email

Gmail — Primary Delivered in 00 sec		Netcourrier.com (FR) — Newsletter Delivered in 06 sec	
Web.de — Unknown Delivered in 03 sec		AOL — Inbox Delivered in 01 sec	
Apple — Inbox Delivered in 00 sec		Centrum.cz — Inbox Delivered in 01 sec	
Eclipso.de — Inbox Delivered in 01:12 sec		Exchange (Office365) — Inbox Delivered in 05 sec	
Gmx.com (Global) — Inbox Delivered in 03 sec		Gmx.de — Inbox Delivered in 03 sec	
Godaddy — Inbox Delivered in 00 sec		Hotmail — Inbox Delivered in 01 sec	
Inbox.com — Inbox Delivered in 02 sec		Laposte.net (FR) — Inbox Delivered in 04 sec	
Libero.it — Inbox Delivered in 00 sec		Mail.com — Inbox Delivered in 02 sec — View headers	
Mail.ru — Inbox Delivered in 09 sec		Outlook — Inbox Delivered in 01 sec	
Seznam.cz — Inbox Delivered in 03 sec		Virgilio.it — Inbox Delivered in 00 sec	
Yahoo (Canada) — Inbox Delivered in 02 sec		Yahoo (Global) — Inbox Delivered in 05 sec	
Yahoo (UK) — Inbox Delivered in 02 sec		Yandex.ru — Inbox Delivered in 02 sec	
Zoho.com — Inbox Delivered in 02 sec			

Info If your message is not delivered to the seed list within a reasonable amount of time, check your mailbox. The messages may bounce back if they were blocked or rejected by a remote server. The remote server may also discard or delete your message without any notification sent to you. In this case, make the changes to your message (change the Subject line, remove or change links, re-write the content etc.) and test it again.

– Postmaster.google.com. After you sign up and verify your domain, your account will have access to the domain's data on Google Search Console. You can use it if you experience deliverability problems to your Gmail users.

– Postmaster.live.com. Microsoft's Smart Network Data Services gives you the information about the traffic originating from your IP address such as the volume of sent emails, complaint rates, and spam trap hits. It's recommended to analyze your SNDS report if you are unable to deliver your emails to your Hotmail, Live, and Outlook recipients.

3. Sending Infrastructure.

In addition to your sender reputation, the receiving ISP is also looking at your sending infrastructure. No matter how valid and confirmed your list is, your emails may still be filtered if your sending infrastructure is not in order.

Let's talk about the most important elements of the sending infrastructure that have the biggest impact on email deliverability: sending IP and authentication.

Shared IP vs. Dedicated IP.

When you send an email, it is transmitted from your IP address to the receiving mail server, which then decides whether or not to accept and deliver your message based on numerous factors including your sending IP reputation. A clean IP doesn't guarantee Inbox delivery yet, as the deliverability is a complicated concept, but it certainly matters.

Considering sending IP options, they include the use of a shared IP, a dedicated IP, or a pool of dedicated IPs.

The shared IP pool means a number of IP addresses used by an organization or a group of organizations to send emails. The shared IP pool is provided by most email service providers.

The good side of using the shared IP is that you don't need to "warm it up." Being used by other senders, the shared IPs already have a reputation.

The downside of using the shared IP is that it makes you dependent on other senders and gives you a limited ability to influence the sender reputation. It exposes you to a greater risk resulting from the sending activity of your IP neighbors.

A shared IP tends to level the performance for the best senders and lower quality senders. Email service providers are extremely skilled at identifying and blocking abusive senders.

A dedicated IP is what exactly how it sounds: an IP exclusively dedicated to your brand.

The advantages of a dedicated IP are: 1) it gives you total control over your reputation because only you define the type of the mail sent from that IP, and 2) it allows you to avoid a sender appendix like brand.esp.com associated with your emails. This appendix is added in the shared IP environment but not with dedicated IPs.

One downside of using a dedicated IP is that it has no sending reputation and needs to be "warmed up."

