

Email Reputation Metrics Troubleshooter

Email Reputation Metrics Troubleshooter

Written By Dale Langley



Dale has been working with clients to improve their email deliverability and response rates, along with leading the development of email marketing systems serving blue-chip clients in Europe for over 7 years.

As a developer Dale has extensive practical knowledge of how companies design systems and store data. As a consultant Dale understands how to implement robust architecture, analyse data, segment, design and deliver for the best possible results.

This combination of experience means that Dale understands how to resolve the problems faced by marketers tasked with growing their subscriber lists and maximising ROI.

Who Should Read This?



Beginner

Beginner content is intended for marketers just starting out or for those who just need a refresher.



Intermediate

Intermediate content is intended for marketers with some experience in the subject matter including strategies and tactics.



Advanced

Advanced content is for marketers who have an advanced level of understanding of email marketing and are looking for advanced strategies and tactics.

This e-book:



Return Path Products

Certification

Join the exclusive list of the most reputable senders in the industry.

Inbox Monitor

The most comprehensive tool for deliverability.

Reputation Monitor

83% of email delivery failures are caused by reputation problems.

Email Client Monitor

Know how to reach your audience.

Inbox Preview

Find broken email creative before it gets to your subscribers.

Inbox Insight

Maximize engagement with actionable competitive intelligence.

Labs

Innovative new solutions to help you optimize the performance of your email marketing efforts.

Professional Services

Let us take your email program to the next level.



Contents:

A rise in subscriber complaints	Page 5
Spam traps on file	Page 6
Deferral rates at specific mailbox providers	Page 7
High number of “unknown user” hard bounces (> 10%)	Page 8
Reverse DNS is suddenly failing	Page 9
IP addresses are appearing on blacklists	Page 10
An increase in rejected emails	Page 11
DKIM authentication is failing	Page 12
Rise in messages being filtered to the spam folder	Page 13



What's Happening?



A rise in subscriber complaints

Possible Cause

- Weak Permission
- Change in frequency
- Compromised email server
- Bad list acquisition source

Next Steps...

1. Sign up or verify you are signed up for all ISP feedback loops (FBLs) which include: Yahoo!, Microsoft/Outlook.com (called JMR), AOL, Comcast, Cox, BlueTie, United Online/Netzero/Juno (UOL), Rackspace (Mailtrust), Road Runner, OpenSRS(Tucows), and USA.net.
2. These complaint counts can be used over time to identify potential problems with your mailing practices. Rapid changes in complaint numbers that do not match your mailing volumes, or escalations over time are both indicators of a complaint problem that may impact your deliverability and should be addressed.
3. Use a List-Unsubscribe header to help facilitate unsubscribe requests from those mailbox providers that use the list-unsubscribe header. For example, while Gmail does not offer a feedback loop, they will ask your subscribers if they would like to unsubscribe when they report your email as spam – but only if you have a list-unsubscribe header present. Read more on [Gmail and the list-unsubscribe header](#).
4. Track list acquisition sources that generate the most complaints, and implement ways to reduce complaints or remove these sources altogether. Common list acquisition sources include paid acquisition, affiliates, and peer-initiated web forms.
5. Audit your SMTP servers for open relays to prevent other parties from exploiting them and deploying email through them that is not yours.



What's Happening?



Spam traps on file

Possible Cause

- High inactives on file
- Lack of, or ineffective, inactive email strategy
- Emailing entire list too infrequently
- Poor list acquisition practices

Next Steps...

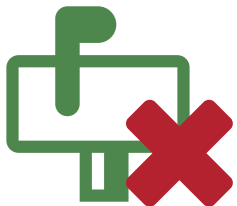
Check your points of acquisition to make sure that you're verifying the email address that's being submitted. Consider asking subscribers to input their email address twice to prevent "fat finger" mistakes. Also think about checking the domain of the email address in real-time using validation scripts or services.

Once data enters your list, make sure you send a welcome or confirmation email and remove any bounces immediately. Ensure your welcome email allows recipients to unsubscribe, just in-case the incorrect email address was entered at the point of acquisition.

Lastly, ensure that you are performing good list hygiene practices and are removing both bounces and inactive addresses.



What's Happening?



Deferral rates at specific mailbox providers

Possible Cause

- IP address has little to no sending history
- Incorrect connection / throughput settings
- ISP employs greylisting techniques
- Exceeded acceptable unknown user or complaint rate

Next Steps...

Refer to the specific code located within your bounce logs. This information can tell you specifically what your issue is and how to address it. If you're sending from a new IP address, it's a requirement to warm up an IP address by sending small volumes and slowly increase volume while keeping complaints and unknown users at a minimum.

If deferrals are due to complaints, see the Complaints section. If referrals are due to high unknown users, see the Unknown User section.



What's Happening?



High number of “unknown user” hard bounces (> 10%)

Possible Cause

- Sending to an old or bad list
- Sending to an opt-out email list
- Mailbox Provider is deactivating old, inactive email addresses

Next Steps...

An unknown user error code is generated when a sender deploys an email to an email address that no longer exists. This could be because the email address never existed, is no longer active by choice, or was abandoned by the end user.

When mailbox providers see a high unknown user rate from an IP address, they may suspect a “dictionary attack” is occurring or that the sender does not have solid data hygiene practices. A dictionary attack is when a spammer uses combinations of words in the dictionary to create random combinations of emails addresses and then deploys spam to those addresses for the purpose of finding valid email addresses. These addresses are then collected, sold and sent more spam. To prevent more unknown users, you should:

1. Verify that your bounce processing system is handling and removing unknown user bouncebacks immediately.
2. Mail to all of your email users no less than once a quarter.
3. Mail a sample of old or opt-out lists before mailing to them to measure the level of risk.



