

AudiencePoint 

EMAIL

DELIVERABILITY



“WHAT DO YOU MEAN, MY EMAILS AREN'T GETTING DELIVERED?”

This phrase, heard in conference rooms around the country can be the last thing heard before jobs are lost. The job loss isn't personal, but so much money is driven by email, that a sending domain that is landing in the spam folder is grounds for termination, why? Because email in the Spam folder is not converting into revenue. It often isn't the email marketer's fault. The email marketer is often overruled by someone higher up in the company who says to “send more email, to more people, I don't care what the technicalities of email are.”

This guide provides “how to know if your email is landing in the Spam folder”, “how it got there”, and “how to recover”. It is meant as a guide only, it is not meant to be comprehensive. If your deliverability problems have been chronic (ongoing and unrecoverable), please consider engaging a deliverability consultant.



HOW TO KNOW



How to know your emails are being delivered

Often the email marketer is not even aware that their email is landing in the spam folder. Inbox placement requires a little bit of detective work to figure it out. Marketers have to put their Nancy Drew hat on and start sleuthing.

The tools tell you so

Google and Microsoft both have postmaster tools. AudiencePoint has an inbox monitoring tool. There are others. These tools do the heavy lifting.

Apple Mobile Privacy Protection (MPP)

You have less than a 100% open rate on AppleMPP-based inboxes.

Your engagement rates drop suddenly or slowly

Monitor your engagement rates, when you see a collapse in your opens or your clicks, something happens that requires your attention.

Monitor revenue

Unexplainable drops in revenue.



User Reporting

Seed your file with known email addresses. It is common for friendly users to notice that email is landing in the spam folder, instead of the inbox especially if you have friendly email addresses helping watch that line with you.



WHY THOUGH?



What are the causes?

Often, there is more than one reason that could cause your email to land in the Spam folder. But just because one of the reasons is true about your program, correcting it may not resolve the Deliverability issue.

Poor domain reputation

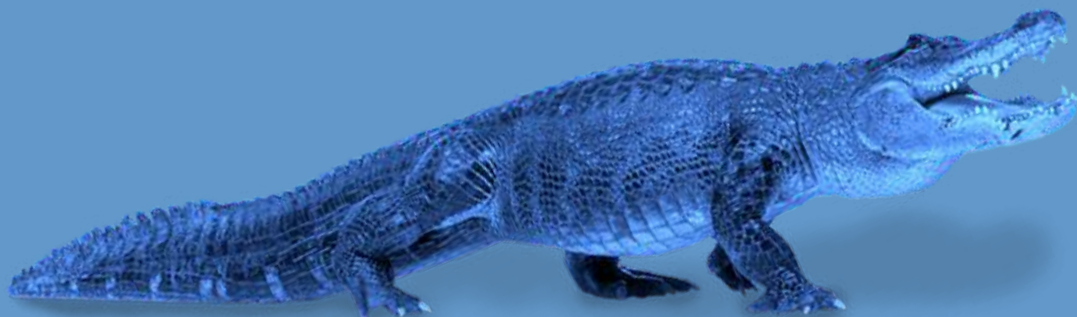
If your domain reputation is bad, your email will not be delivered. Our domain is audiencepoint.com, and if we were sending questionable emails from our domain, then our domain reputation would go down. There is both good and bad reputation and a good reputation will take longer to build than a bad one. Every domain is hosted on an IP address. IP Addresses are the language of the internet. Every IP address has a reputation as well which can impact deliverability. AND domain and IP reputation affect each other. IP reputation gets you in the door with the mailbox provider, and then your domain reputation takes over.

Snowshoe spamming

One of the early solutions to Yahoo and Google restrictions was to create a bunch of sibling domains that would diversify the risk of impacting your sending domain. This is called snowshoe spamming. While snowshoe spamming may get you some advantage in the short run, you are potentially leveraging your future deliverability for potential visibility today. Domains that act like snowshoers are treated like snowshoers and land in the spam folder.

Sending to Spam Traps or Honey Pots

Email addresses that are abandoned for a while or never related to a real person, could be honey pots or spam traps. They are created as a trap for the aggressive email marketer willing to bend some rules to grow their list by any means necessary. Having one of these problem emails in your files is a clear indication to the mailbox provider that you aren't responding to the inactivity signals.



WHY THOUGH?



What are the causes? - continued

Authentication

Many well-intentioned email marketers don't even know what authentication is. This is the process of establishing key records that exist both on your DNS record (the one that tells email where to go) and on your sending email platform. It is a public record that tells the world that you are who you say you are. The three leading authentication tools are SPF, DKIM, and DMARC. BIMI (Brand Indicators for Message Identification) takes authentication one step further and as a carrot, assigns your email address to the logo of the sending domain.