Below is one of the IP warm-up scenarios for the first seven days on the new dedicated IP:

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

As most reputation systems store data for the last 30 days, you should not interrupt your sending activity on that IP address for 30 days or more. If you do, then you will need to start from scratch.

Here you can read more about how to warm up a new IP address.

One more thing:

You must warm up your IP at EACH ISP. Make sure that each ISP is receiving a comparable amount of emails each day. Don't warm up Gmail on Monday, Yahoo! on Tuesday, Hotmail on Wednesday, etc., but evenly disperse your mail stream to each ISP on each day of the warm-up period. If you don't do it, your sending activity will look sporadic, and you won't be able to build a solid reputation with ISPs.

Frequently asked questions about the sending IP:

Should I go with a shared IP or a dedicated IP?

If you have a small list and send less than 50k messages per month, a shared IP will work just fine. With 50k+ messages per month, you can think about getting a dedicated IP. 200k+ messages per month, dedicated IPs are the best option.

Does a dedicated IP guarantee that nobody else can impact my sender reputation?

Not always. The truth is that the ISP can block the whole IP range your dedicated IP belongs to if it sees a bad behavior in that IP range. When purchasing a dedicated IP, choose an ESP that has a good reputation and ask questions about other senders in your IP subnet and their sending history.

How many dedicated IPs do I need?

You can certainly maintain a single IP. But we recommend that you differentiate IPs for your marketing email and transactional email streams. Transactional emails are more important and are treated as "wanted" mail by the ISPs. They are generally granted a little more "indulgence." Marketing emails typically have a greater risk of being filtered or blocked. That means you should have two IPs at minimum.

If you are a large sender and your ESP has hourly throttling limits, consider the max volume you can send per hour and stick to the hourly throttling limits per IP. You'll see how many IPs are required.

The bottom line:

If email marketing is an important part of your business, look at the overall budget of your marketing program and I bet you'll agree that the

extra $20/month or so you'll pay for a single dedicated IP address with SendGrid or SparkPost is a drop in the sea compared to your ROI from successful campaigns.

And don't forget your transactional emails that must be delivered to minimize customer inquiries and optimize your brand experience. So, if email is critical to your business and revenue, cost should not be the decisive factor when it comes to choosing the sending IP address.

Blacklists.

Blacklists present a real problem for email marketers. If the IP address that you're sending emails from has been associated with spam in some way, it may be on blacklists.

Before checking the content of the email, the filters check the sending IP address to see whether it is whitelisted or blacklisted. If it is whitelisted, the email is delivered without its content being checked at all.

If the IP is blacklisted, the email will be "black holed," bounced back or flagged as spam without the content being checked.

