**A Brief Overview – Configuring DMARC**

**Introduction:**

* The purpose of DMARC is as a means to prevent email fraud.
* This is achieved by creating a DMARC record.
* This is a DNS TXT record which contains a directive to a recipient email server, receiving mail for the domains which DMARC is configured on.
* This directive is to either ignore, quarantine, or reject mails which fail DMARC checks. Rejection is preferred, being the stricter directive, and will be used in the guide below.
* This directive can be ignored by the recipient mail server, but this is uncommon in a correctly configured mail security solution
* To pass DMARC checks, a mail must either contain a valid DKIM key, or have been sent (and align to) a mail system included in an SPF record.
* The goal in configuring DMARC, is:
  + To ensure that all valid services sending mail on behalf of a domain are verified using DKIM and SPF
  + To ensure that all unauthorized mail senders are unable to imitate (spoof) the domain.

**Basic Configuration:**

1. Decide on a solution which you would want to receive DMARC reports. Valimail is free for Office 365 users, and Cloudflare has a built-in solution, if your domain nameservers are configured there.
2. Create a DNS TXT record  
   This puts DMARC into report-only mode.
   1. Name: *\_dmarc*
   2. Content: *“v=DMARC1; p=none; rua=mailto:****example@dmarcreports.com****;”*
      1. Replace the red text with the email address the solution from step one provides.
3. Within 24 – 48 hours, DMARC aggregate reports should start being received by the solution from step one. This will need to be monitored for some time. Weekly checkups are recommended.
   1. If you see any valid email services reported as failing DMARC, configure SPF and DKIM for those services, and check back in a week.
   2. If you see any unrecognized email senders, it is highly likely that a malicious party is spoofing your domain
   3. If all valid email services are reporting as passing DMARC after 2 – 4 weeks, the DMARC record can be updated to:  
      v=DMARC1; p=reject; sp=reject; rua=mailto:example@dmarcreports.com;  
      At this point, DMARC is enforced, and your domain is protected.
4. To maintain compliance with your DMARC policy, any new email services you use will need to be configured with SPF and/or DKIM
5. It is good practice to check up on DMARC reports on a regular basis
   1. Weekly after making changes to DMARC policy
   2. Monthly once you’re confident that all valid mails are passing DMARC compliance checks.