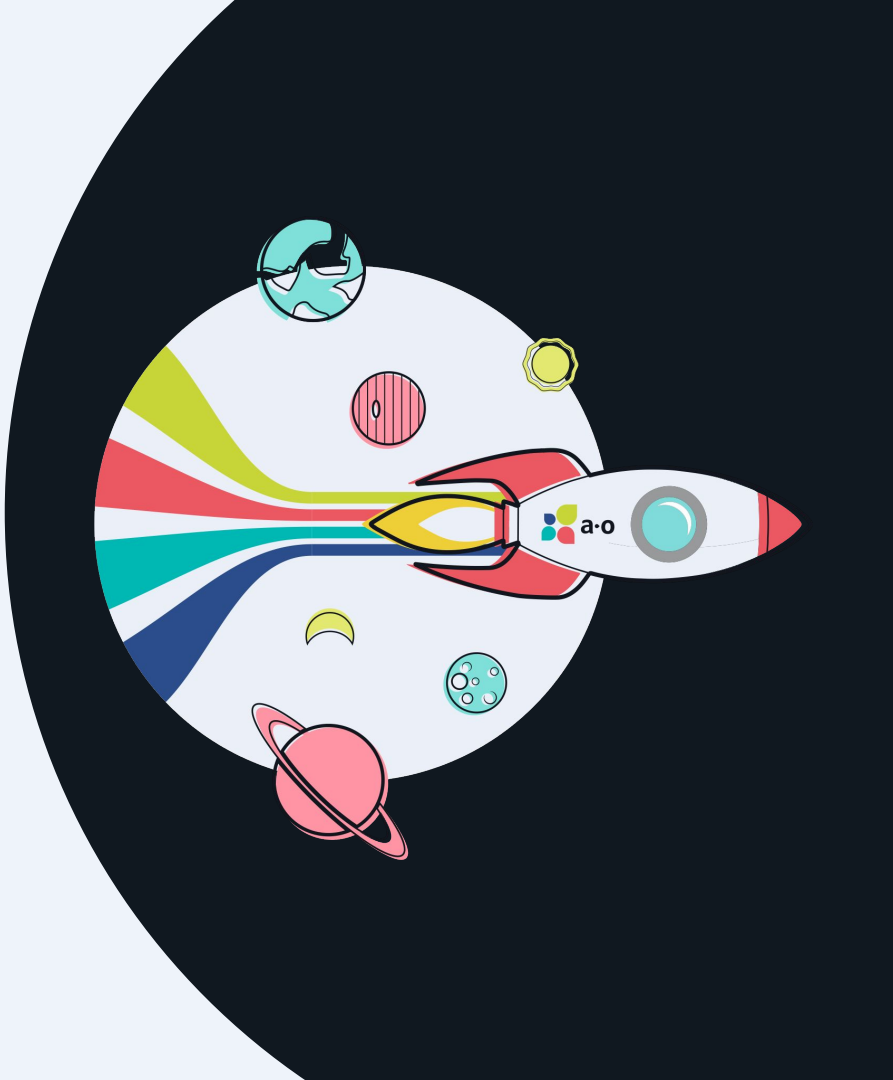
act·on

Office Hours:

Google & Yahoo Sender Guidelines 2024

Brian Willis
Manager of Deliverability Services



Brian Willis

Not to be confused with Alfie, appearing on the right

- Manager of Deliverability & Professional Services
- he/him
- With Act-On for ~6 years
- Mildly PNW obsessed. Coast, mountains, outdoors, food, beer, wine, coffee. It's all great.
- Passionate about the email world and customers' email success

Today's Agenda

- Google & Yahoo Briefly
- Required DNS: What does it all mean?
  - DKIM
  - SPF
  - DMARC
- Spam Complaints
- One-click Unsubscribe
- Open Office Hours with Deliverability Team

act·on

Google & Yahoo's Changes, In Brief

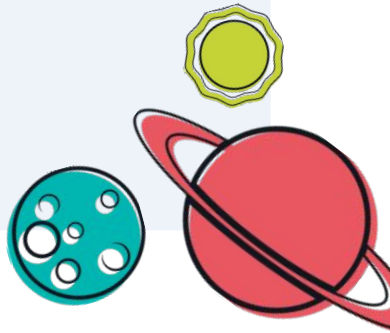
Beginning February 1, 2024, Google & Yahoo updated email requirements for reaching any of their consumer domains (Gmail, Yahoo, AOL, etc...)

