

Why Read This Guide?

Whether you send transactional or marketing emails, getting to the inbox is critical. If your messages don't reach the inbox, then they can't be read. This is why understanding the science and technology of email deliverability is becoming more important every day.

In this guide, you're going to learn everything that you need to know about email deliverability, such as:

- What's email deliverability in the first place?
- The costs of poor email deliverability.
- 6 things that you can do to maintain high Sender Reputation so your emails reach the inbox.
- The 10 engagement factors that will maximize your deliverability.
- How to setup your email infrastructure for success.
- Top bonus tips to help get your emails to the inbox.
- and more...



Ready? Let's do this.



Contents

3	Chapter 1 Email Deliverability: A Brief Explanation
5	Chapter 2 The Costs of Poor Email Deliverability
7	Chapter 3 Email Sender Reputation Best Practices for Great Deliverability
19	Chapter 4 10 Little Known Engagement Factors to Improve Your Deliverability
22	Chapter 5 The Building Blocks to Good Email Deliverability
31	Chapter 6 (Bonus Tips) How to Get the Best Email Deliverability

CHAPTER 1

Email Deliverability: A Brief Explanation



Recent studies show that 20% of global email never reaches the inbox¹

And we're talking about legitimate marketing and transactional email like:

- Critical password resets from apps and websites
- E-commerce messages such as order receipts and shipping notifications
- Welcome and on-boarding messages
- Marketing and sales messages designed to generate revenue
- And so much more...

Unfortunately, most senders don't realize that they're experiencing an email problem until it's too late. This is because issues quietly accumulate overtime, thus lowering deliverability rates.

So what is email deliverability?

Email deliverability refers to your ability to successfully deliver emails to a recipient's inbox as intended. There are many factors that go into deliverability like Internet Service Providers (ISPs), throttling, bounces, and spam issues — all of which we'll cover soon.

With that said, there's far more to achieving great deliverability (hitting your recipient's inbox) than pressing send. From hidden spam traps to the rise of smarter spam filtering technologies, reaching the inbox is getting more complex. Simply put, email deliverability is both an art and a science — one that SocketLabs has spent over 10 years mastering.

Ready to learn more about the art and science of achieving great email deliverability?

Let's continue with what poor email deliverability may end up costing you.

¹ Source: Return Path's 2017 Deliverability Benchmark Report

CHAPTER 2

The Costs of Poor Email Deliverability



So why care about your email deliverability anyway?
Let's consider the costs of poor deliverability.

In Chapter 1, we shared that 20% of global email never reaches the inbox. With that number in mind, let's run a quick calculation:

Imagine that your email list contains one million subscribers. If an email from a recent mailing fails to reach 20% of your subscribers' mailboxes then 200,000 email subscribers are left out in the cold.

If that doesn't convince you enough, then let's take a look at some of the costs of poor deliverability.

Costs of Poor Deliverability	Benefits of Good Deliverability
Emails don't reach the inbox and won't be open or read.	More emails will reach the inbox to be open and read.
New & existing customers won't hear important news from you.	New & existing customers will receive your latest content and news.
Customers may miss important transactional messages like shipping notifications & password resets.	Customers won't miss important transactional messages like shipping notifications & password resets.
Bad for branding if your emails land in the spam folder.	Your emails will stay out of the spam folder.
Loss of email ROI - email marketing will become less effective for you.	Increase in ROI so email marketing becomes more effective for you.
Competitors with good deliverability are more visible in the inbox.	Gain the competitive advantage over your competition by being visible in the inbox
Your list will become less engaged and responsive to future content.	Increase engagement with your list since recipients will be receiving your content.
Lost opportunities to track key performance metrics like open rates, click-throughs, complaints, and ROI.	Properly track key performance metrics like open rates, click-throughs, complaints, and ROI.

Hopefully by now you're sold on investing some time into achieving good deliverability. In the sections that follow, we'll reveal some best practices to help you maximize your deliverability. Let's start with your Sender Reputation...

CHAPTER 3

Email Sender Reputation Best Practices




Sender reputation is a score that an ISP (i.e, Gmail) assigns to both your IP Address (a unique numerical address that defines an internet location) and Domain (who the email is from, your website) that you use as a sender.

A high sender reputation helps you get good deliverability to the inbox, while a poor sender reputation will cause your mail to be rejected or placed in the recipients' spam folders.

Generally speaking, your sender reputation should be greater than 80. If your sender reputation is less than 80 then you have some work to do.

So how do you maintain a high sender reputation? We'll discuss this in the sections that follow.



Keep Your Sender Reputation and Deliverability High

IMPROVE YOUR DELIVERABILITY NOW



Get Permission and Send Wanted Email

Good email deliverability and your sender reputation are both influenced by many factors. One of the most important things that you can do as a sender is to get permission to email your audiences.

Before you send any email, stop and ask yourself this one question:

“Did I get permission to send email to this person?”

