Configuring Domain Fraud Protection with Barracuda

https://campus.barracuda.com/doc/90443238/

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email-validation system designed to detect and prevent email spoofing. It can be used to defend against certain types of email attacks, including phishing and email spam. In these types of attacks, the email sender's address is forged, but the email itself appears to be legitimate. DMARC attempts to counter the illegitimate usage of the exact domain name in the From: field of email message headers. If you have DMARC enabled and other organizations are recognizing DMARC, then your domain cannot be spoofed in phishing attempts, thereby protecting the reputation of your domain.

A DMARC policy allows a sender's domain to indicate that their emails are protected by Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) or both. The DMARC policy instructs receivers as to what to do if neither of those authentication methods passes (for example, rejecting the message). DMARC makes explicit how to handle these types of failed messages. DMARC policies are published in the public Domain Name System (DNS).

To ensure the sender trusts this process, receiving mail servers send daily aggregate reports indicating how many emails have been received and if these emails passed SPF, DKIM, or both and were aligned. The sender can examine any failed IP addresses and identify the domains responsible for distributing fraudulent email. For more detailed information, see Step 2 - Working with Email Sources.

> Note that when you first configure DMARC, it is in Reporting Mode only – it reports issues but does not protect against them.

The complete process of enabling DMARC enforcement includes the following three steps: