Messaging, Malware and Mobile Anti-Abuse Working Group

M3AAWG Best Practices for Sending Mandated Emails to Large Audiences

December 2020

The reference URL for this document is: https://www.m3aawg.org/SendingMandatedEmailsBP

Introduction

There are a number of scenarios in which senders may be required or compelled to send a bulk message despite the fact that such messages are highly likely to exhibit poor delivery metrics such as increased bounces or complaints. These messages are not intended to be used for standard marketing or transactional notices; these are the exceptions to the rule. Prominent examples of high-risk sends would be items such as breach notifications, product recalls, health and safety notices, or other notifications that might need to be sent to individuals who have been previously been suppressed or unsubscribed.

High-risk messages are intended to inform individuals of a significant change in policy and typically include information to help individuals mitigate damage they may have, offer assistance or provide noncommercial information about their account with an organization (e.g., offer to reset a password and/or provide a free credit monitoring service, for example).

While each organization bears the responsibility to determine if these high-risk sends are necessary, they should balance them with the potentially abusive nature of the messages and how frequently they occurred. Care should be taken to ensure that they are not overly intrusive. This M^{3}AAWG Best Practices document is intended to help senders make sure that worthy messages have the best chance to be delivered to the recipient, and that this effort is as minimally disruptive as possible, reducing any avoidable nuisance to users and to recipient Mailbox Providers (MBPs).

Before Sending High-Risk Messages

When determining whom to notify in advance of a client sending a mandated email, start by using the preferred points of contact for each MBP (Ex: postmaster@mailboxprovider.com, or the preferred postmaster contact information page). Personalized notifications should be sent to the most relevant MBPs for the individual organization sending the mandated email. When appropriate, sending a notice to a personal contact or the appropriate industry groups should be at the discretion of the sending platform and the organization responsible for sending the notices.

Tasks for Sending Organizations

Technical setup of sending infrastructure is key to successfully deploying these notifications. This may include:

- Consult the organization's email service provider (ESP) for possible technical requirements and solutions to help maximize the message's effectiveness and minimize its impact on the organization's IP and domain reputation.
- Provide guidance, instructions and timelines from relevant regulators or legal team.
- Organization configuration:
    - Consider a new email alias for these notifications instead of the usual marketing email alias (notice@sub.example.com, e.g.).
    - The sending organization should be unequivocally verified with domain authentication by sending from a branded organization domain. Please refer to M3AAWG BCP https://www.m3aawg.org/sites/default/files/m3aawg-email-authentication-recommended-best-practices-09-2020.pdf.
    - Do not use a newly registered cousin domain (or a variation on the normal sender domain) or register a new domain to send these notifications.

    - Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting & Conformance (DMARC) should all be configured for the sending domain.
    - Transport Layer Security (TLS) should be supported on the sending server for receivers which implement TLS.
- Identification: use an appropriate from name for the message like "[Organization name]: Notification" and "Important notification" in the subject line.
- Send emails with minimal use of tracked elements in the message:
    - Limit the number of links to just those that are required, or none at all.
    - Limit the contents to material exclusively relevant to the issue, with no marketing at all.
- Use an appropriate template style for the notification type—plain or minimal in appearance.
- Suspend marketing communications during the notification period.
- Consider who should receive these messages based on actual requirements of the notification. Build strategy to focus on the least risky to the most risky communication groups.
    - Impacted users
    - Active users
    - Subscribed users
    - Unsubscribed users
    - Bounced users (Exclude known dead addresses. These should never be messaged as they will not be received by the intended recipient.)
- Internal teams should coordinate to have a consistent message across all customer service teams. This includes social, call center and frontline staff interacting with customers.
- Consider alternative contact methods to reach user segments (a non exhaustive list):
    - Postal
    - Social media
    - Traditional media
        - Newspaper
        - Radio
        - TV
    - SMS
    - Website notification
- Determine if information is needed for auditing purposes, and what that would entail.

Tasks for Email Service Providers (ESPs)

When working with clients to send notifications, ESPs may not be able to influence the message content much, as it will likely be written by a legal professional to cover the organization's responsibilities under the notice. When communicating with MBPs, notifications should include details on:

- The appropriate contact details for the organization or agency where recipients can get more information, and include a copy of the message itself if possible.
- The appropriate sending volumes and days required.
- The appropriate sending infrastructure to be used.
    - Some mailbox providers encourage reserving an IP range exclusively for mandated email notification IP addresses.
    - Sending domains/hostnames
    - Dates and times
    - Volume expectations

- Throttle sending speeds over time to help avoid volume peaks, which may be onerous to receiving networks and may trigger anti-spam mechanics.

- SPF, DKIM, and DMARC should all be configured for the sending domain.
- TLS should be supported on the sending server for receivers which implement TLS.
- Consider having a preferred breach or mandated email process in your contract or Data Protection Agreement.

Conclusion

When considering the target audience for these notifications, some groups of recipients are inherently more complicated to reach out to and alternative methods of communications may be worth considering. For known bounce addresses, or users that have reported a brand as spam in the past, consider alternative options such as postal notification or notifications in relevant newspapers.

It's important to remember that this process should only be used for mandated messages that are an exception to normal sending practices and which are likely of special relevance to the recipient.

As with all documents that we publish, please check the M3AAWG website (www.m3aawg.org) for updates