If you did not get permission then do not proceed. Sending cold, unsolicited email will most likely land your message exclusively in the junk folder. This will not only lower your Sender Reputation, but it will also make future emails less likely to be delivered to the inbox.

So how do you get permission?

The answer to that question lies in your data collection practices. For example, many senders use an opt-in form like the example below to build a permission based list. The art and science of building a great email list is to fill it with opt-in subscribers because these people have said “Yes, send me this type of email!”

But be warned! You should never assume that your subscribers want every type of email communication from your company.



Maintain Low Bounce Rates

Bounce rate refers to the percentage of email addresses on your list that were returned by the recipient's mail server. For example, if you send 1,000 emails and 20 messages are returned back (i.e, bounce) then your bounce rate is 2%.

Email bounces come in two forms:

Hard Bounce: A hard bounce is an email message that has been returned to the sender because the recipient's address is invalid. A hard bounce may occur because the domain name doesn't exist, the email is no longer active, or because the recipient is unknown.

Soft Bounce: A soft bounce is an email message that gets to the recipient's mail server but is returned back undelivered before it gets to the intended recipient.

A soft bounce may occur for a few different reasons. For example, when the recipient's mailbox is temporarily full.

As a sender, it's your job to keep your bounce rate as low as possible. This is because a high bounce rate may cause your email to look like spam to a mailbox providers when they see a majority of your mail being returned.



Maintain Low Bounce Rates

There are a number of things that you can do to maintain a low bounce rate (i.e, < 0.1% of your list), such as:

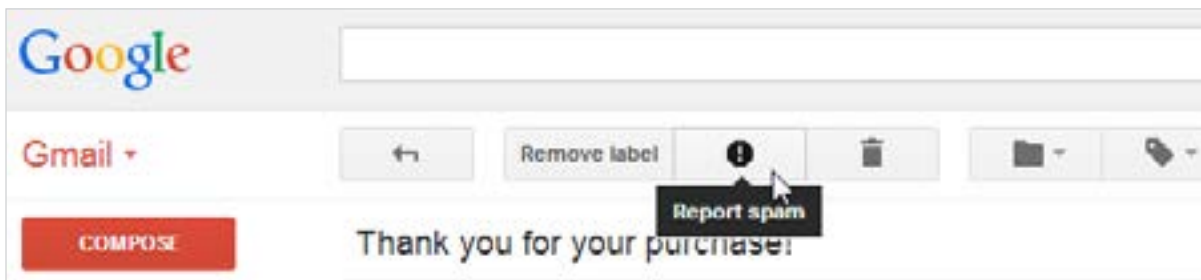
- Regularly cleaning your lists. This means removing hard bounces, complaints, and contacts you haven't engaged with for a number of years.
- Sending mail only to opt-in contacts (here's why you should [think twice](#) before sending to a purchased list).
- Immediately removing any "hard bounces" from your list after each mailing. At SocketLabs, our Suppression List feature automatically does for customers, allowing them to instantly remove bounces from their list.

In addition to your bounce rate, you must keep your complaint rate low. In the next section, we'll reveal the threshold metric that your complaint shouldn't go above.



Complaint Rate (Keep It Low)

A complaint occurs when a recipient marks an email message as spam by clicking the spam or junk button in their email client.



Complaints are major red flags to all mailbox providers that your subscribers are not happy with your mail. As your complaint rate for each mailing increases, your Sender Reputation will drop, thus making it harder to reach recipients in the future.

So what's an acceptable complaint rate?

Try to keep your complaint rate less than .1% of the email that you send. This seems super low right? Well, yes it is, because mailbox providers take complaints very seriously.

If you do get complaints, then you should immediately remove the recipient from your list so you don't email them again in the future.



Format Your Emails (Especially for Mobile)

In addition to bounce rate and complaints, the formatting of your content will also influence how mailbox providers handle your mail, ultimately impacting your sender reputation.

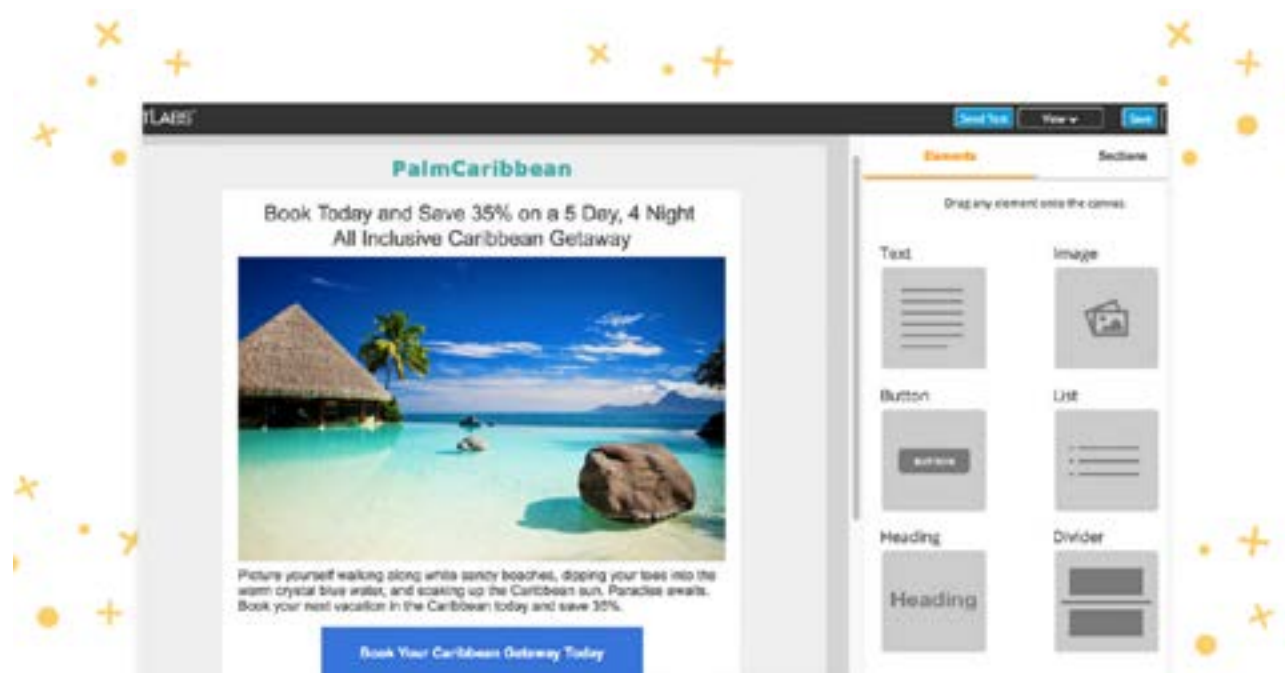
It's more important than ever that you send quality email that your subscribers want to receive because according to Statista ([Daily number of e-mails worldwide 2017 | Statistic](#)) 269,000,000,000 emails were sent and received each day in 2017.

There's no denying that the inbox is a crowded place and the expectations for quality mail are higher than ever.

So before you press send, ensure that:

- HTML is properly formatted. Poorly coded emails get caught in spam filters and won't render properly.
- The unsubscribe link is visible, giving recipients a clear opt-out process so they have an alternative to clicking the spam button.
- Your email is compatible across most major email clients.
- Your content is mobile compatible.

Design Beautiful Mobile Friendly E-mails Using Our Drag & Drop Email Designer



TRY IT FREE

Or continue with the next section



Stay Clear of Spam Traps

Spam traps or “honey pots” are a type of fraud management system, used by blacklist and mailbox providers to identify spammers to block their email. A spam trap looks like a real email address, but it doesn’t belong to a real person.

There are two types of spam traps: “pristine” and “recycled.”

Pristine Spam Trap: These email addresses are typically created by ISPs (like Gmail) and blacklist providers, then published on public websites.

This type of spam trap tells ISPs and blacklists that companies who send to these bad addresses are using poor collection processes, like scraping the web for email addresses or purchasing a list which often include scraped emails.

Recycled Spam Traps: These email addresses were once used by real people, but eventually became abandoned. After an email address has been abandoned for a specific period of time it gets converted into a Recycled Spam Trap by the mailbox provider.

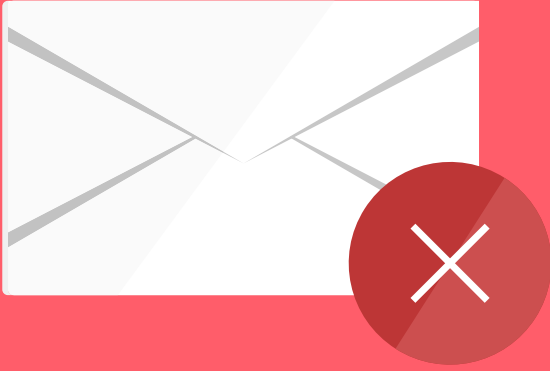
As of 2018, Gmail and Outlook will convert an abandoned email address after 270 days of inactivity. Yahoo! will convert an email into a spam trap at roughly the 180 day mark. And AOL waits for about 90 days of inactivity.



Stay Clear of Spam Traps

After an email address has become a spam trap, it won't hard bounce (i.e, being returned back to the sender with an error) anymore. That's why purchased lists are often riddled with old addresses that have become spam traps.

To avoid spam traps: segment out unengaged recipients, don't use lists that were collected with poor opt-in practices, monitor your list for low quality emails (be sure to look for typos like 'gmall') and immediately suppress bounces that could eventually turn into a spam trap.



Blacklists! (A Dying Breed)

What's a blacklist?