Email Marketing or Bulk Mail

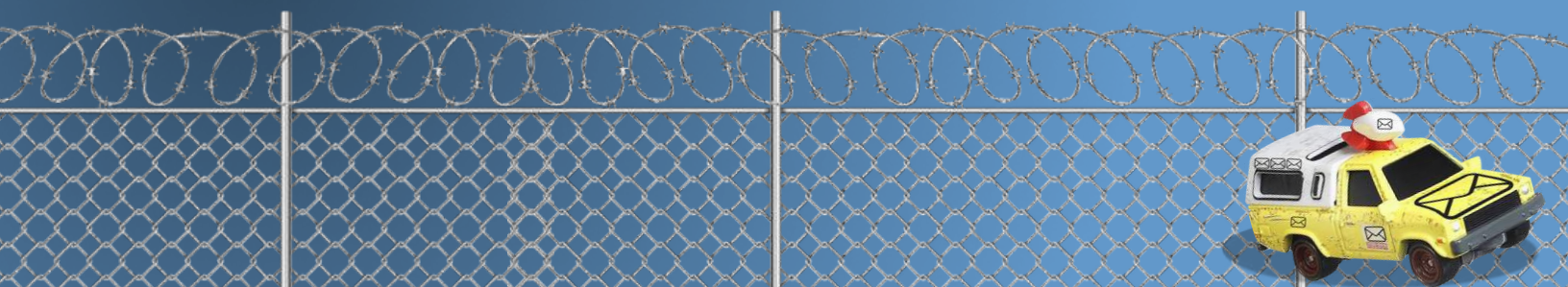
Prior to this paragraph, the causes of landing in the spam folder are pretty universal to anyone sending email. Bulk email, or email marketing, has its own set of rules. If you are sending mass email, you should only be sending confirmed opt-in, solicited bulk mail. The best practice goes deeper than that marketers should also be honoring an inactive policy such that they stop emailing someone when their email has not been opened or clicked in a period of time (60, 90, or 180 days). That inactivity policy should vary by the sender and should be personalized to the needs and goals of a sending brand.

Role Accounts and Feedback Loops

Role-based email addresses typically don't opt-in to receive emails and generally have high spam complaint rates. They are more likely to bounce, and negatively impact your sender reputation and deliverability. If your feedback loop accounts are not set up, you are missing out on key information on how your email is being treated. Not every mailbox provider provides a feedback loop, but those that do provide fantastic information back to the emailer so that they can proactively prevent domain reputation impact.

Clean hosting

If you are hosting your email through a service like Google or Microsoft, your IP reputation is probably very good. However, if you are hosting any email on a shared IP address, then you could be running into problems that are not of your own doing. Shared IP addresses are very common with cheap and cheerful email service providers that promise a simple user experience and an inexpensive price tag. Beware, the low cost of those ESPs often is a byproduct of shared IP for your marketing email.



WHY THOUGH?



What are the causes? - continued

Improperly warmed IP addresses

When you first start sending email from a given domain/IP address combination, you need to teach the mailbox providers that you are safe. There is a way to warm IP addresses that the mailbox providers like. You follow the recommended warming patterns limiting the number of emails that you send to each mailbox provider until your IP addresses are fully warmed and the mailbox providers are receiving the expected amount of traffic from you on a patterned basis.

Substantially increasing or decreasing your send volume

The key to email marketing is to be predictable. The mailbox providers want to get to know you and want to predict your habits. So for example, if you are sending out 100K emails a day for the entirety of the month, and then all of a sudden decide to send 3 million emails all at once, the mailbox provider might consider you to be untrustworthy and stop delivering your email to the inbox.

High reported spam rates or poor engagement.

Recently Yahoo and Google published a standard such that when a sending brand goes above a certain reported spam-rate, the email will start going into the spam folder. At AudiencePoint, we have observed that poor engagement on your email is also a death sentence for missing the inbox.

High bounce rates

There is a tolerance for email bounces, but that tolerance is not very high. Often your email service provider monitors your bounce rate, but AudiencePoint does have customers who pay for our Bounce Stream feed. That feed surfaces all email addresses that have bounced daily.





How do you fix it?

Well, email landing in the spam folder is not good. It is also not an email death sentence. Some deliverability issues resolve themselves, but some require much more attention. Poor email deliverability happens to a lot of good email marketers, so if you find yourself to be one of those people while you read this, relax, it is going to be OK.

Lock down your sends.

You are going to have to pare down your list. If you keep sending to the full file, you are going to make things worse. This is not a long-term plan, it is a “stop the bleeding” plan.

Identify the root causes of why your email is landing in the spam folder

Correct it. The root cause(s) can often be a bit of conjecture. The recipe for repair then becomes the following:

- 1 part addressing the perceived issues
- 100 parts focusing on best practices.

Are you blacklisted?

Check to see if your domain was added to a spam [blacklisting](#) service.

Confirm that your SPF, DKIM, and Dmarc records are set up correctly.

Some [tools](#) will help confirm that your records are set correctly. Also, BIMI lets you associate your logo in inboxes with your sending brand’s email. For BIMI to work, you have to have your SPF, DKIM, and DMARC records set up correctly.

Set up deliverability monitoring services

ListFit with [Inbox Monitoring](#) can tell you exactly which emails are landing in the inbox and which ones are not. Email the ones that are landing in the inbox and remove the ones that are not. Once you have stopped the “spam folder” bleeding, then we can talk about which emails you should add back to your list.

Set up Seed lists

Albeit antiquated and much less effective, consider a seed-list monitoring tool. They measure overall sender-reputation which is still a factor of deliverability services.





How do you fix it? - continued

Set up your feedback loops and reputation monitoring ([1](#) [2](#))

Make checking these [services](#) part of your daily routine

Consider getting dedicated IP addresses for your email.

Identify all outgoing mail from your domain and what IP addresses are being used. Consider creating a subdomain with a dedicated IP per subdomain. The impact of dedicated IP addresses will vary based on your list size and industry. IP reputation gets your foot in the door with the mailbox providers, once you are established your engagement stream takes over.

Use ListFit to identify and purge your list of lapsed email addresses.

[ListFit](#) tells you which emails are not engaging with your brand, or with anyone else. This will likely catch your spam trap

Institute an inactivity policy

Start aggressively filtering, remove emails that have not engaged in 45 days, By gradually increasing the length of your inactivity policy, you can identify and purge those spam traps.

Rewarm your domain

[Rewarm](#) your IPs (reduce your send volume, and follow the same warming schedule that you do when you first start sending.) Monitor your inboxes for non-delivered emails, back off when you see negative signals.

Maximize your engagement with optimization services

Can you get more juice out of the lemon? Services like Subject Line Optimization and [AudiencePoint's Send Time Optimization](#) increase engagement. This has multiple benefits, you have higher engagement rates and smaller chunks of sends. Both have a positive impact on your deliverability.





How do you fix it? - continued

SCRUB all new emails new to your file
with a service like the AudiencePoint [email verification tool](#)

Join an online community
[EmailGeeks](#) is open 24/7 and has experts in every aspect of email that can help answer more of your technical questions.

Evangelize email best practices internally
Rarely is it the person put in charge of cleaning up the mess that is the cause of the mess. Educate those around you about the problems with poor email practices. Emails that aren't delivered aren't seen and that impacts revenue!

Let the mailbox providers know what happened
Send a report to [Gmail](#) indicating what happened and what you have done to resolve it.

Consider bringing in a deliverability professional.
Some problems need to be negotiated with services like Spamhaus, or the mailbox providers themselves. The deliverability professionals have relationships with the mailbox providers and can help broker a return to good standing. Contact sales@audiencepoint.com and we can direct you to our network of deliverability professionals.



CONCLUSION



Conclusion

Timing matters, this was the catchphrase of AudiencePoint when we first started the company. The spirit is true here as well. The longer that you engage in bad practices, the longer and harder it will be to recover from those practices.

Email is a growth market. It continues to deliver on revenue year over year. Because it is so effective big brands are taking notice, and we are starting to see more and more regulations on the industry. Email deliverability is complicated, but is all based on behaving like a responsible citizen.

Do your best to be the brand that you think the mailbox providers are looking for. Follow best practices. With that said, if you follow best practices, the loyalty of your email subscribers will continue to produce revenue for you.





Links from the e-book

<https://audiencepoint.com>

There are a lot of links to our site, which we believe can help provide a lot of the answers resolving deliverability issues.

<https://aboutmy.email/>

Provides a service where you send it an email and the service alerts you to poorly setup email domains.

<https://mxtoolbox.com/blacklists.aspx>

Check to see if your domain has been added to the blacklists of Spam.

<https://glockapps.com/isp-feedback-loops/>

A list of feedback loops and how to sign up for them.

<https://www.gmail.com/postmaster/>

Google postmaster tools, a reputation monitoring tool for Gmail.

<https://sendersupport.olc.protection.outlook.com/pm/>

Outlook postmaster tools for monitoring your reputation with Micorosoft properties.

<https://email.geeks.chat/>

A fantastic online community of email experts from around the world read to help answer questions.

https://support.google.com/mail/contact/gmail_bulk_sender_escalation

Google mechanism for emailers to interact with the gmail team