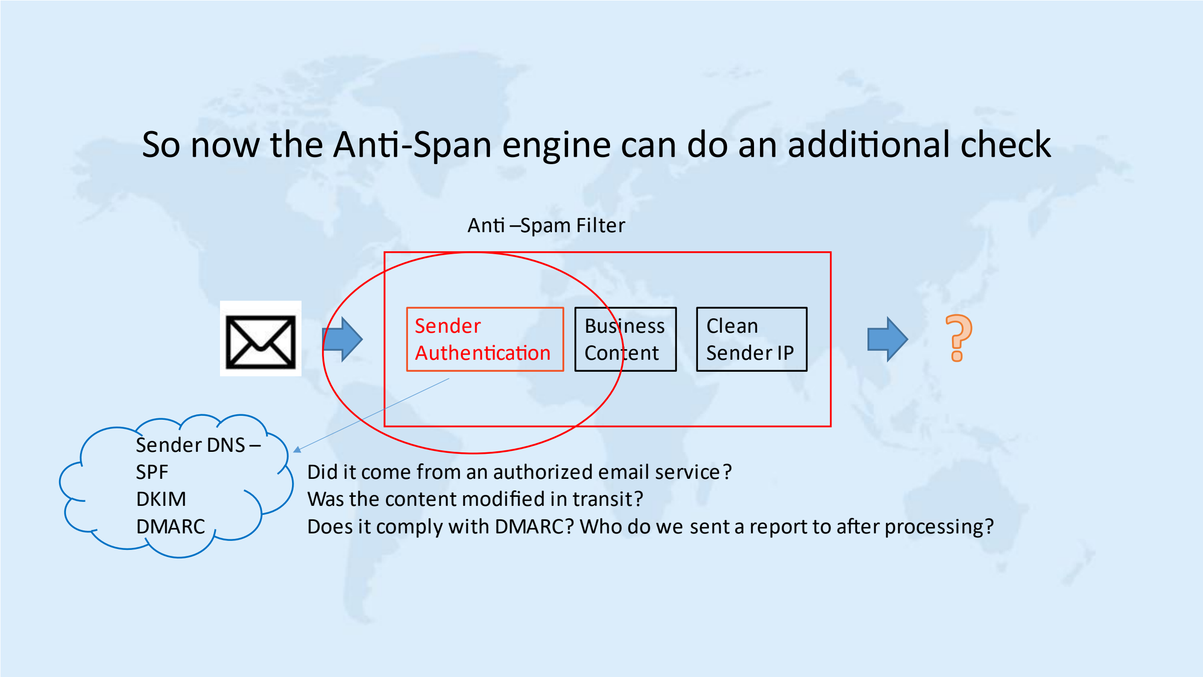
DMARC Guidance and Implementation for Microsoft 365

Executive Summary

Despite Microsoft 365 containing robust email security, there is an often-ignored section called **sender authentication** and is often not properly configured within Microsoft 365. Without **Sender Authentication**, an anti-spam engine will have one less tool to determine if an incoming mail is spoof or genuine.

Sender Authentication uses 3 protection standards, SPF, DKIM and DMARC. When properly configured and used together, they protect a Microsoft 365 domain from being impersonated and subsequently used to attack users and external parties (customers, suppliers, public)



So now the Anti-Span engine can do an additional check

Did it come from an authorized email service?
Was the content modified in transit?
Does it comply with DMARC? Who do we sent a report to after processing?

This consulting service is to help the customer to **<u>properly</u>** turn on **Sender Authentication Services** in the context of Microsoft 365, to protect both your users and external parties from impersonation attacks using your email domain name.

Correct use of DMARC requires SPF and DKIM to be correctly implemented, thus the rest of this document will generally refer to DMARC only as its implied SPF and DKIM needs to work as well.

The weakness of email and the benefits of DMARC

Email has been the most prominent aspect of the internet for well over two decades. Its importance to business has increased substantially during the same period.

Email lacks the ability to verify authenticity of all received emails. This fundamental flaw has allowed its exploitation by fraudsters and cyber criminals for malicious purposes.

DMARC is an internet based technical specification that describes how to make email easy to identify and authorise. It is widely supported by the large consumer email providers such Google, Yahoo, Outlook and AOL.

Email domains configured with DMARC can provide the following key benefits:

- Decrease and stop illegitimate use of valid domains by criminals in spam emails
- Prevent Enterprise spear phishing, and other attack variants such as CEO email fraud
- Detect misconfigurations of the underlying SPF and DKIM settings
- Inventory of all email senders using the valid email domain

Key features of the **DMARC Guidance and Implementation Service** include:

- Expert implementation advice
- Self Service portal access for reviewing all email sources and received xml reports
- Post implementation support for analysis of received data and reporting
- Best practice policy recommendations for adding additional email sources or bulk marketing/email providers.

The client is required to invest in a DMARC reporting app service in order to capture DMARC reports and implement the service correctly. We use the DMARCIAN app for this purpose.

The deliverables of DMARC Guidance and Implementation Service is to **accurately** deploy DMARC, allowing it to improve email delivery, combat fraud, and to monitor domain-wide usage of email.

DMARC – what security issue does it solve ?

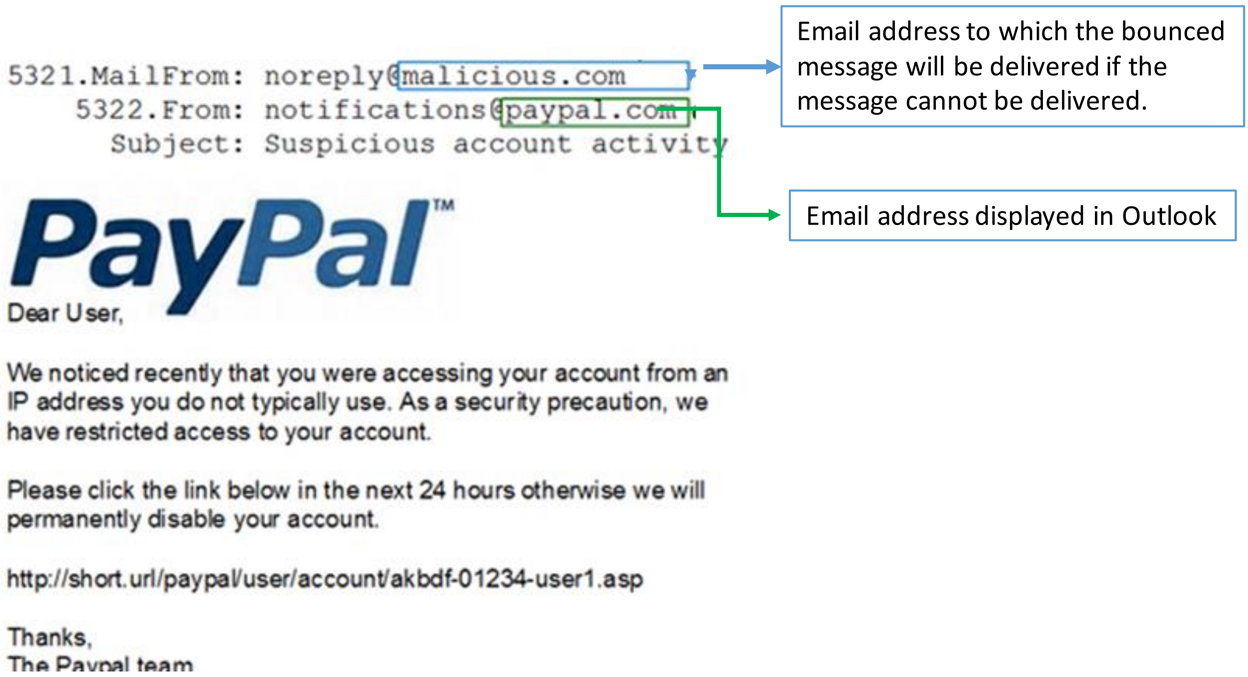
The ubiquity of e-commerce and the rise of the social internet has provided criminals a tremendous financial incentive to compromise user accounts to enable the theft of passwords, bank accounts, credit cards, and more.

