

Are you ready for the changing Email Authentication Requirements?

Ryan Xiong
Senior Engineer



Agenda



Business Impacting Event



Deploying DMARC on Your Own



What should we expect from a successful implementation of Email Authentication?



Summary

Business Impacting Events



Email Authentication Required for Email Delivery

New Gmail protections for a safer, less spammy inbox

Oct 03, 2023 | Starting in 2024, we'll require bulk senders to authenticate their emails, allow for easy unsubscribe and stay under a reported spam threshold.
2 min read

 Neil Kumaran
Group Product Manager, Gmail Security & Trust

← Share



More Secure, Less Spam: Enforcing Email Standards for a Better Experience



Source: <https://blog.google/products/gmail/gmail-security-authentication-spam-protection/>

Source: <https://blog.postmaster.yahooinc.com/post/730172167494483968/more-secure-less-spam>

Google and Yahoo Requirements for Senders

<5,000 per day

- SPF or DKIM email authentication required
- Ensure valid forward and reverse DNS records
- Spam rates reported in [Postmaster Tools](#) below 0.3%
- Message format adheres to [RFC 5322](#) standard
- No Gmail Impersonation in FROM headers (Gmail setting DMARC Quarantine policy)
- Email Forwarding requirements

>5,000 per day

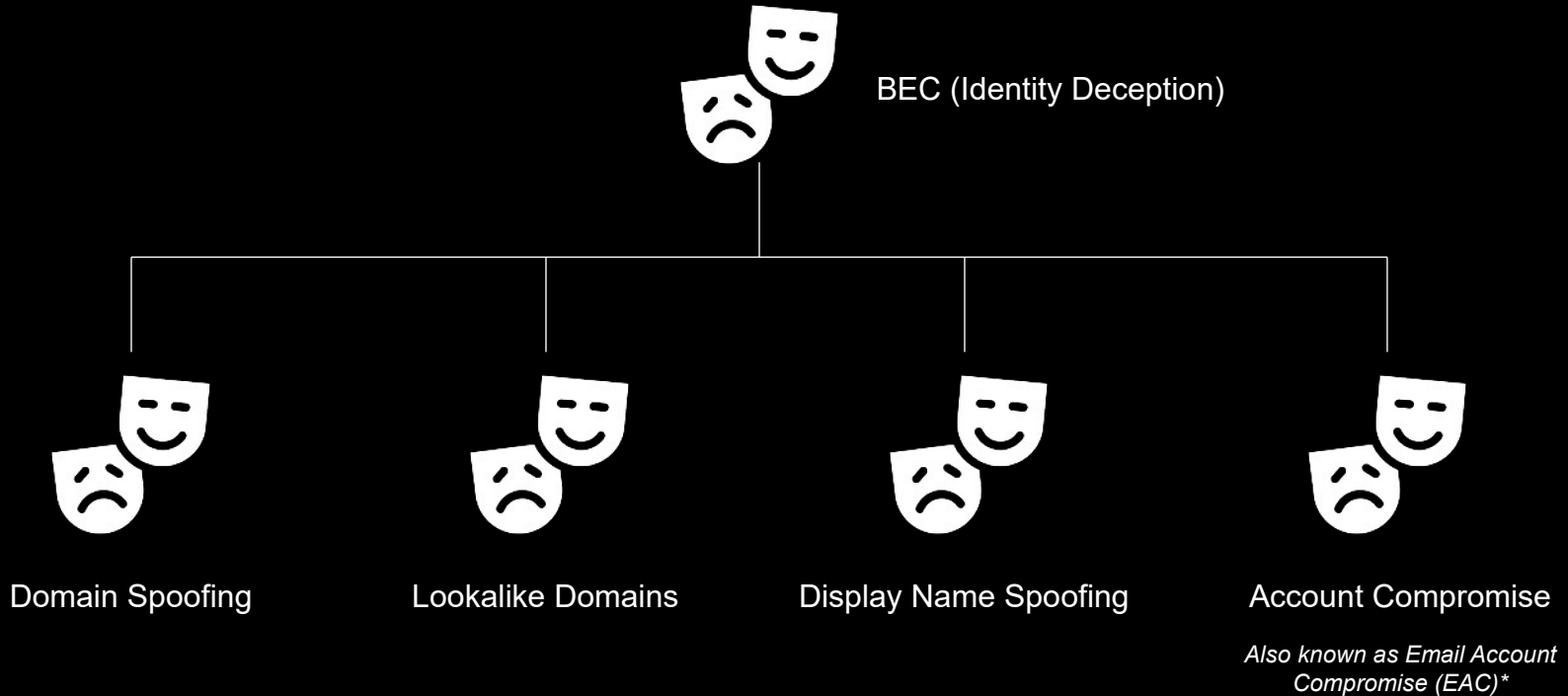
- SPF and DKIM email authentication required
- Ensure valid forward and reverse DNS records
- Spam rates reported in [Postmaster Tools](#) below 0.3%
- Message format adheres to [RFC 5322](#) standard
- No Gmail Impersonation in FROM headers (Gmail setting DMARC Quarantine policy)
- Email Forwarding requirements
- DMARC email authentication for your sending domains
- From: header must be aligned with either the SPF domain or the DKIM domain
- One-click unsubscribe for subscribed messages

DKIM ,SPF ,DMARC – What are these?

What?	How?	Why?
DKIM	Email authentication standard that works by assigning a digital signature to messages sent from (outbound) an email account.	Helps protect email senders and recipients from spam, spoofing, and phishing
SPF	Each domain lists in one DNS record the list of servers that are allowed to send emails for that domain. As owner of a given domain, you will tell the world which servers you will send emails from. That is typically your SMTP server.	When an email provider like Gmail sees an email sent from an address @example.com but coming from a server not listed in the SPF record, it knows it is likely spam , non-legitimate and Spoofed
DMARC	DMARC's alignment feature prevents spoofing of the "header from" address by: Matching the "header from" domain name with the "envelope from" domain name used during an SPF check, and Matching the "header from" domain name with the "d= domain name" in the DKIM signature.	DMARC ensures that legitimate email is properly authenticating against established DKIM and SPF standards, and that fraudulent activity appearing to come from domains under the organization's control (active sending domains, non-sending domains, and defensively registered domains) is blocked. Two key values of DMARC are domain alignment and reporting.

Common BEC Tactics

Business Email Compromise (BEC)





Change Payment Request

Message ?

Delete | Reply | Reply to All | Forward | Attachment | Meeting | Move | Junk | Rules | Read/Unread | Categorise | Follow Up

Change Payment Method

 Philip Sow <philip.sow@club22sg.com> Today at 14:49

To:  ryan.xiong@club22sg.com

Hi Ryan,

Please take note of the latest changes in the payment method for Shipment #5689.

You must process the payment transfer to the DBS Bank Account: 095-7782506.

Best regards,

Philip Sow

Message Header

14:49

PS

Philip Sow

Change Payment Method

To: ryan.xiong@club22sg.com,

Reply-To: hacker@malware4rent.org

Content-Type: text/plain; charset=us-ascii

Mime-Version: 1.0

Content-Disposition: inline

X-Authentication-Warning: m0314289.pops.net: www-data set sender to www-data@malware4rent.org using -f

User-Agent: Mutt/1.5.21 (2010-09-15)

Received: from mx1-eu1.ppe-hosted.com (unknown [10.80.45.101])

by pure.maildistiller.com (PPE Hosted ESMTTP Server) with ESMTTPS id AB21C60061
for <ryan.xiong@club22sg.com>; Tue, 13 Aug 2024 06:49:09 +0000 (UTC)

Received: from ip-10-253-38-75.us-west-2.compute.internal (ec2-54-214-13-31.us-west-2.compute.amazonaws.com [54.214.13.31])

by mx1-eu1.ppe-hosted.com (PPE Hosted ESMTTP Server) with ESMTTP id 75BE120005C
for <ryan.xiong@club22sg.com>; Tue, 13 Aug 2024 06:49:09 +0000 (UTC)

Received: from m0314289.pops.net (localhost.localdomain [127.0.0.1])

by ip-10-253-38-75.us-west-2.compute.internal (Postfix) with ESMTTPS id 211161B001295
for <ryan.xiong@club22sg.com>; Tue, 13 Aug 2024 06:49:03 +0000 (UTC)

Received: (from www-data@localhost) by m0314289.pops.net (8.14.7/8.14.7/Submit) id 47D6n3rf011595

for ryan.xiong@club22sg.com; Tue, 13 Aug 2024 06:49:03 GMT

<20240813064903.GA11593@m0314289.pops.net>

Authentication-Results: ppe-hosted.com; spf=pass smtp.mailfrom=malware4rent.org; dmarc=fail header.from=club22sg.com header.policy=reject;



Reply-To Address



DMARC Fail



Mail From

Hi Ryan,

Please take note of the latest changes in the payment method for Shipment #5689.

You must process the payment transfer to the DBS Bank Account: 095-7782506.

Best regards,

Philip Sow

The Benefits of DMARC



DMARC empowers senders to...



Gain visibility into who is sending on your behalf, what email is authenticating, what email is not and why.



Instruct email receivers on how to handle mail that does not pass authentication.



Block phishing attacks spoofing owned domains before they reach employee and consumer inboxes.



DMARC empowers receivers to...



Distinguish between legitimate senders and malicious senders.



Foster consumer loyalty and employee protection.



Improve and protect the reputation of the email channel.

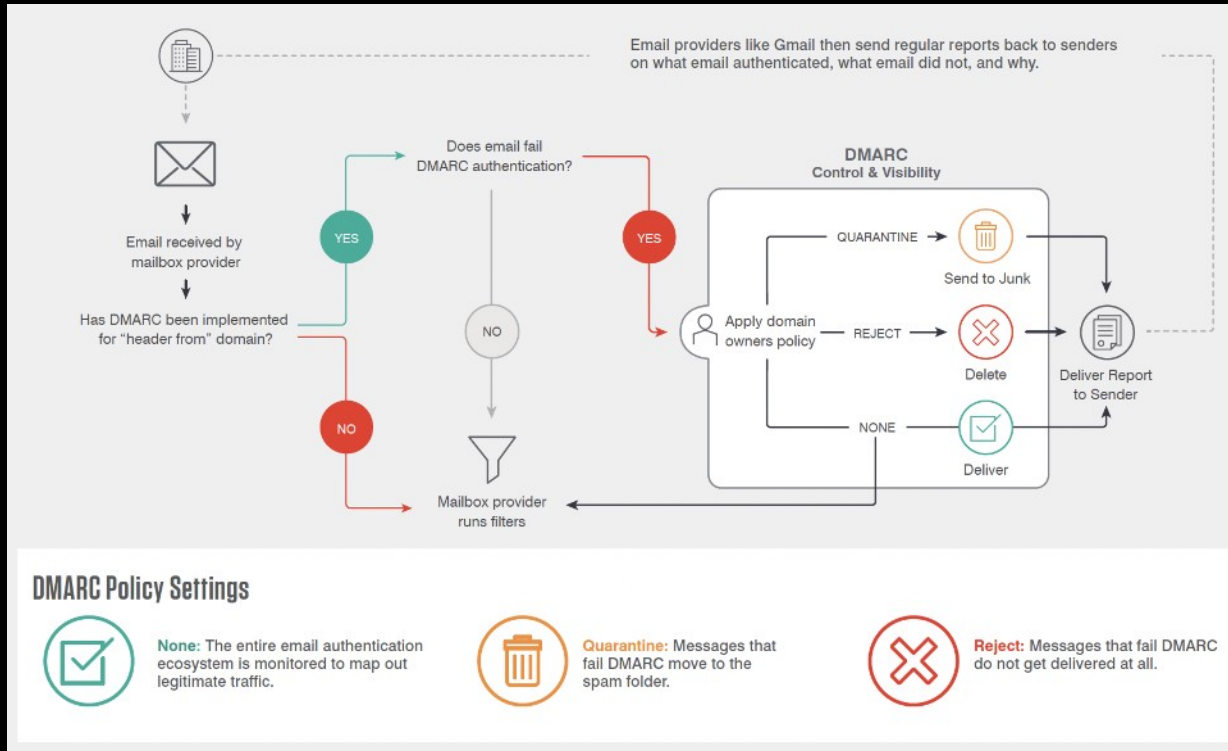
Deploying DMARC on Your Own



DMARC Quarantine vs. DMARC Reject: Which Should You Implement?