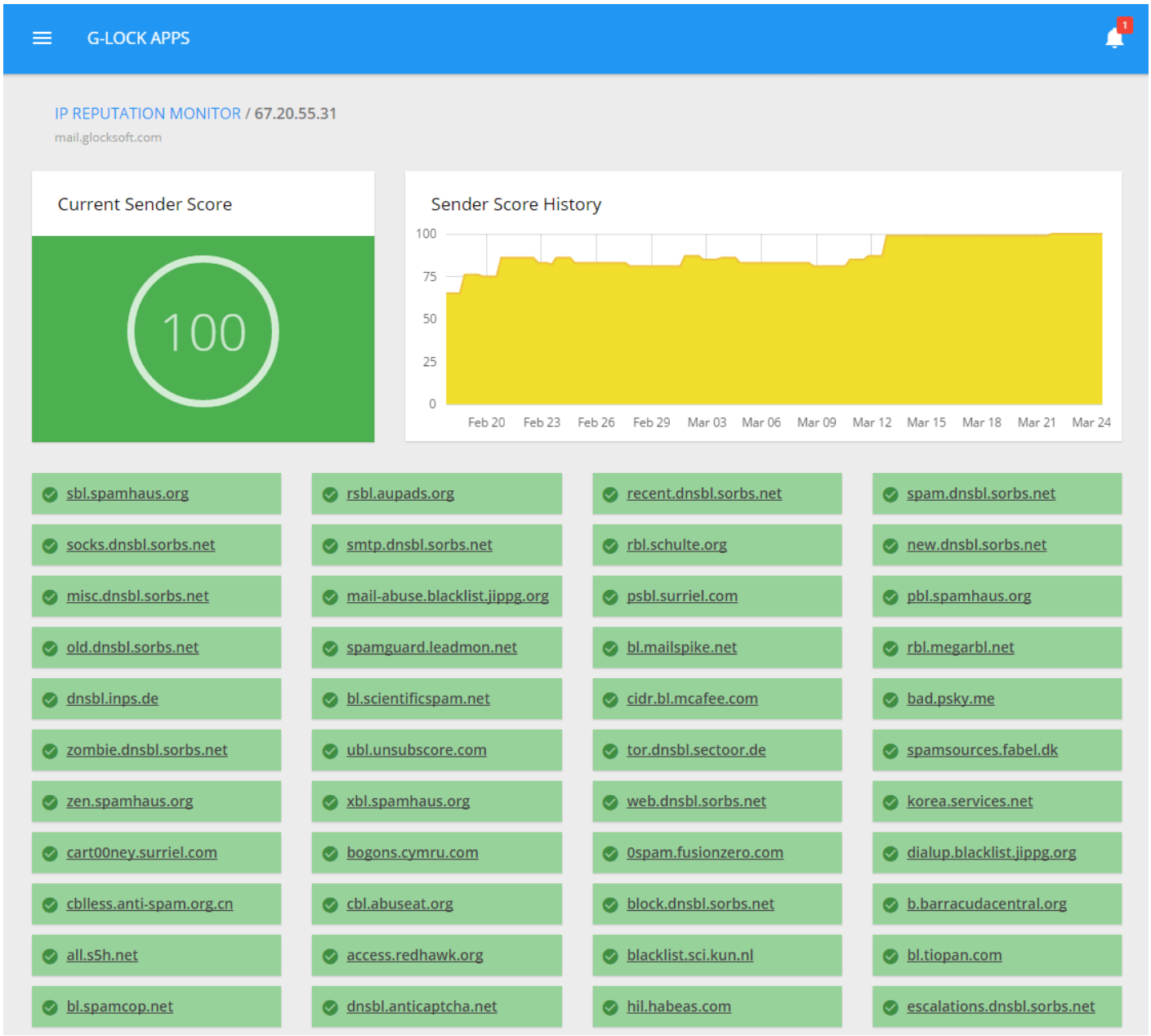
Black holed emails are not delivered to the user and are saved in a place accessible by administrators in case they are needed later. This approach is often used for emails that contain viruses to keep end users from opening them on accident.

There are a lot of blacklists, including widely used public lists and privately held ones. The most popular blacklists are Spamhaus, Spamcop, SURBL, Barracuda Reputation Block List, and MultiRBL.

It's important that you monitor your IP address reputation and if you find your IP listed on a blacklist, take time to find out and resolve the root problem that caused you to be blacklisted and then submit a delisting request. The delisting instructions are usually stated on the blacklist's website.

You can use tools like MXToolbox and GlockApps to test your IP against blacklists. In GlockApps, you can even enable email notifications to be warned if your IP status changes.

GlockApps IP reputation monitor



AOL has its own IP reputation monitor that rates the sender's IP reputation as "bad", "neutral", or "good." If your IP reputation is "bad" with AOL, your emails will be filtered out as junk mail or blocked altogether. A "neutral" reputation is generally OK.

Final thoughts:

You'll want to avoid blacklisting issues for both your IP and your domain. There is a number of blacklists that can severely impact your deliverability. Scan your IP and domain regularly to make sure they are not blacklisted.

Email Authentication.

Our next point is authentication.

