DMARC FAQ

What does DMARC protect against?

- Spoofing and Phishing

What risks are associated with implementing DMARC?

- If DMARC us implemented incorrectly, the policy will drop legitimate mail messages. It is important to start the policy at the lowest level (None) and move to the highest level (Reject) once all legitimate mail message issues are resolved.

Why is DMARC needed?

(DMARC.org - https://dmarc.org/wiki/FAQ#Why_is_DMARC_needed.3F)

End users and companies all suffer from the high volume of spam and phishing on the Internet. Over the years several methods have been introduced to try and identify when mail from (for example) IRS.GOV really is, or really isn't coming from the IRS. However:

- These mechanisms all work in isolation from each other
- Each receiver makes unique decisions about how to evaluate the results
- The legitimate domain owner (e.g. IRS) never gets any feedback

DMARC attempts to address this by providing coordinated, tested methods for:

- Domain owners to:
  - Signal that they are using email authentication (SPF, DKIM)
  - Provide an email address to gather feedback about messages using their domain – legitimate or not
  - A policy to apply to messages that fail authentication (report, quarantine, reject)
- Email receivers to:
  - Be certain a given sending domain is using email authentication
  - Consistently evaluate SPF and DKIM along with what the end user sees in their inbox
  - Determine the domain owner's preference (report, quarantine or reject) for messages that do not pass authentication checks
  - Provide the domain owner with feedback about messages using their domain

A domain owner who has deployed email authentication can begin using DMARC in "monitor mode" to collect data from participating receivers. As the data shows that their legitimate traffic is passing authentication checks, they can change their policy to request that failing messages be quarantined. As they grow confident that no legitimate messages are being incorrectly quarantined, they can move to a "reject" policy.

Why is it discouraged to start the policy at Quarantine or Reject?

Companies often have complex mail systems with several mail servers that are authorised to send, as well as third parties that can send on behalf of the domain. If these are forgotten in the DMARC record, then legitimate mail will end up in spam or be dropped entirely. Therefore, it is best to start at None and monitor the reports, and then gradually move up to Reject.

Should I configure DMARC for domains which don't send any mail?

If you have domains that don't send mail, but customers regularly see them (for example, a web domain that customers visit) it is best to configure DMARC to not allow any mail from that domain. This is because customers will likely trust an email that seems to come from a website that they visit regularly.

Do I need to configure DMARC if I'm using a service like Office 360 or G Suite?

Yes, you will still need to configure SPF, DKIM and DMARC. These services and others offer DMARC reporting, but that does not mean that DMARC is automatically configured for domains using these for email.

How can I view the reports in a human readable way?

Tools such as DMARCian and onDMARC can provide a comprehensive breakdown of what has happened in each report

What email address should I use for reporting?

It is recommended that you set up a new email address specifically for receiving the reports. This helps prevent your main inbox from becoming too cluttered and helps to integrate with various DMARC analytics services.

How can I find my organisations mail server?

You can find the name of your organisations SMTP server by using the command line tool "nslookup". By typing "nslookup" into the terminal, and then "set type=mx", then your domain name you can find a list of all SMTP servers associated with that domain.