A blacklist is a database that determines if a sender's emails could be considered spam. Some mailbox providers use blacklists to help decide if they should accept or reject an email so they can keep spam out of the inbox.

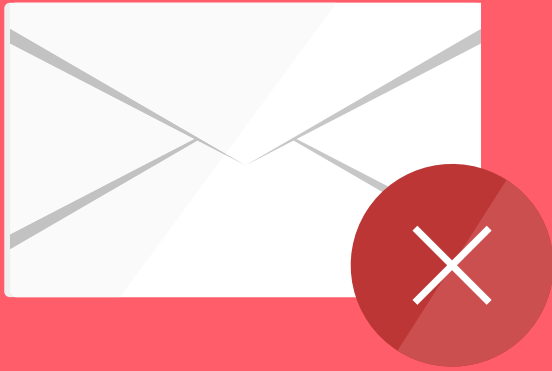
So how do you land on a blacklist?

Landing on a blacklist is usually the result of engaging in spammy email practices, sending to purchased lists, or hitting a spam trap.

And what happens if you land on a blacklist?

Not all blacklists are created equal. But, if you land on a more reputable blacklist (like Spamhaus), then your mail will get blocked by some major ISPs. If this happens, then you'll need to get your IP removed from the blacklist.

The good news however, is that blacklists are quickly dying as email continues to move to the cloud and evolve. For example, Gmail, the leading mailbox provider worldwide, doesn't use any blacklists to filter mail anymore.



Blacklists! (A Dying Breed)

Now this is where you might be wondering,

“Should I even worry about hitting a blacklist?”

The short answer is that you must always send good mail and follow best practices regardless of whether or not blacklists are becoming less effective.

Just because the blacklist is a dying breed, doesn't mean that you should abandon best practices. In fact, following email best practices is more important than ever, as ISPs like Gmail invent more sophisticated ways to deal with abuse.



QUALITY SCORE

Pull Back the Blinders & Improve the Performance of Your Mail

IMPROVE YOUR DELIVERABILITY NOW

CHAPTER 4

10 Little Known Engagement Factors to Improve Your Email



In recent years, sending content that recipients engage with has become critical for successful email deliverability, especially at Gmail. In this chapter, we'll explain what recipient engagement is and the key engagement factors that mailbox providers are looking for.

[hint: successful engagement goes well beyond just opens and clicks]

Understanding Recipient Engagement: Send Relevant & Timely Emails

Do you know how your recipients are interacting with your emails?

As an email sender, you're often limited to gauging the reaction of your recipients to opens and clicks.

However, mailbox providers have a greater array of actions and metrics to use when analyzing and measuring engagement. As a result, recipient engagement has become a big part of email deliverability.

So what exactly are these invisible engagement factors that mailbox providers use to measure engagement?

In a recent article - [Engagement Is More Than Opens & Clicks](#), Brian Godiksen, SocketLabs' expert Email Delivery Manager, reveals insights into what actions are valued by the mailbox providers. These actions, which are listed below - are classified as either positive or negative reactions.

Positive Reactions	Negative Reactions
<p>Messages Read: Mailbox providers know exactly which messages were read and which were not read. Details like how long the message was visible on the screen is what makes this metric even more valuable.</p> <p>Moved to Folders/Organized: Placement of messages into specific folders is a positive action from users, since this action implies the recipient wants to keep the message or expects to receive the message.</p>	<p>Messages Deleted Immediately After Being Read: While reading a message is initially a positive reaction, immediately deleting the message after reading implies that there really wasn't that much interest in the content by the recipient after all.</p> <p>Messages Deleted Without Being Read: This action sends a negative signal to mailbox providers that a recipient is not interested in the message. While not as damaging as marking a message as spam, repeated mailing to an address that does not engage increases the risk of a message being filtered out of the inbox in the future.</p>

Positive Reactions Cont'd

Forwarded a Message: Taking a message and passing its content along to others is a very strong indicator that the message was expected and desired.

Added to Address Book: The first action of most anti-spam systems is to see if the sender is in the recipient's address book. If present, it will likely guarantee inbox placement regardless of how poor other metrics are.

Message Marked as Not Spam: Rescuing a message from the spam folder is easily one of the most important metrics considered by mailbox providers. Marking a message as not spam takes considerable effort on the part of a recipient and reflects as such upon the mailbox providers.

Negative Reactions Cont'd

List Unsubscribes: While mailbox providers are not tracking clicks to content in the body of email messages, they do track clicks to the List-Unsubscribe header that they pull from the message headers and display in a friendly manner to recipients.

Blocking Sender's Address: Offered by a few mailbox providers, a recipient can choose to block further messages from that specific sender address. This is one of the most negative reactions possible from recipients.

Marked Message as Spam: The strongest indicator that a recipient does not want your mail. This will automatically put all subsequent messages from that sender into the particular recipient's spam folder. It increases the likelihood of being automatically filtered in other recipients' mailboxes as well.