Email authentication allows the mailbox provider to confirm that the sender is the one who he pretends to be and based on the result decide what to do with the message.

Authentication is a mandatory practice if you want to deliver to Inbox because spammers have become more malicious and clever. By spoofing your domain (i.e., your identity), they use a phishing technique to trick your customers and steal their personal information.

There are three primary methods of authentication:

1. DKIM is DomainKeys Identified Mail. It says that the message has not been altered in transmission. Your email service provider will keep the private key on the Mail Transport Agent (MTA), while you will update your DNS records with the public key. The public key and private key have to match to ensure that nothing happened to the message in transit. DKIM is intended to prevent forged sender addresses, a technique often used in phishing and email spam.

2. SPF is Sender Policy Framework which states which IPs are authorized to be sending on behalf of the "From" domain and allows the

receiver's host to verify that the email is being sent from the server it asserts it's sent from.

3. DMARC is the Domain-Based Message Authentication, Reporting and Conformance. It allows ISP to identify and treat email that is not properly authenticated by the DKIM and SPF standards.

DMARC allows you to use policies to protect your brand and email. The policy you select in your DMARC record will tell the participating recipient mail server what to do with the email that doesn't pass SPF and DKIM, but claims to be from your domain that contains the DMARC record.

The available policies are p=none, p=quarantine, and p=reject.

"p=none" tells the receiver to perform no actions against an email that does not pass the authentication, but still send email reports to the mailto: in the DMARC record for any infractions.

"p=quarantine" tells the receiver to quarantine the message that does not pass the authentication. Quarantine means "set aside for additional processing".

"p=reject" tells the receiver to completely deny any unqualified mail for the domain. With this enabled, only email that is verified as 100% being signed by your domain will even have a chance to get to the Inbox.

Important note:

The Microsoft properties (Hotmail, Outlook, MSN. and Live.com) are using Yahoo and AOL's DMARC p=reject. That means that when an email from a yahoo.com or aol.com address comes for a user with a hotmail.com, outlook.com, msn.com, or live.com account, if that email isn't actually sent from a Yahoo or AOL mail server, then it is being rejected (bounced).

That means if you're sending emails from your yahoo.com or aol.com email address, but not using the Yahoo or AOL mail server, change your "From" domain to prevent message rejection by the Microsoft properties.

In fact, there are at least a dozen major inbox providers who respect the DMARC policies and will reject the mail.

What authentication method should I use?

Using all three methods are required for the best email deliverability because DMARC relies on both SPF and DKIM you cannot have a working DMARC Authentication with either/or.

Here is a 3-minute foolproof guide to implementing DMARC from Andrew Bonar.

You have to implement email authentication if you are sending from your mail server or using a delivery service like Amazon SES, SparkPost, Mailgun or other. Email service providers, as a rule, authenticate your emails by default.