- The DMARC policy options: “**none**” “**quarantine**” and “**reject**”.
- **p=none**, which allows emails that fail to go through still
- **p=quarantine**, indicates that the recipient side should "quarantine" emails that fail DMARC, considering them to be potential spam
- **p=reject**, which instructs the recipient side to block emails that fail, and the additional bonus is completely blocked.

DMARC Report Visibility



Why Deploying DMARC on Your Own is Risky



High Risk of Blocking
Legitimate Email



Requires Deep
Expertise



Store and Render
Large Data Sets



Identify & Contact
Stakeholders



Ongoing Support
and Management

SPF Record Limit

Internet Engineering Task Force (IETF)
Request for Comments: 7208
Obsoletes: [4408](#)
Category: Standards Track
ISSN: 2070-1721

S. Kitterman
Kitterman Technical Services
April 2014

Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1

[4.6.4.](#) DNS Lookup Limits

Some mechanisms and modifiers (collectively, "terms") cause DNS queries at the time of evaluation, and some do not. The following terms cause DNS queries: the "include", "a", "mx", "ptr", and "exists" mechanisms, and the "redirect" modifier. SPF

implementations MUST limit the total number of those terms to 10 during SPF evaluation, to avoid unreasonable load on the DNS. If this limit is exceeded, the implementation MUST return "permerror".

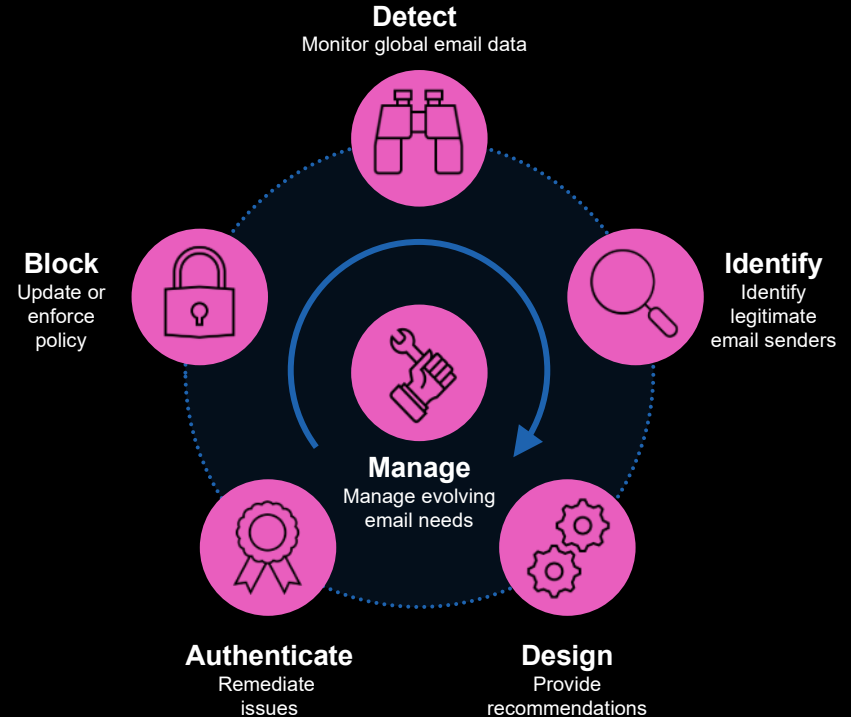
What should we expect
from a successful
implementation of Email
Authentication?



Email Authentication Service

Authenticate email being sent from your organization and coming in, to protect your employees, customers, and partners.

- **Monitor** records on all sending domains with DMARC
- **Identify** high-volume legitimate senders
- **Work** on the sender remediation processes required for the identified high-volume senders
- **Expedite** remediation steps with Hosted SPF, DKIM and DMARC



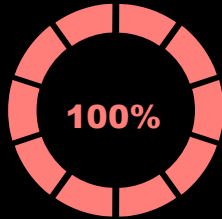
Complete **Visibility** into Your Email Traffic

Good Email Authentication Service should help you:

- **See** all emails being sent using your trusted domains, including 3rd party senders
- **Identify** suspicious emails sent on your behalf
- **Validate** sender reputation
- **Provide** insights into B2B and B2C emails sent to and from your organization