At the end of the day, your goal is to make your recipients happy so your reputation doesn't go up in flames.

Let's continue to Chapter 5, the technology that helps you maximize your email deliverability...

CHAPTER 5

The Building Blocks To Good Email Deliverability



Infrastructure and authentication are the building blocks to good email deliverability. If both are setup incorrectly then there's a big chance that you're going to experience email delivery issues.

We don't want that to happen. That's why Chapter 5 is dedicated to infrastructure & authentication.

In this chapter, we'll start by discussing what goes on in the background to help get your emails delivered, this is your email infrastructure.

Then we'll dive into authentication. This is where we'll reveal how to tell mailbox providers that your mail is coming from you and not someone else. Ready? Let's go...



CHAPTER 5: SECTION 1 OF 2

Your Email Infrastructure

Think of your email infrastructure as the foundation to your email deliverability. This foundation consist of your Mail Transfer Agent (MTA), IP Addresses, Bounce Handling, Feedback Loops, and so much more. Without a proper infrastructure in place, you're going to have trouble achieving successful email deliverability.

Since email infrastructure is a huge topic that could be a guide of its own, we're going to keep things simple with a high level overview of some of the most important things that you should be aware of when it comes to your infrastructure.

When To Use a Dedicated IP Address?

With a Dedicated IP Address, you are the only organization sending email over that IP Address. This is the ideal way to control your reputation since you don't have to worry about being affected by other senders.

Dedicated IP's are typically reserved for high volume senders who send over 100k emails per year.

A Dedicated IP is not for everyone, especially senders who are just starting out. If you send less than 100k emails per year then you'll want to start out with a Shared IP Address, which we discuss below.



SocketLabs Offers Dedicated IP Management Starting At Our Pro 100k Plan

When to Use a Shared IP Address?

With a Shared IP Address, your domain sends over the same IP as other senders.

The benefit to a Shared IP is that it allows your organization to reap the benefits of an IP Address with a high reputation. So if the senders who you're sharing an IP Space with are following best practices, then this will work in your favor. Just make sure to use an email service that monitors their senders closely, like [SocketLabs](#).

A Shared IP essentially gives you more wiggle room in terms of sending patterns and volume. This is one of the reasons why small senders start on a Shared IP, then migrate slowly when they are ready to optimize performance.

Manage Complaints Using Feedback Loops

One of the challenges of sending marketing and transactional email is that it can be difficult to see if recipients complain about your mail. This is where feedback loops can help you.

A feedback loop is a service offered by some mailbox providers (not all) that report complaints, like when your recipient clicks on the spam or junk button.

After you know which email addresses logged complaints about your mail, you can (and should) remove the email addresses from your list so you don't contact them again in the future.

Remember, one of the keys to achieving successful delivery is maintaining a low complaint rate. If a recipient marked your message as spam once, they will probably continue to complain about your mail.

“A pattern of spam complaints is one of the strongest signals to mailbox providers that recipients do not want the sender's content.”

- Brian Godiksen, SocketLabs Email Delivery Manager

When choosing an email infrastructure, look for a system that has feedback loops built in, along with an automated system for suppressing the complaints from your list — for example, all SocketLabs accounts come with feedback loops and Suppression Lists to help automate most of the complaint management for you.



Keep in mind that some ISPs like Gmail do not provide access to Feedback Loops

Ensure That Your “From Address” Can Receive Email

It’s also in your best interest to ensure that your Reply-To “From Address” points to an inbox that can receive email. This will allow your recipient to respond to the address that you’re sending from, which is better for engagement.

The deliverability value here is that by replying to your message, your address gets added to your recipient’s contacts. When an address is in a recipient’s contact list, you’re usually guaranteed inbox placement.

Setup Engagement Tracking

Whether you’re sending marketing or transactional email, it helps to obtain data about how your recipients are interacting with your content such as: opening your messages, clicking links, and bouncing.

Engagement data will help you optimize your mail stream to improve your chances of reaching the inbox — for example, by removing recipients who complain about your content.

Manage Hard Bounces

In Chapter 3, we revealed that keeping your bounce rate low is an important component to your sender reputation and achieving good email deliverability.

As a reminder, bounced emails fall into two categories, either a hard or soft bounce.

A hard bounce occurs when the recipient’s address is invalid. While a soft bounce may occur for a number of reasons, such as the recipient’s mailbox being temporarily full.

So how do you even begin to identify emails that bounce back?

Use an email service that has a bounce processing system built in, such as a Suppression List.

An email bounce processing system enables you to determine why your outbound emails are being returned, so you can remove the bounced email addresses from your list, or fix the issue.

For example, a potential recipient may have entered their email address with a “.cno” suffix instead of “.com”. With that information, you would be able to re-enter the email address in the appropriate format and not lose out on this contact.

