Activate

Deliverability
2024

AGENDA

- **Set the scene: how we got here**

- **Highlight the key elements of the 2024 Google and Yahoo mail policy requirements**

- **Implementing DMARC**

- **Live Q&A**

Seth Charles

Senior Director,
Iterable Delivery Operations

Connecting people
with the products that
bring them joy

Yahoogle in 2024

What's happening:

In October, Google and Yahoo made a joint announcement that beginning in 2024, they would begin enforcing infrastructure *and* feedback threshold requirements will affect <u>every commercial email marketer on the planet.</u>

Survey time

"How confident are you that your email program, as it stands today, *is* compliant with the "new" Google+Yahoo mail policies?"

Primary Elements of Requirements

1 **Message Authentication**

Messages must be signed with both an SPF record as well as a DKIM signature

2 **IP <> Domain FCrDNS**

A sending IP is mapped to a domain configuration using a PTR record, which in turn resolves back to the originating IP with an A record

3 **Domain and Brand Security**

Sending domain configurations must include a DMARC record within their DNS with at least a "none" policy

4 **User Reported Spam Rate**

Commercial messages should maintain at or below a .1% spam rate, and not spike above .3% within Google Postmaster Tools or Yahoo CFL
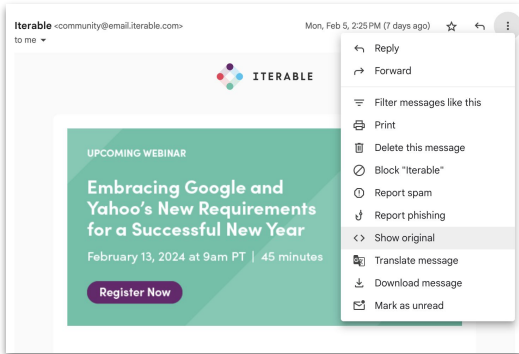
5 **"One click" List-Unsubscribe**

All commercial mail will need an RFC compliant list unsubscribe mechanism included within its header

Message Authentication

- **SPF (Sender Policy Framework):** The IP responsible for sending the message has been given permission to do so by the domain owner

- **DKIM (Domainkeys Identified Mail):** Public and private key cryptography to verify the integrity and authenticity of an email's content fingerprint

Original Message

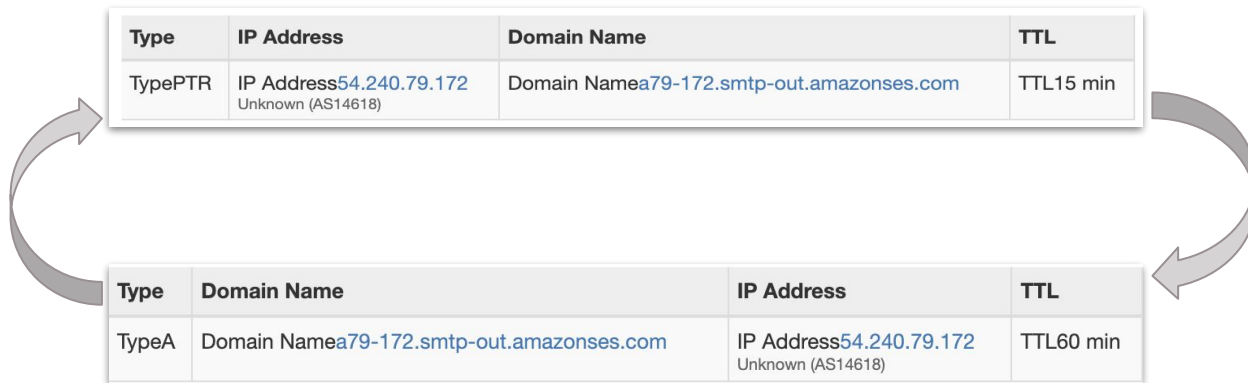|	
Created at:	Mon, Feb 5, 2024 at 2:25 PM (Delivered after 0 seconds)
From:	Iterable <community@email.iterable.com>
To:	seth.charles@iterable.com
Subject:	[PROOF] Upcoming Webinar: Embracing Google and Yahoo's New Requirements
SPF:	PASS with IP 54.240.79.172 Learn more
DKIM:	'PASS' with domain iterable.com Learn more
DMARC:	'PASS' Learn more

IP <> Domain FCrDNS

Type	IP Address	Domain Name	TTL
TypePTR	IP Address54.240.79.172 Unknown (AS14618)	Domain Namea79-172.smtp-out.amazonses.com	TTL15 min

