Email deliverability update: Why e-mail deliverability is getting harder

Received: 3rd September, 2024

Guy Hanson

GUY HANSON

Vice President, Customer Engagement (International) at Validity Inc.

Guy is a passionate advocate for intelligent use of customer data to drive responsive sales and marketing programs. Guy has had a long-term involvement with the Data and Marketing Association (DMA), previously sitting as Chair of the email council and leading the production of the council's research.

Email: guy.hanson@validity.com | www.linkedin.com/in/guyhanson/

DOI: 10.69554/QKGL3189

SETTING THE SCENE

Back in October 2023 Yahoo and Gmail jointly announced new requirements[1] for all bulk e-mail senders. Many readers would already be very familiar with these by now, but for completeness, here are the key elements; the new ABC of e-mail marketing:

- Authentication: E-mail senders must implement stronger email authentication standards, including Sender Policy Framework (SPF),[2] Domain Keys Identified Mail (DKIM)[3] and, most importantly, Domain-based Message Authentication Reporting and Compliance (DMARC).[4]
- Better unsubscribing: Senders must also support RFC8058[5]-compliant one-click unsubscribes and honour all opt-out requests within two days.
- Complaint rates: Both providers will start enforcing a maximum spam complaint rate threshold of 0.3 per cent to ensure users only receive marketing e-mails from legitimate, high-quality senders.

Compliance was required from February 2024 onwards, although enforcement of the DMARC and one-click list-unsubscribe requirements was deferred to June. Enforcement was initially in the form of temporary failure notifications, with outright rejection of non-compliant e-mails phasing in from April onwards. So the full impact is still to come, but we are already seeing early indicators of the impact.

EARLY IMPACT

It was widely expected that the new requirements would mean improved e-mail deliverability. Strong authentication, simple unsubscribing and low complaint rates are established best practices, and it felt reasonable that their enforced adoption would deliver improved e-mail performance.

Two important global KPIs, however, are suggesting the opposite, and there are several reasons for this:

- Perhaps unexpectedly, we have seen a sharp increase in spam complaint rates[6] since enforcement began. This is a double whammy for senders because the list-unsubscribe requirement was supposed to *lower* complaint rates. This may be a case of unintended consequences; when e-mail users action the new list-unsubscribe functionality they may *also* be given the opportunity to mark the e-mail as junk or move it to spam as part of the opt-out dialogue.

- There has also been a big increase in unknown users.[7] These are e-mails that no longer exist (or are believed to no longer exist). This is partly due to the new bulk sender requirements, but there is also another factor at play because both Gmail and Yahoo are also deleting inactive accounts (Gmail after 24 months and Yahoo after 12 months).

Complaints and unknown users have a big impact on any e-mail programmes' sender reputation, which in turn harms their deliverability. This is exactly what we have seen: during the first three months that the new bulk sender requirements have been effective, average spam folder placement[8] has increased from 4.7 to 6.7 per cent. Although not a huge change (yet), it is still a 40 per cent uplift, which will increase further as full enforcement of DMARC and list unsubscribe comes into effect, and soft fails are replaced by hard rejections.

FURTHER GUIDANCE

Over the past few months I have hosted webinars with Yahoo, Gmail (and Microsoft) to talk about these new requirements. We have received literally hundreds of questions, and there is still plenty of confusion about how the new requirements are being applied. Here is some of the top guidance I have been giving in response:

- When an RFC8058[9]-compliant list unsubscribe is present, a blue unsubscribe link appears next to the sender name at the top of the e-mail. However, many senders report that the link only displays intermittently, even though the list-unsubscribe record has been correctly deployed. Why is this happening?

  Gmail reserves the right to *not* expose list-unsubscribe links until it has assessed the sender's domain and is satisfied they are reliable. This stops scammers from inserting the headers and using responses to validate the e-mail addresses. Yahoo's FAQs echo this, stating: '[users] will see the blue "Unsubscribe" […] if we see sufficient reputation and engagement for your sending email address.'

  So while it is not great if your link is not showing, it is an extremely useful data point. It means that you are seen as a low reputation sender and that you should take steps to fix this because it will be hurting your deliverability.
- We have also heard plenty of questions around the 'unfairness' of subscribers using list unsubscribe to opt out and then *still* marking the e-mail as spam, especially when the principle of list unsubscribe (in theory) is to provide a trusted opt-out that makes spam complaints *less* likely.