Detect and Correct Bottlenecks

On March 2, 2018, AOL experienced issues processing email on their side. The emails were accepted immediately from most email providers like SocketLabs, however receiving mailboxes at AOL were delayed due to an issue at AOL.

If you were sending email that day and noticed deliverability issues, then how would you know whether the issues were a result of your infrastructure or the result of an issue at the receiving mail server, like AOL?

This is why having a real-time email monitoring service in your infrastructure is important.

If setup properly, an email monitoring service can track issues, identify bottlenecks, and tell you where the problem is occurring. **At SocketLabs, we call this [360 Monitoring](#).**

When it comes to your infrastructure, you can either build it yourself and hire a dedicated team to manage it, or you can let an [email service provider](#) like SocketLabs take care of this for you.

Now let's discuss the next big piece of the email deliverability puzzle - Email Authentication.



CHAPTER 5: SECTION 2 OF 2

Email Authentication

Email authentication is a way of proving to ISPs that your mail is from you, and not forged by someone else. ISPs like to receive authenticated email because authentication makes it easier to block harmful uses of email, such as phishing and spam.

Why authenticate your mail?

One of the reasons for authenticating your outbound mailstream is that it's a way for you to differentiate yourself from spammers and other bad senders within the inbox.

In the sections below, we'll discuss the three most commonly used email authentication standards: DKIM, SPF, and DMARC.

Sign Your Emails With DKIM

DKIM stands for Domain Keys Identified Mail.

In short, DKIM defends against malicious modification of your email message in transit by ensuring that the message that arrived in your recipient's inbox was not faked or altered in transit.

SPF Record (Sender Policy Framework)

An SPF (Sender Policy Framework) record is an email authentication protocol that allows you to specify which IP addresses are authorized to send email on behalf of your domain.

How does SPF work?

SPF records are published in your Domain Name System (DNS). Follow these [best practices](#) when publishing your SPF record.

When you send email, mailbox providers will perform an SPF Check. During the SPF Check, the mailbox provider verifies the SPF record by looking up the domain name listed in your DNS. Then one of two things will happen:

Pass SPF Authentication

If the IP Address that's sending on your behalf is listed in the SPF record, then the message passes SPF Authentication

OR

Fail SPF Authentication

If the IP Address that's sending on your behalf is not listed in the SPF record, then the message fails SPF Authentication

Why SPF matters?

An SPF-protected domain tends to be less attractive to malicious individuals and therefore less likely to be delivered to the spam folder.

DMARC Authentication

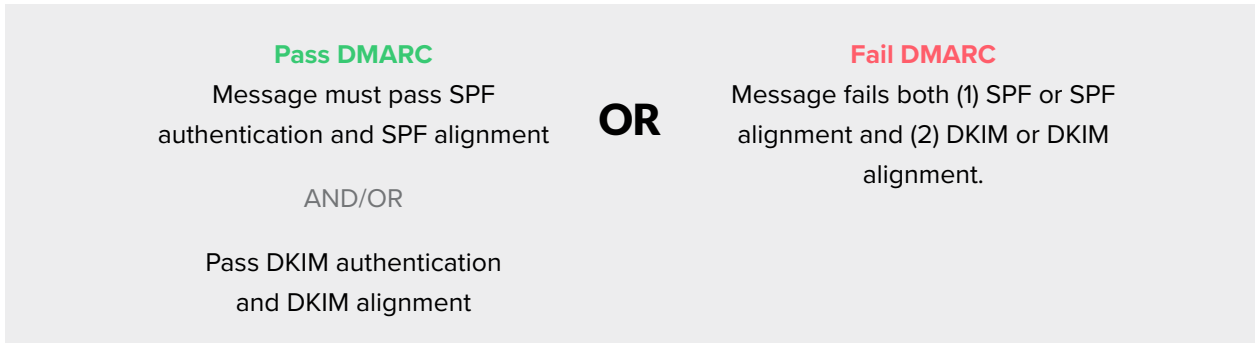
DMARC, which stands for Domain-based Message Authentication, Reporting, & Conformance is the latest advancement in email authentication and it's on pace to become the most widely deployed authentication technology.

What's the purpose of DMARC?

DMARC unifies SPF and DKIM authentication into a common framework by ensuring that legitimate email is properly authenticated against SPF and DKIM standards. This means that if mail coming from your organization's domain is found to be fraudulent, then the messages are blocked.

How does DMARC Work?

A message can either pass or fail DMARC.



DMARC gives senders the ability to instruct mailbox providers on how to handle unauthenticated mail via a DMARC policy. Senders can choose from one of the three types of DMARC policies:

1. **p=none:** If you set your DMARC policy to p=none, then the mailbox provider won't take any action if the emails fail DMARC.
2. **p=quarantine:** Setting your policy to p=quarantine means that emails that fail DMARC are treated suspiciously by mailbox providers. As a result, the email gets delivered to an area outside of the inbox, such as the spam or junk folder.
3. **p=reject:** This policy indicates you want mailbox providers to reject and block all emails that fail DMARC.