- Email Authentication (SPF, DKIM, DMARC) as requirements
- Keep your spam complaint rates down!
- Ensure easy access to unsubscribe process

act·on

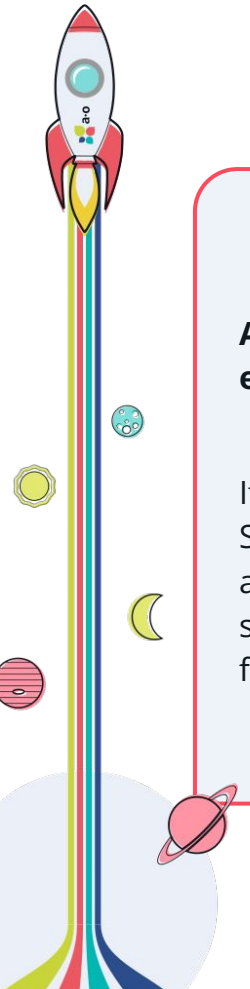
A few terms defined

- **From Domain**: Visible domain used in email address (ex: example.com)
- **From Address**: Full email address used for sending email (ex: act-on@example.com)
- **Envelope Domain**: Frequently referred to as the Return Path. Only visible in email headers. Used to route delivery information, spam complaints, unsubscribe requests, etc...
  (ex: mailer.example.com)



act·on

DNS Authentication Requirements



SPF

Act-On is authorized to send emails on your behalf.

If Act-On is not included in the SPF entry, many email servers assume we lack permission to send your emails, and may filter email accordingly.

DKIM

I am who I say I am.

DKIM, similar to SPF, authenticates the sender of an email by adding a digital signature to the message header. It verifies the sender's identity, ensuring that they are who they claim to be.

DMARC

I pass DKIM or SPF *and* it's with the same domain.

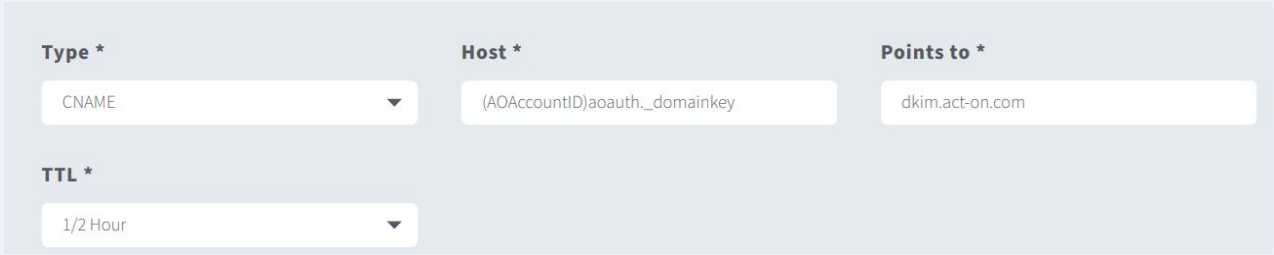
DMARC, the newest requirement, ensures you have DKIM or SPF with the same domain in the From Address.

