New Google/Yahoo Bulk Sender Requirements

https://campus.barracuda.com/doc/104367158/

Google and Yahoo have recently announced more stringent sender requirements starting **February 2024** to protect their customers from email attacks, including SPF, DKIM, and DMARC.

For more information from Google, see https://blog.google/products/gmail/gmail-security-authentication-spam-protection/.

For more information from Yahoo, see https://blog.postmaster.yahooinc.com/post/730172167494483968/more-secure-less-spam.

The following is a composite list of requirements:

For all senders:

- Use SPF for email authentication

OR

- Set up DKIM for message integrity
- Have valid PTR records for each sender IP
- Require TLS encryption
- Keep the spam rate threshold < 0.1% and not reach 0.3%+
- Do not impersonate Gmail

For senders of over 5,000 messages per day to Google and Yahoo recipients:

- Use SPF for email authentication

AND

- Set up DKIM for message integrity
- Have valid PTR records for each sender IP
- Require TLS encryption
- Keep the spam rate threshold < 0.1% and not reach 0.3%+
- Do not impersonate Gmail
- Must have DMARC policy
- Must pass DMARC alignment
- Include easy one-click unsubscribe

These requirements will affect every organization sending email to recipients hosted by Google, Yahoo, and AOL, which total over two billion mailboxes worldwide. Failure to comply with these requirements may result in your messages being rejected or marked as spam by your intended recipient.

Next Steps

1. Familiarize yourself with sender authentication protocols. See Domain Fraud Protection Background for more information.
2. Implement DMARC record – If you do not already have a DMARC record in place, begin by setting up a record in reporting mode. This will aid you in ensuring proper SPF/DKIM verification/alignment. Without these records, the next two step will be more challenging. For more information, see Configuring Domain Fraud Protection with Barracuda.
3. Verify SPF records – Ensure your SPF record is current and includes all sources from which emails using your company domain can originate. Use your DMARC reports to help troubleshoot. For more information, see Addressing SPF Issues.
4. Implement DKIM signing – Ensure you have DKIM signing configured. This includes your own mail systems as well as third-party services, such as Mailchimp or SendGrid.

   See the following for some of the more common mail services:

   Microsoft 365 or Google Workspace – Configure DKIM signing for your outbound mail through the administrative portal:
    - Microsoft 365 – How to configure DKIM signing for your domain
    - Google Workspace – How to configure DKIM signing for your domain

   On-prem Exchange – There is no native DKIM signing; you must use a 3rd party tool, such as Email Architect.
   3rd party services – 3rd party services offering DKIM signing capabilities varies. Run a quick search on any search engine to get setup information. Each email vendor will have their own instructions to configure DKIM. For example, some common 3rd party services:

    - SendGrid
    - Salesforce
    - Mailchimp
    - Postmark

Note that this is not an exhaustive set of instructions. For instance, you may also need to implement PTR records for each sender IP, add one-click unsubscribe, or implement additional requirements mentioned earlier in this article.