When it comes to choosing a DMARC policy, you should tailor your policy to your organization. For example, p=reject policy tends to be more suited for organizations that deal with sensitive information, such as financial institutions.

Whew, that was a lot to take in!

But don't worry, we aren't expecting you to become an email deliverability expert overnight. That's why services like SocketLabs exist. We give you the ability to send your important transactional and marketing email from one platform, without having to build and manage everything yourself.

Now let's move on to the fun stuff... although we think it's all fun :)

CHAPTER 6

(Bonus Tips) How To Get The Best Email Deliverability



In the chapters above, we gave you a high level overview of what it takes to achieve successful email delivery.

In this chapter, we're going to cover some of our favorite best practice tips. Ready? Let's go!

1

Build an Opt-in List (Don't send to a Purchased or Scraped List)

It can be tempting to take a shortcut by sending to a purchased, rented or scraped list. But, doing so can be a costly mistake.

Why?

The first reason why you should not send to a purchased, rented, or scraped list is because the contacts on your list never gave you permission to email them in the first place. As a result, your email will likely get poor engagement and high complaints, which may cause your message to get filtered to the spam folder.

Another reason is because it's easier to hit a spam trap which will negatively impact your ability to reach the inbox in the future.

What should you do instead?

Build an opt-in, permission-based list.

2

Understand That Nothing Lasts Forever (Not Even Consent)

Just because a subscriber gave you consent five years ago, doesn't mean that you should send the subscriber your latest promotion, especially if this person hasn't recently engaged with your content.

Consider this example:

A mortgage company that sends home buying tips through email to potential home buyers may have a shorter time of consent than a dog grooming business that sends a weekly grooming email newsletter to dog parents.

In other-words, the home buyer list will churn faster than the dog groomer's list of dog parents. This is because people tend to buy homes in less than one year, while Fido is living longer and longer these days :)

Our challenge to you is to think about how long consent in your industry lasts. And if your subscribers haven't engaged with you in awhile, then follow the next tip.

3

Engage Your Unengaged Subscribers

Throughout this guide we discussed the importance of engagement (Chapter 4) and why it's becoming more important than ever to send to an engaged list.

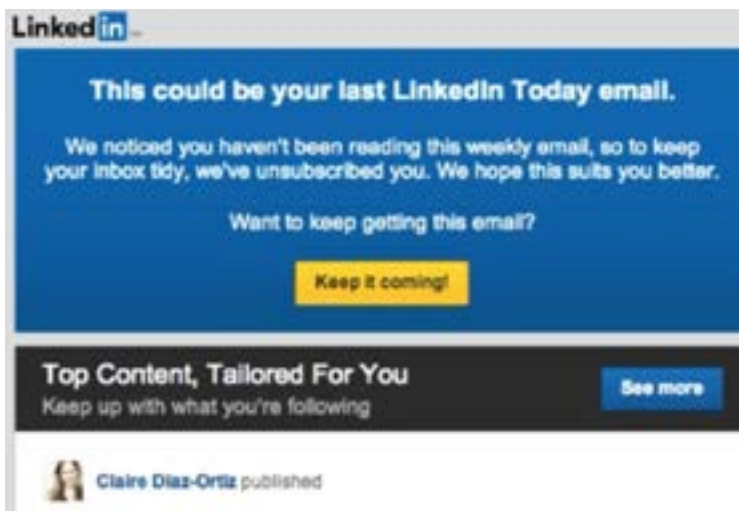
So what should you do when some of your subscribers go silent?

Well, before you completely stop emailing them, it's a good idea to give your unengaged subscribers one last chance to indicate that they are still interested in receiving content from you. And you can do this by sending a re-engagement email.

Here's a great example of a re-engagement email from LinkedIn.

In this email, LinkedIn politely tells the unengaged subscribers that they have been unsubscribed due to a lack of responsiveness.

LinkedIn also gives subscribers a way to opt back in.



4

Clean Your Lists to Avoid Spam Traps, Complaints and Hard Bounces

Throughout this guide, we discussed how spam traps and bounces can damage your sender reputation, ultimately impacting your ability to successfully reach the inbox.

With that in mind, you should have a routine process in place for cleaning your lists. Setting some time aside to clean your lists will help you avoid potential issues down the road, such as hitting a Recycled Spam Trap.

You'll also want to get into the habit of immediately removing complaints and hard bounces from your lists.

A complaint can be extremely damaging to your sender reputation, while a high number of hard bounces is a red flag to ISPs that you're engaging in spammy email practices.

5

Segment Your Lists for More Relevant Mailings

Email segmentation helps increase engagement and relevance of your campaigns.

What's relevance?

In email, relevance is the measure of how closely related your content is to the wants and needs of the subscriber.

