WHITE PAPER

Prevent your email from being filtered as spam

The most common problems that companies encounter in online emailing is spam. It is not the spam they received instead, their own emails are going straight to the junk even if it's as authentic as they intend it to be. Many business owners, especially those in the email campaign department are the usual victims.

Going cloud indeed is a huge leap of relief for many business owners who have embraced cloud platforms to becoming more productive for ease and lesser worries from potentially unwanted programs. Auto-detection of malware and phishing activities are gradually improving these days with the help of dedicated experts that handles data protection in the cloud. However, together with this security protection in-place at the backend, it also affects legitimate emails in going to the junk folders of the recipients. It can get blocked by spam filters and flag your hard work as spam.

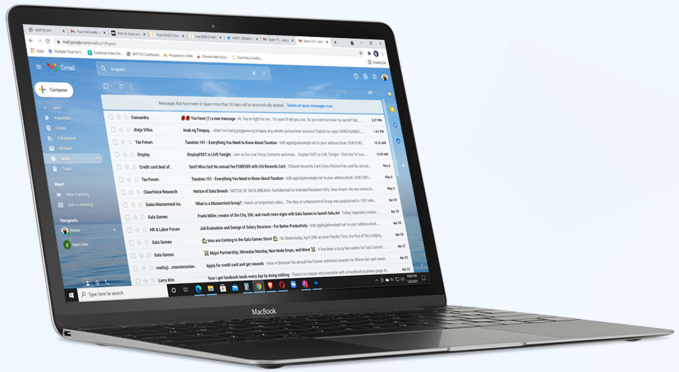
When your email is authentic, that does not ensure deliverability to the inbox of your recipients. **Your emails pass through many security checks** along every network nodes before it reaches your intended destination.

Don't be frustrated!

We got the solutions for you with Google Workspace!

Identify and prevent email spamming

Senders are responsible for the messages they send out to the cloud because spam filters are set-up to block, delete or redirect unauthenticated emails to the spam or junk folders. So, how do we prevent these from happening to our legitimate emails? Well, make sure that your email's origin is verified.



As a security standard, email authentications are set forth by every email service providers in order for their server to be identifiable and verified. **Google Workspace** complies with the 3 requirements of email authentication which are the Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and the Domain-based Message Authentication, Reporting & Conformance (DMARC).

Best practices in preventing your emails from going to the junk, promotional, spam folder, bounced email or undelivered.

Set up the Sender Policy Framework (SPF) - Google's SPF is TXT records added to a domain's name server. It provides identification of the permitted mail server being used to send email on behalf of the domain. This prevents spammers from imitating your email addresses on Google Workspace. By default, the Google's default SPF is **v=spf1 include:_spf.google.com ~all** of which other mail exchanger's IP address can also be added in the string of codes in order to permit another mail exchangers.

When you're using your Google Workspace email address to send email in 3rd-party apps that are hosted from another server, you must permit the IP address of such apps in order to be verified by the spam filters. Example for permitted multiple mail exchangers would look like this: **v=spf1 ip4:83.206.106.17 include:_spf.google.com ~ all** where the **ip4:83.206.106.17** is the IP address of the mail exchangers of the 3rd party email service provider. Some mail service providers may have their own SPF codes such as for example with the MailChimp's SPF: **v=spf1 include:servers.mcsv.net?all** The rule of the thumb in your DNS records must only have one TXT for the SPF.

So, instead of having two TXT values as :
v=spf1 include:_spf.google.com ~all
v=spf1 include:servers.mcsv.net ?all

Find the IP address of **servers.mcsv.net** through the nslookup command and add it to the Google's string of codes for SPF.

Set up the DomainKeys Identified Mail (DKIM)

While SPF provides verification of the mail servers, the DKIM, on the other hand, puts an encrypted digital signature to the headers of your outgoing emails. This is to prevent eavesdroppers from hijacking your emails in their rogue server, forge it and then deliver it to your recipients. DKIM helps in keeping the original seal of your emails as it is being transported to the other mail server. Every time an email arrives at the mail server, spam filters do the security checkup. With the SPF validating your origin and DKIM proves unaltered headers of the email during its transport, this clears your message and will be flagged for inbox and not as spam.

Did you know that there are DNS hijackers eavesdropping to your emails? They can piggyback on your emails forging it as it gets delivered to your recipients.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

DMARC is the 3rd part of email authentication that adds a link for SPF and DKIM to protect against direct domain spoofing. This allows the owner of the domain to create a policy on what to do to unauthenticated emails whether to delete, quarantine, report or reject. NOTE: An SPF and DKIM must be set first.
Google Workspace follows the DMARC.org standard and Google Workspace customers can set up their own policies for it either to be rejected, quarantined or do nothing. Log reports are created for owner's personal review. Filtered emails can be auto-forwarded as well to postmaster@yourdomain.com and dmarc@your_domain.com for further review of any possible new threats.

Enhance your credibility by providing your recipients to opt-out from your constant emails than letting them choose to tag your email as spam and don't forget to allow servers to breathe.

Add an Unsubscribe option

No matter how well we create our messages and its contents, let's face it, our subscribers may change their mind or could get frustrated that they want to opt-out from receiving your emails. So instead of letting them mark your messages as spam, which will affect your spam score or online credibility. The best way is to add an "unsubscribe" link to your emails.

Slow down and keep your pace

Although we can send massive emails in just a single click and all the authentications in place, mass emailing can create a bounced or rejected message when spam filters detect that you are sending more than the limit or congesting the network pipe. When sending emails directly from Google Workspace, users are limited to send up to 2,000 emails a day. However, one-time sending of these number would most likely get rejected by email servers due to flooding. Trickle your emails by batch, right about 100-200 emails every minute. An Email scheduler helps with this technique so that you don’t need to manually send the emails yourself.

Finally, preventing emails from being flagged as spam starts from the sender's end. As long as the content and the source is valid and you have all the digital signatures in place, your emails can have better chances to be read than going straight to the junk.

LaQuest™
Tasks Simplified

PLEASE WRITE US IF YOU'VE ANY QUESTION OR NEED SUPPORT:

SUPPORT@LAQUEST.NET

INFO@LAQUEST.NET

WWW.LAQUEST.NET