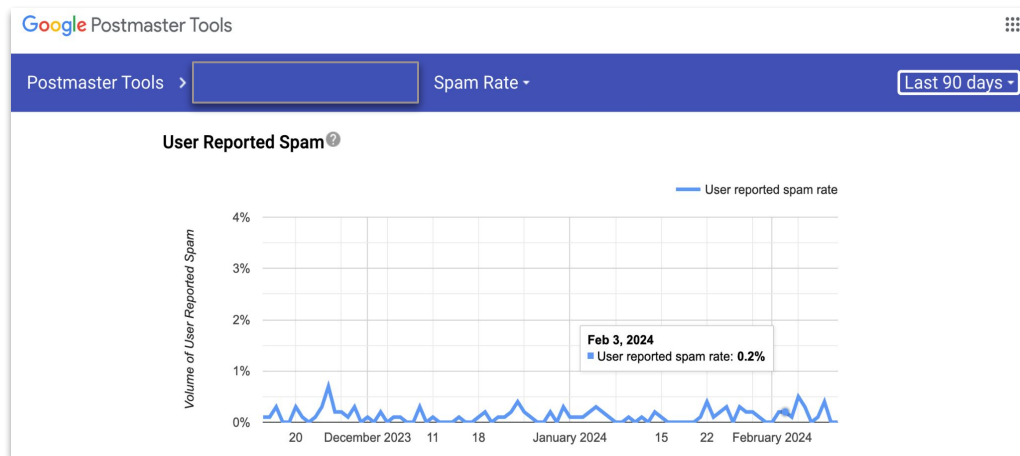| Type	Domain Name	IP Address	TTL
TypeA	Domain Namea79-172.smtp-out.amazonses.com	IP Address54.240.79.172 Unknown (AS14618)	TTL60 min

IP "PTR" RECORD

DOMAIN "A" RECORD

User Reported Spam Rate

- This is the percentage of user-reported spam vs emails that were sent to the inbox. Emails delivered to the spam folder are not included in the calculation. Only emails authenticated by DKIM are eligible for spam-rate calculation.

- Keep rates below 0.10% and avoid ever reaching 0.30% or higher.

- Maintaining a low spam rate makes senders more resilient to occasional spikes in user feedback.

- Similarly, maintaining a high spam rate will lead to increased spam classification. It can take time for improvements in spam rate to reflect positively on spam classification.

One Click List-Unsubscribe
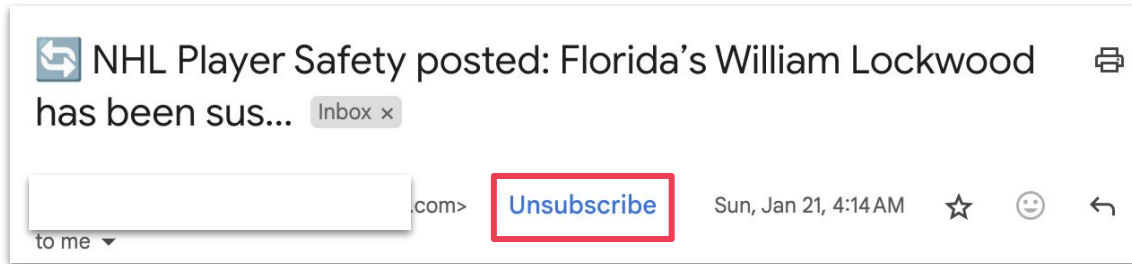
- Letting people opt out of your messages can improve open rates, click-through rates, and sending efficiency. One-click unsubscribe makes it easy for people to opt out. If you send more than 5,000 message per day, your marketing and subscribed messages must support one-click unsubscribe.

- To set up one-click unsubscribe, include both of these headers in outgoing messages:

  - List-Unsubscribe-Post: List-Unsubscribe=One-Click

- All in accordance to **RFC 8058**

**Activate Virtual:
Deliverability**

Survey time

**"How does your brand monitor, manage, and
adapt to your domains' DMARC data?"**

Domain and Brand Security: DMARC

- Simple record that lives within the domain's DNS location "**_dmarc.domain.com**"

- Any root domain policy is automatically applied to all subdomain combinations, unless they themselves have an explicit DMARC record

- Conditions of passing DMARC:
  - SPF or DKIM domain must pass authentication AND align with FROM domain

- Most important fields are "v="; "p="; and "rua="

- Policy Types
  - "none" - Take no direct action
  - "quarantine" - messages that fail DMARC routed to SPAM folder
  - "reject" - messages that fail DMARC are bounced

- **TXT record for "derschnurrbart.com"**

- **"v=DMARC1; p=quarantine; rua= email@myDMARCtool.com"**

Thank You!

Live Q&A

ITERABLE

Follow us!

Not everyone is a leader, be a follower. For marketing tips, tricks, and updates, scan to follow us on all social platforms.