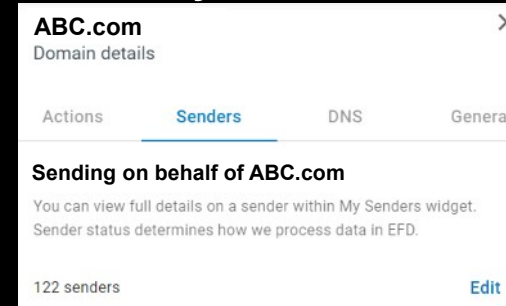
Organization Risk Insights

Domain Risk



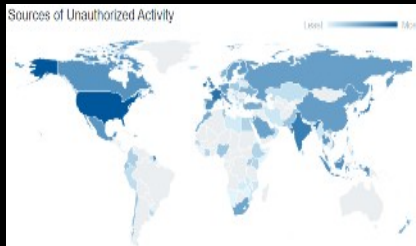
of your domains are open to all forms of Identity Deception

3rd Party Sender Risk



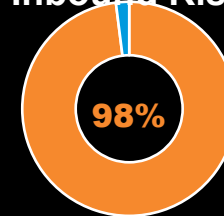
56% of Approved senders are seen failing to authenticate fully and some are being blocked

Unauthorized IP Risk to Brand



10,187 Unauthorized Emails

Inbound Risk



of your inbound email from domains with a DMARC policy of "reject" are still getting through, increasing your risk of a BEC attack.

SPF **Hosted Services** and Telemetry

Good SPF Hosted Services should help you:

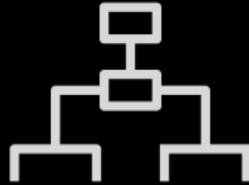
- **Overcome** the DNS lookup limit of 10
- **Reduce** overhead of making SPF updates
- **Report** Real-time propagation
- **Provide** total visibility of authorized sending IPs
- **See** which IPs are actively sending and which are not
- **Remove** inactive sending IPs can help lower a company's overall security risk

Dynamically Identify **Lookalike** Domains



SCAN

Continually scan over domains for threats



CLASSIFY

Classify and identify potential BEC domains



INVESTIGATE

Provide detailed intel around registrant info, email traffic, and web content



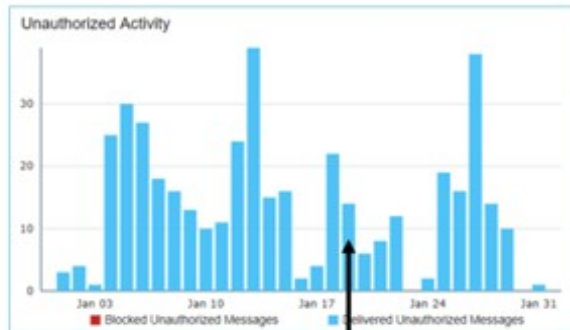
RESPOND

- Add to block list
- Limit access
- Takedown

Final Step

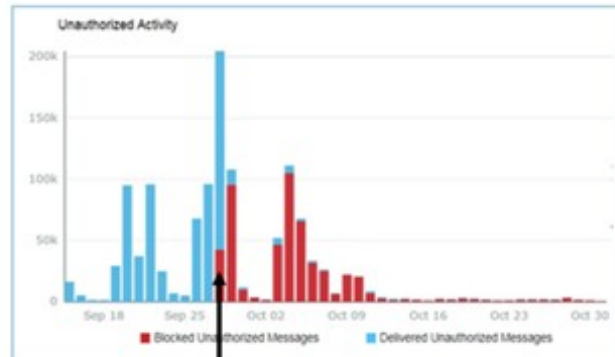
What success looks like – post ‘Reject’

(Company Info) (pre-“Reject”)



unauthorized messages delivered per day

@hmrc.gov.uk (post-“Reject”)



DMARC 'Reject' policy declared

bad actors give up 2-weeks later

Key Takeaways

- **New** Email Authentication **Requirements**
- **Sender Impersonation** comes in many forms
- Implementing the DMARC is a **Challenge**
- DMARC **Reporting Tool & Managed Service**
- Identify **Supplier Risk** & Malicious **Lookalike Domains**
- SPF **Hosted Service** and Telemetry
- **Protects Your Brand** Comprehensively



THANK YOU