What's Happening?



Reverse DNS is suddenly failing

Possible Cause

- DNS server is down
- Network connectivity issues
- An incorrect change to your DNS record was made

Next Steps...

1. Validate that your DNS is reachable through the Return Path tools, MX Toolbox, or DNS Stuff.
2. Contact your network engineer to verify that no changes to your DNS were made and to verify that your DNS host isn't experiencing connectivity issues.

What's Happening?



IP Addresses are appearing on blacklists

Possible Cause

- Spam traps were acquired on your email list
- Not processing complaints or bounces

Next Steps...

A blacklist is a list of IP addresses that mailbox providers, spam filtering companies, or anti-spam organizations create and maintain to assist with the filtering or blocking of spam. The blacklist owner will publish the list and allow other organizations to use it to help them filter or block email. To ensure the deliverability of email, it is important to stay off of widely used blacklists such as Spamhaus, SpamCop, CBL, and the Return Path blacklist.

An IP address may be listed on a blacklist when deployed email hits a spam trap (refer to spam trap section) or generates end user complaints (refer to complaints section). If a blacklist owner sees frequent spam trap hits and/or complaints the owner may place that IP address on their blacklist.

With some blacklists, inclusion is based on infrastructure failures such as an open relay. To avoid placement on these blacklists, make sure your deployment infrastructure is following industry best practices and standards.



What's Happening?



An increase in rejected emails

Possible Cause

- A mailbox provider blacklisted your sending IP address(es)
- Your IP address(es) appeared on a blacklist
- You are experiencing reputation issues with complaints, spam traps and/or unknown users

Next Steps...

A sudden drop in inbox placement usually indicates a change in your sending practices, so think about what's changed in your company recently.

Have you switched hosting providers for your website or corporate domains? If so, are all the DNS entries for your email authentication present and correct?

Have you rolled out a new template design as part of a rebranding exercise or a refresh of content? If you're going to go through this process you should test new templates to ensure that your response rates don't drop. If subscribers no longer recognize the branding or language used in your emails they're unlikely to engage with your content, and that means bad news for inbox placement.

Have you introduced a new set of data into your list recently, maybe as part of an acquisition or an attempt to win-back old subscribers? The quality of this data is going to affect your ability to get to the inbox across your entire list so factors such as data hygiene and subscriber engagement should be at the front of your mind when going through this process.

Once you've identified the change that contributed to a drop in inbox placement, you can put a plan in place to address it.



What's Happening?



DKIM authentication is failing

Possible Cause

- Check key length
- Invalid / Missing Public Key

Next Steps...

Although 512 bit keys have been used for a while, they're no longer recommended due to the ease with which they can be hacked. Late in 2012, Gmail started failing emails signed with less than a 1024-bit keys as invalid.

It's also possible that you have a problem with what's known as the Public key. This is a DNS record that is "paired" with the hash included in the outbound email to validate your email streams. Part of the Public key is a string of random characters, if you have copied this from a DKIM record generator into your DNS, it is possible that there may be some invalid characters in the record. Depending on your DNS host, you may also find that certain escape characters are needed when adding the record, check with your provider if you are unsure how to update your record. Finally, if you want to test your records you can send an email from your DKIM signed domain to checkmyauth@auth.returnpath.net and you'll receive a report detailing any problems.



What's Happening?



Rise in messages being filtered to the spam folder

Possible Cause

- An increase in complaints, spam traps or unknown users
- Lack of win-back program
- Missing Feedback Loops
- Spam keywords or email message structure are failing spam filter checks

Next Steps...

Having a drop in subscriber engagement can really affect your ability to get to the inbox. Therefore, It is important to try to re-engage these subscribers before it becomes a problem. You should define what an inactive subscriber looks like as the definition varies from business to business and only by understanding your customer lifecycle can you truly define inactivity.

Once you know this definition, try to work on what will re-engage your inactives. Maybe it's an added benefit or special offer, or it could be more relevant content or information they can't get anywhere else. You should also know when to let go. If someone has truly become disengaged, sending them more and more email is not going to win them back, and it's likely to make them reach for the "spam" button which could be much worse than just letting them go.

If someone is marking your email as spam or junk, then it's important to make sure you're no longer sending them email. Not only will your email get filtered to the junk folder but your deliverability as a whole starts to head south. So, make sure that you're enrolled on all the available feedback loops and mailbox providers will send you notifications of complaints so that you can remove the subscribers from your list. There are some requirements for acceptance into Feedback Loops (FBLs) which involve meeting best-practices such as SPF, DKIM and IP reputation but the requirements are easily met by most marketers.

Canada
rpinfo-canada@returnpath.com

United Kingdom
rpinfo-uk@returnpath.com

Germany
rpinfo-germany@returnpath.com

France
rpinfo-france@returnpath.com

USA (Corporate Headquarters)
rpinfo@returnpath.com

Brazil
rpinfo-brazil@returnpath.com

Australia
rpinfo-australia@returnpath.com

About Return Path

Return Path is the worldwide leader in email intelligence. We analyze more data about email than anyone else in the world and use that data to power products that ensure that only emails people want and expect reach the inbox. Our industry-leading email intelligence solutions utilize the world's most comprehensive set of data to maximize the performance and accountability of email, build trust across the entire email ecosystem and protect users from spam and other abuse. We help businesses build better relationships with their customers and improve their email ROI; and we help ISPs and other mailbox providers enhance network performance and drive customer retention. Information about Return Path can be found at: returnpath.com