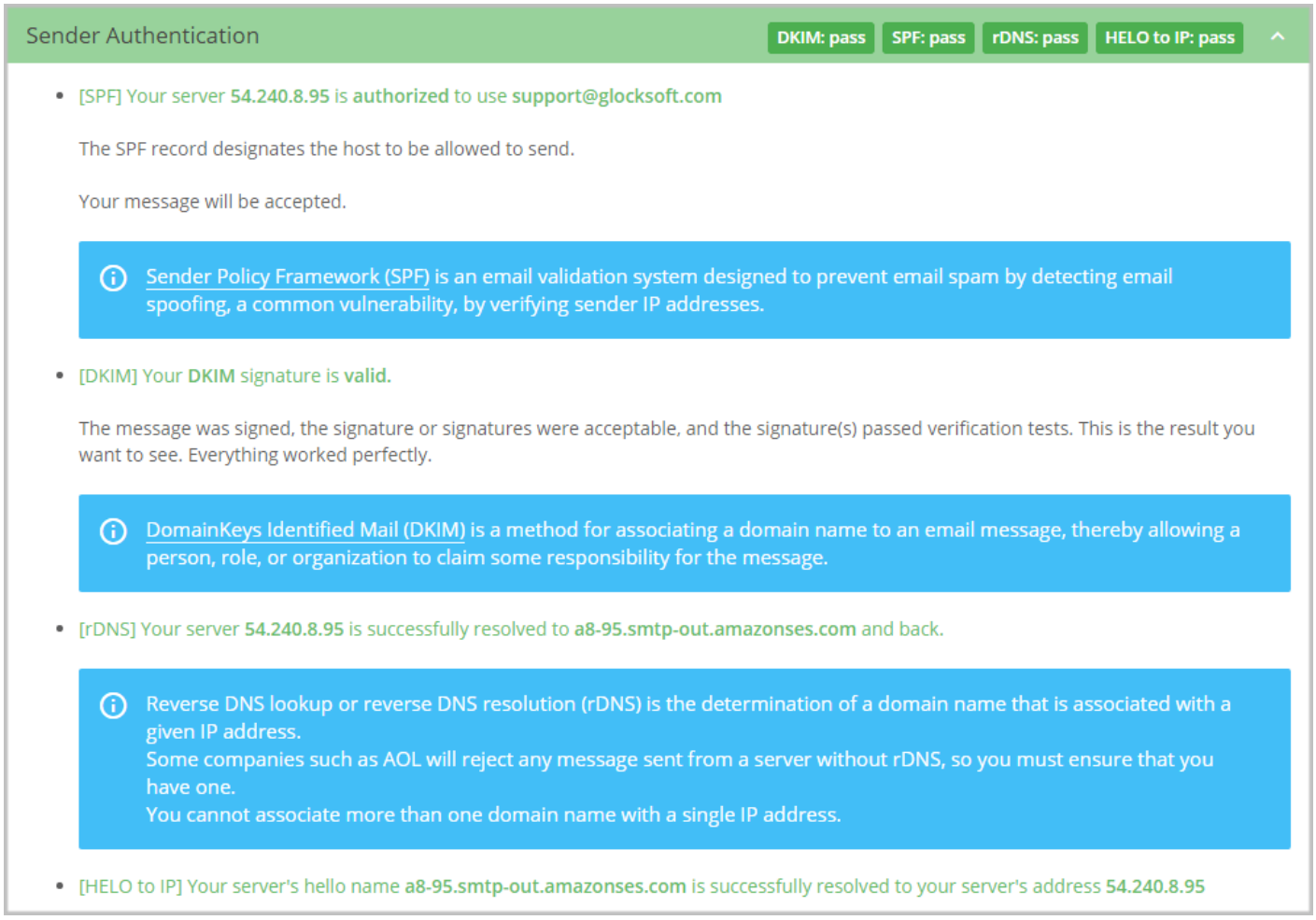
Amazon recommends that all AWS Email Service users publish SPF and Sender ID records to their DNS to ensure deliverability. With SparkPost and Mailgun, adding an SPF and DKIM records to your DNS is a requirement.

Many domain registrars provide self-service tools for managing DNS records. You can use these tools to modify your domain's DNS records, or contact your registrar for assistance.

And it's critical to perform email authentication testing on a regular basis making sure that the emails pass SPF and DKIM checks. Sometimes someone may make a change to a DNS record that may cause

authentication failures.

GlockApps email authentication test



Feedback Loops

Finally, let's consider feedback loops.

A feedback loop is the mechanism Internet service providers use to report spam complaints (or abuse complaints) to senders. Spam complaints are generated when a subscriber clicks on the "this is spam" button in their email client.

When it happens, the ISP forwards the message back to the email address that has been set up by you or your email service provider with the expectation that the user who complained will be suppressed from your database. A spam complaint should be considered as an indication that the recipient wants to opt-out of that mail stream.

The FBL email arrives very soon after the recipient hits the spam button. Knowing when a subscriber complains about your message is critical, and you have to act on it, immediately. Because sending messages to recipients who have opted-out of those messages by means of complaints is the fastest way to kill your reputation. You can land in the spam folder, or worse, be suspended by your ESP.