Illegitimate use of email domains is called spoofing. This is made possible due to the fact that email has 2 “From” addresses:

- (RFC) 5321.Mail From - commonly referred as the envelope address or bounce email address, and
- (RFC) 5322 From – commonly referred as the display address that is displayed in the email client ie Msft Outlook

Due to this fundamental design flaw within the architecture of email, criminals have found spoofing to be a proven way to exploit user trust of well-known brands. Simply inserting the logo of a well known brand and using the brand’s email such as accounts@mybank.com into an email gives it instant legitimacy with many users.

Users can’t tell a real message from a fake one. In the diagram below, the fundamental flaw can be identified **but only by viewing the email header**. The average consumer would see this as Paypal email.



```
5321.MailFrom: noreply@malicious.com
    5322.From: notifications@paypal.com
      Subject: Suspicious account activity
```

Dear User,

We noticed recently that you were accessing your account from an IP address you do not typically use. As a security precaution, we have restricted access to your account.

Please click the link below in the next 24 hours otherwise we will permanently disable your account.

http://short.url/paypal/user/account/akbdf-01234-user1.asp

Thanks,
The Paypal team

Email address to which the bounced message will be delivered if the message cannot be delivered.

Email address displayed in Outlook

What is DMARC ?

Most organizations have deployed SPF and additionally DKIM in order to provide some level of email security and authenticity. SPF only provides protection to the 5321.MailFrom address.
Although they function well, criminals have been able to exploit a major weakness - ***they do not protect the email address that the user sees in their inbox***. Ie 5322 From address.

DMARC addresses these issues and helps email senders and receivers work together to better secure emails, protecting users and brands from painfully costly abuse.

DMARC is an internet based technical specification that describes how to make email easy to identify and authorise. **It is widely supported by the large consumer email providers such Google, Yahoo, Outlook and AOL.**

Deployment Methodology

DMARC deployment is broken into three distinct phases:

1. Assess,
2. Implement, and
3. Manage.

Assess

Phase 1 of the deployment is essentially to

- Initiate domain management function (DMF) within your organisation and make appropriate recommendations
- Identify all valid *known* domains of the organisation and determine DMARC requirement
- Implementation of DMARC is enabled for the required domains (***pass through only***)
- Check for SPF, DKIM configuration errors in Microsoft 365
- Access portal and confirm correct implementation of DMARC

Deliverables

- Initial identification of all email streams and SOW for next steps
- Domain management function review, recommendation and implementation

Implement

Following the initial implementation of DMARC, a period of review occurs to

- Monitor and Identify all email streams across period
- Ensure all email streams - vendors and partners, comply with your DMARC policy
- Investigate all unknown streams and either add them as valid or take action to remove them
- Correct any SPF, DKIM errors in Microsoft 365

Deliverables

- Clearly identify ALL email streams
- Define, deploy and monitor initial **SPF record**
- Impact Assessment reports before policy changes from pass through to quarantine to reject

Manage

- Comprehensive view of all valid email senders that utilise your email domains
- Documented domain management function that ALL departments adhere to
- Change control process to add/remove authorised senders
- Monthly reporting

Deliverables – Quarterly activity reporting and ensure domain management function maintains the accuracy of DMARC deployment and ensures all email streams remain DMARC compliant.

Pricing Formula

Pricing of the service depends on the following:

1. Complexity of the customer's email domains that it wants to protect and that may include.
   a. Primary domains and sub-domains associated with work emails.
   b. Domains associated with marketing and other emails.
   c. Amount of authorized and unauthorized impersonations happening prior to implementation.
   d. Other factors that may increase or lessen effort required.
2. Reporting Tool subscription cost that is based on:
   a. Number of domains to monitor.
   b. Number of emails, per month, that is being sent externally.
   c. Other features required as found in https://dmarcian.com/pricing/

Notes :

1. This is an advisory service to help customer to implement DMARC
2. Customer contact Fedelis and Dmarcian for advice during the contract term for advice and consultation over the implementation and best practices of the DMARC standard.
3. The advisory will provide guidance to identify email sources and compliance issues, guidance in fixing these issues, and ultimately move to -quarantine- or -reject- setting in DMARC
4. The service concludes by providing quarterly DMARC analysis reports from the DMARCIAN dashboard, for customer to monitor for issues and DMARC compliance.
5. This excludes actual service to configure SPF, DKIM and DMARC, which can be done by customer's internal IT team, and also the respective email product vendors including email hosts, marketing, survey and monitoring services that send out email on behalf of customer.