For example, an abandoned shopping cart email is relevant to a subscriber who abandoned your checkout process within the last seven days. However, this same email is less relevant to subscribers who did not start the checkout process.

6

Create Emails That Are Readable on Mobile Devices

There is no denying that people are consuming more content on mobile devices.

According to Litmus, 47% of emails are now opened on a mobile devices:

“More email is read on mobile than on desktop email clients. For example, recent stats say 47% of email is now opened on a mobile device.”

– Litmus “The 2017 Email Client Market Share” (Jan 2018)

With that in mind, you should verify that your content is legible and optimized for email, before you press send.

Failure to provide your subscribers with a great mobile experience may negatively impact your engagement rates for your campaigns.

If you’re a SocketLabs user, then you can use our Email Designer to create mobile optimized experiences without any additional work.

7

Send a Welcome Message to New Subscribers

When someone subscribes to your list, it's a good idea to send a welcome message to kick-off the relationship.

Here's a great example from Litmus, a popular tool that helps you build, send, test, and analyze emails.



Notice how Litmus leads in with a fun, catchy headline.

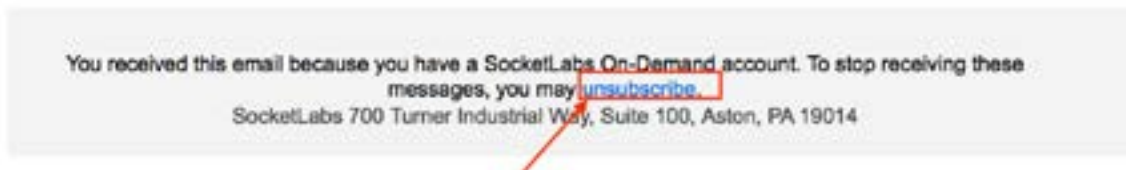
Litmus also starts the relationship by providing value through a responsive email design guide.

Your welcome message will help set the tone for the type of mail your subscribers should expect to receive from you. This is when you can explain what type of email they'll be receiving, how frequently they will receive email, a reminder about why they signed up for your list, and information about how to unsubscribe from your list.

8

Make it Easy to Unsubscribe

Don't be afraid of unsubscribes!



Some senders make the mistake of trying to hide or bury the unsubscribe link. In theory, this sounds like a great way to prevent someone from opting-out of future emails, but hiding the unsubscribe link may come back to bite you.

This is because a recipient's alternative to the unsubscribe link is the report spam button.

The truth is that if someone doesn't want to hear from you, they'll use the next best option to get off your list, which is clicking the spam or junk button. A spam complaint can hurt your sender reputation, ultimately impacting your entire campaign.

As a sender, the last thing that you want to do is damage your entire campaign as a result of a high complaint rate. Therefore, you should always include the unsubscribe link and make it easy to find.

9

Know the Difference Between Transactional and Marketing Email

Many customers at SocketLabs send both transactional and marketing email.

Transactional email tends to be mail that people want to receive and are looking for: password resets, shipping notifications, order receipts, and other types of time-sensitive mail.

Marketing email tends to be less desirable than transactional mail. This type of mail includes: newsletters, promotional offers (even if they are time-sensitive), lead nurturing emails, sales emails, and other content that drives a business goal.

In most cases, it makes sense to separate your transactional mail from your marketing email into different mail streams, so your time-critical transactional mailings are not impacted by the performance of your marketing email.

10

Follow the Law

It goes without saying that following the law is always a good idea. Staying compliant with the law helps you avoid tarnishing the reputation of your business while staying clear of hefty fines. Here are a few things to keep in mind:

- Ensure you have permission to email the subscribers on your list
- Don't use misleading header information
- Include your physical mailing address in the email
- Include a way to opt-out of receiving future emails
- Honor opt-out requests promptly - CAN-SPAM laws stipulate that you must honor a recipient's opt-out request within 10 business days
- You're responsible even if you're not sending campaigns yourself (i.e, outsourcing)

Keep in mind that email laws are looser for transactional emails like order receipts, shipping confirmations, password reset emails, etc.

Most of the above can be attributed to the CAN-SPAM laws. In addition, you should also familiarize yourself with [GDPR](#), which went into effect on May 25, 2018.



Get Started With SocketLabs

Phew! We put A TON of work into this guide. So we hope you enjoyed it. As you can see, reaching the inbox is no easy task. That's why email delivery platforms like SocketLabs exist.

SocketLabs helps you send your transactional and marketing email without having to manage your own email infrastructure. Our core features include:

- Industry leading deliverability
- SMTP servers for transactional and marketing email
- Email APIs that allow developers to embed email functionality into any app or website
- A suite of powerful, yet simple email marketing tools
- Rich reports and analytics
- And so much more!

The best part? You can get started with SocketLabs Right NOW.



[CLICK HERE TO CREATE AN ACCOUNT TODAY!](#)