  Subscribers may actually see several different versions of the dialogue box, and rules determine which version is shown. For compliant senders, *only* the text confirming the unsubscribe request is shown. The additional option to report the e-mail as spam is usually triggered by senders who are not honouring opt-out requests within the required 48 hours.

  Senders should test the list-unsubscribe experience for their programmes. If they see the 'mark as spam' dialogue they should validate they are processing these requests within the prescribed time frame.
- Some senders are compliant with *all* the new requirements, but their e-mails are still going to spam. What else should they consider?

  Remember the new requirements are much broader than *just* the ABC described previously. They also stipulate the need for valid DNS (Domain Name System) records, use of TLS (Transport Layer Security) encryption, RFC5322-compliant message formatting, use of ARC records

for forwarding and compliance with 'no impersonation' rules. Yahoo is also influenced by factors such as obfuscation of URLs, invalid domains in the rDNS and e-mails that are not RFC compliant.

IN SUMMARY

Gmail and Yahoo are not unreasonable, and compliant senders *should* avoid the spam folder. Mailbox providers often say they *do not* have a problem with legitimate, permission-based e-mail marketing. Their first priority, however, is to protect customers from bad actors. If your e-mails get caught by their filters it is usually because they look spammy. The first rule of getting delivered is simple: 'Do not look like a spammer.'

There are helpful new tools to stay aligned with the new sending requirements. Gmail has already added a compliance status dashboard to its Postmaster Tools[10] reporting, while Yahoo is updating its Sender Hub[11] with a beta version currently being trialled.

Compliant senders can request mitigation if their e-mails are generating false positive placement in their customers' spam/junk folders. Gmail's bulk sender escalation form can be found at https://support.google.com/mail/contact/gmail_bulk_sender_escalation, while Yahoo's sender support request form is available at https://senders.yahooinc.com/contact/.

The new sender requirements are established best practices, and e-mail marketers will benefit as they establish greater trust and engagement with their subscribers. It has already been reported that Microsoft also plans to align with these requirements, meaning all the major mailbox providers will soon operate a common set of sender expectations.

We can expect the requirements to become tougher in future. My guidance to senders is to be proactive. Start upgrading DMARC policies to p-quarantine/reject, process opt-out requests in real time and keep complaint rates *way* below 0.3 per cent. Doing so will future-proof you against stricter requirements down the road. In the meantime, you will enjoy even more amazing performance from your e-mail programmes.

References

(1) Kumaran, N. (2023) 'New Gmail Protections for a Safer, Less Spammy Inbox', available at https://blog.google/products/gmail/gmail-security-authentication-spam-protection/ (accessed 3rd September, 2024).

(2) Validity. (2021) 'Email Authentication: What Is Sender Policy Framework?', available at https://www.validity.com/email-authentication/sender-policy-framework/ (accessed 3rd September, 2024).

(3) Validity. (2021) 'Email Authentication: DKIM: Everything You Need to Know', available at https://www.validity.com/email-authentication/dkim/ (accessed 3rd September, 2024).

(4) Validity. (2021) 'Email Authentication: What Is DMARC?', available at https://www.validity.com/email-authentication/dmarc/ (accessed 3rd September, 2024).

(5) Levine, J. and Herkula, T. (2017) 'Signaling One-Click Functionality for List Email Headers', available at https://datatracker.ietf.org/doc/html/rfc8058 (accessed 3rd September, 2024).

(6) Email Glossary. (2020) 'What Is a Complaint Rate?', available at https://returnpathhelp.zendesk.com/hc/en-us/articles/220226808-What-is-a-complaint-rate#:~:text=The%20complaint%20rate%20is%20a,delivered%20to%20your%20subscribers'%20inboxes (accessed 3rd September, 2024).

(7) Validity. 'What Is An Unknown User?', available at https://knowledge.validity.com/s/articles/What-is-an-unknown-user?language=en_US#:~:text=Unknown%20users%20are%20invalid%20or,Unknown%20user (accessed 3rd September, 2024).

(8) Validity. (2024) 'Webinar: State of Email Live – Beyond DMARC!', available at https://www.validity.com/resource-center/state-of-email-live-beyond-dmarc/ (accessed 3rd September, 2024).

(9) Levine and Herkula, ref 5 above.

(10) 'Postmaster Tools', available at https://www.gmail.com/postmaster/ (accessed 3rd September, 2024).

(11) 'Any Questions So Far?', available at https://senders.yahooinc.com/contact/ (accessed 3rd September, 2024)