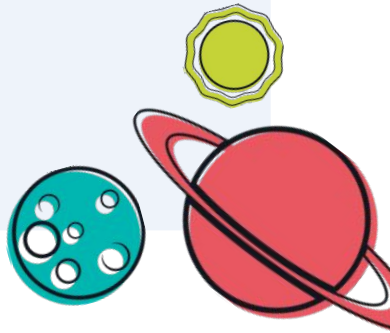
Tells mail servers what to do with mail if it fails DMARC.

act·on

DKIM (DomainKeys Identified Mail)

- “I am who I say I am”
- Every single From Domain you use for mailing should be authenticating with DKIM. Arguably the most important authentication element from a reputation standpoint.
- Like a secret key or password encrypted in email headers. Google or Yahoo will check the key, and confirm with the sender that they’ve got the right secret password





act·on

SPF (Not the sunscreen one)

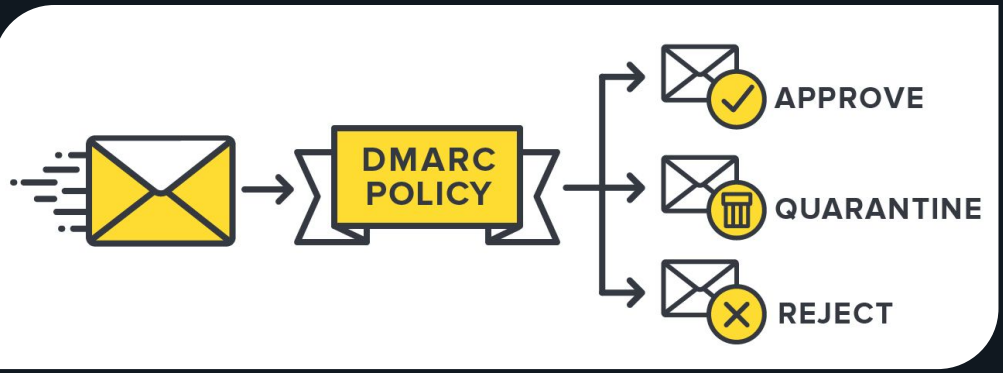
- Primarily looked for on the Envelope Domain of an email
- Is this mail server allowed to send on our behalf?
- TXT Record:
  - v=spf1 include:_spf.act-on.net -all
  - If you already have a SPF record, just paste the “include:_spf.act-on.com” between the already existing v=spf1 and -all.
- Act-On also requests SPF on the From Domain. This is because of an antiquated “Sender ID” policy from Microsoft (hotmail/outlook/live/msn). This should be dead as a policy, but we’ve seen indications of it pop up randomly over the years, so we still request this.

act·on

DMARC

DMARC (Domain-based Message Authentication, Reporting, and Conformance):

- Provides a framework for handling unauthenticated emails.
- Specifies where feedback and reporting should be sent, aiding in abuse detection.



Crafting your record for success

Basic, minimum requirement DMARC record *

To add DMARC to your DNS, create a TXT record such as:

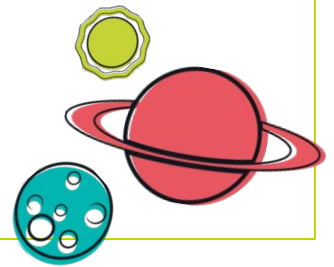
- Name: _dmarc or _dmarc.yourdomain.com (depending on your DNS provider)
- Type: TXT
- Value: v=DMARC1; p=none

* This is a simplified version of what most DMARC policy records can look like

act·on

Any time you use a new top level domain for mailing, ensure you have a DMARC record.

Must align with SPF and DKIM with the "From" domain for enhanced security.



Expanding on DMARC

Beyond the “none” policy.

- p=quarantine *or*
- p=reject

What should a mailbox provider do if I fail DMARC?

- Spam or Quarantine folders?
- Bounce it?

Reporting

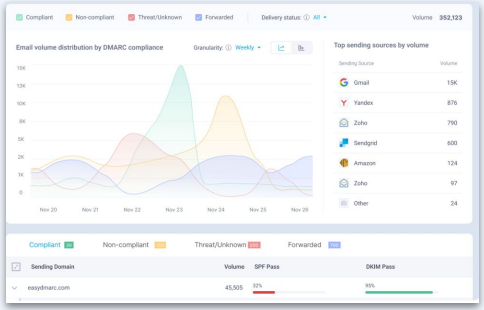
Use a reporting tag to get reports on where DMARC passes and fails!

rua=mailto:postmaster@example.com

Do not set this as your own email address. Your inbox will never be the same again.

