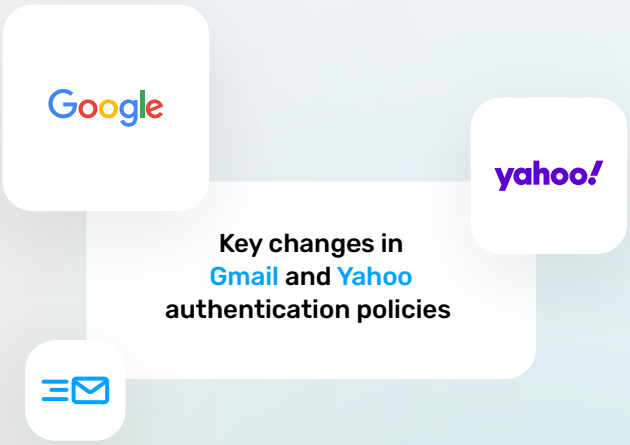
GetResponse

Adapting to New Email Standards in 2024



In February 2024, Gmail's and Yahoo!'s new email authentication requirements and spam prevention policies will come into force. This infographic will guide you through these changes and help you steer your email marketing campaigns in the right direction.

What's changed?

- Custom Domain Requirement
- Email Authentication with DKIM and DMARC
- Google Spam Complaints Limit <0.3%
- One-Click Unsubscribe & Prompt Unsubscribing

Who's impacted?

Bulk senders

Google defines bulk senders as those sending over 5,000 messages to Gmail addresses daily, while Yahoo's criteria remain unclear. Regardless of list size or frequency, we advise all email marketers to comply with these new rules for safety.

How to adapt in 4 steps

Step 1

Get a custom domain

Start sending emails with your own domain and ditch free email domains like @gmail.com

Step 2

Authenticate your emails

Protect your brand against spam or phishing and verify that emails are genuinely sent by you.

Step 3

Manage your email list

Monitor your spam complaints and keep them below 0.3% by ensuring your list is clean and engaged.

Step 4

Simplify unsubscribing process

Implement 1-click unsubscribe and honor unsubscribing requests within 2 days.

Email authentication for beginners

Custom domain

Your own unique branded domain you'll use to send emails, e.g. @yourcompany.com.
It can enhance your credibility and deliverability.

Email authentication

A process used to verify that an email is legitimately from the sender it claims to be, helping to prevent spam and phishing attacks.

SPF (Sender Policy Framework)

SPF is an email authentication method which ensures the sending mail server is authorized to originate mail from the email sender's domain. To put it simply, SPF defines which IP addresses can be used to send emails from your domain.

Example record

```
_spf.getresponse.com → "v=spf1
ip4:104.160.64.0/23 ip4:104.160.67.128/25
ip4:104.160.68.224/27 ip4:104.160.69.0/27
-all"
```

How it works:

Let's take a look at servers' conversation:
Mike's server: Hey, Bob's server. I've got a new message from Mike. **Bob's server:** Hi Mike's server. What's your SPF? **Mike's server:** There you go, here's my SPF. There's a whole list of IPs that Mike himself declared as the ones which can be used on his behalf. **Bob's server:** Ok, let me see... And the message you have for me is sent from IP 64.233.160.19. Ok, it's on the list. Everything looks fine. Gimme the message, I'll show it to Bob. Thanks!

DKIM (DomainKeys Identified Mail)

DKIM standard has been created for the same reason as SPF: to prevent the bad guys from impersonating you as an email sender. It's a way to additionally sign your emails in a way that will allow the recipient's server check if the sender was really you or not.
To make that possible you have two keys: a private one and a public one.

Example record

```
k1024f._domainkey.getresponse-mail.com →
"k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNAD-
CBiQKBgQDGuwrmvQLYTRSpi-
hV3aVo8mJqKUzyIRCXM77aDJJoDhxC+hzaJNPfec9jm6Q
HBZDScGnaInIPt3P+UCskzU8hw1mSPUphFm3Xr6at8rOp
FX4wLxgamgfOszd+vxbcz1uNNXqAdDTmdZXUfwXS+WEld
srAaNw8nczIu0wr01Q7rywIDAQAB"
```

How it works:

Let's say you want to send a letter. To do it you have to have the envelope and some paper. Your envelope is already signed and everyone knows who will deliver it (that's what SPF record does) but to be sure that recipients will know that the letter comes from you, you put a special seal on the envelope (public key). Only you have such unique seal, and it can be identified by you (private key).

DMARC

DMARC is a protocol that protects the domain from being spoofed. It is done by adding a proper policy to the domain. There are three policies – none, quarantine and reject. DMARC checks the SPF and/or DKIM, if both of them fail, then based on the policy message is treated differently – nothing is done and message gets accepted (none), message is quarantined or placed in the spam folder (quarantine), message is rejected (reject).

Example record

```
_dmarc.getresponse.com →"v=DMARC1; p=reject;
sp=none; rua=mailto:dmarc_agg@d-
marc.250ok.net,mailto:getresponse@d-
marc.postmastery.com; ruf=mailto:dmarc_fr@d-
marc.250ok.net; rf=afrf"
```

How it works:

Let's go back to the "letter" example.
You always receive a letter from one of your friends on Monday. It is always delivered by the same postman (SPF) and has the same seal (DKIM). One day, a different postman delivers the message and the seal is broken. There is a text on the envelope that says what you have to do in such case (DMARC). You can accept the letter (policy none), place the letter in a trash can (policy quarantine) or do not accept the letter (policy reject).

If the letter would be delivered by a different postman but the seal wouldn't be broken you could still accept it.

If the letter would be delivered by the same postman but the seal would be broken, you could also accept the letter.

Learn more about email deliverability

Want to learn more about email deliverability? Discover other insightful articles on the GetResponse blog and start making more impact with your email campaigns.

EXPLORE THE BLOG →