For most email marketers, email service providers are handling feedback loop (FBL) emails in the background. However, a high complaint rate can have such a serious impact on your deliverability and reputation, so we feel that it's imperative for you to have a basic understanding of feedback loop services. Knowledge is power.

Marketers who run in-house email systems and manage own SMTP servers have to set up the process of handling FBL email messages for further suppression of these from their mailing list.

How to Start with Feedback Loops

1. Setup a dedicated email address.

As the sender, you need to create a email account dedicated to receive the reports back from the ISP. And you're going to need it when you register for FBLs.

2. Signup for feedback loops with ISP.

Most major ISP provide the feedback loop service. Yahoo, AOL, and Microsoft make it easy to enter. Gmail allows only ESP to enter their FBL program.

The most common information requested during the registration process is the contact information, IP address, and the dedicated email address for receiving FBL reports.

Most FLBs are IP based, but Yahoo! offers a domain-based FBL and requires senders to authenticate with DKIM to enter the feedback loop program. Also, Yahoo! will ask you for the d= and s= values from your DKIM signature. So, be ready to spend a little more time to sign up for the Yahoo!'s FBL service.

You can find the links to FBL signup pages for all ISP that support the service here.

3. Collect data.

Complaint reports from the ISP come typically in the Abuse Reporting Format (ARF) and contain a copy of the email that triggered the spam complaint. You can collect the information contained in these reports including the complainant's email address so you can quickly suppress it.

Some ISPs redact the recipient's email address from the message, which can complicate the identification process. Advanced mailing programs will include tracking links in the email body or subscriber's identifiers in the x-header to help find the complaining user.

Using FBL Email Handling Tool

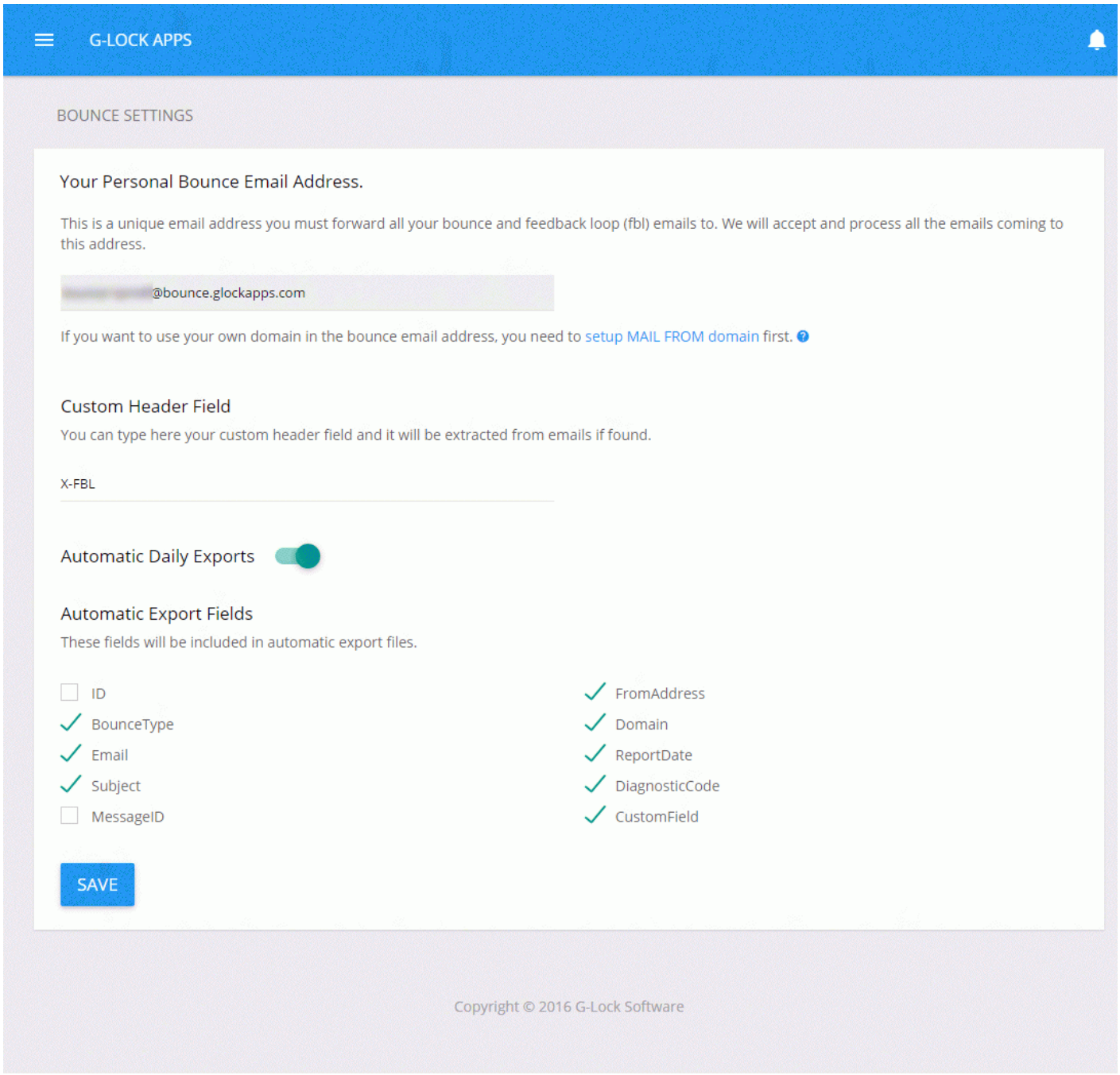
You can manually dig through FBL email reports and extract the complainants' email addresses. It's time-consuming and not always easy, but definitely you can do it.