DMARC Tooling

Use 3rd party reporting tools to understand where you may be failing DMARC, and if others are sending unauthenticated mail from your brand!



act·on

One-click (or one-step) unsubscribe

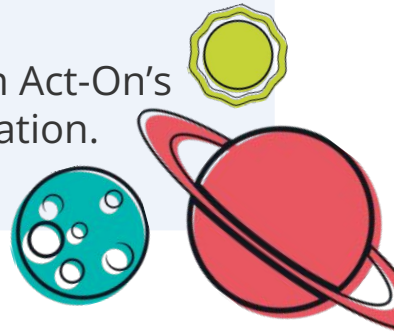
> Our users should be able to unsubscribe from unwanted emails without any hassle. It should just take one click. While we have promoted solutions for some time, adoption of these common sense standards have been low. We will require senders to support one-click unsubscribe and honor our users requests within two days

yahoo!

Upon clicking the unsubscribe link, can a recipient successfully unsubscribe from that page, or do they need to complete other steps/forms/process?

Subscription management is good and liked by providers. Let people choose what mail they want to receive, or choose to opt-out altogether.

None of this is a real change from Act-On's vantage point, just a good clarification.



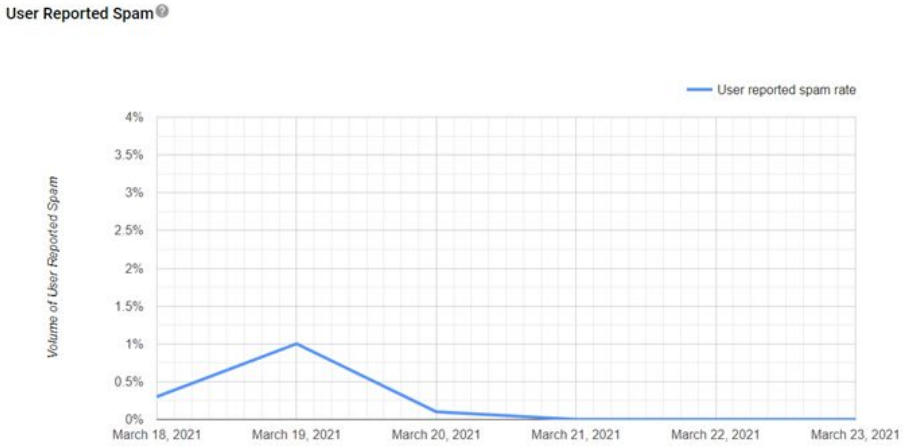
act·on

Spam Complaint Rate Guidance

Gmail: "Keep spam rates reported in Postmaster Tools below 0.10% and avoid ever reaching a spam rate of 0.30% or higher"

Postmaster Tools is the only way to know anything about Gmail spam complaints.

Yahoo: "**Keep your spam rate below 0.3%"**



Complaint Feedback Loop

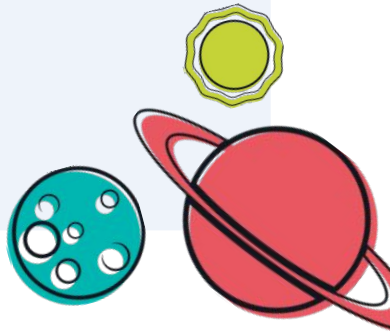
Identify opportunities to improve how well your emails are received.

act·on

Spam Complaint Rates

Keep below a 0.3% spam complaint rate... or else?

- This is an important threshold and *can* cause problems
- One message with a high complaint level won't hurt you, especially if you have a high reputation with Gmail or Yahoo
- Show a pattern? You can definitely lose with those providers and see decreased inbox placement



act·on

Thank You!

act·on