If you prefer a quick and easy way, technology helps you.

GlockApps offers the ability to centralize your feedback loop and bounce email monitoring in one place.

You only need to setup your mail agent to forward your feedback loop and bounce emails to your personal email address provided to you by GlockApps.

GlockApps Bounced Manager



The tool will accept and process all the emails coming to that address from you.

It will extract the bounce email address and message ID of each email which generated a complaint and, where possible, the email addresses of

the recipients who complained to help you detect and remove problematic and non-existent recipients. It can also extract custom header fields from bounce and complaint emails.

Collected reports will be stored in your account that you can access and download reports at any time. You can also choose to receive the reports via email.

Using GlockApps allows you to:

- save your time for bounce and FBL email processing;

- process bounce and FBL emails timely and accurately according to the latest bounce rules;

- understand which campaigns and at which ISP are generating the highest complaint rates;

- extract custom header fields from bounce and FBL emails for easier user's identification and suppression.

Note: you must subscribe to a GlockApps monthly plan to be able to use an FBL and bounce email handling tool.

The Bottom Line

The reality is that there is no other communication channel that is as pervasive, accessible, efficient, and affordable as email in the modern world. And the role of email communication seems to only grow with time.

Marketers are seeing a great success and ROI with email marketing. According to the "Email Marketing Industry Census 2016" by Econsultancy

and Adestra, 73% percent of companies rate their email marketing campaign performances as "good" or "excellent" in terms of ROI. This is a 66% increase from 2015.

But the value of email is entirely in its ability to reach recipients, i.e. email deliverability.

Email deliverability is a "whimsical lady" and should be on the mind of every marketer. By implementing some of the recommendations in this post, you should be able to better position your email campaigns for success, and see improvements in the delivery of your emails to Inbox and an improved ROI for your email marketing.

About the author:

Julia Gulevich is an email marketing and deliverability expert and customer care service consultant at G-Lock Software with 10+ years of experience. She is the author of numerous articles, newspapers, and ebooks about email marketing, list building and email deliverability.