What is DMARC (Domain-based Message Authentication, Reporting and Conformance)?

Tell Me

1. Here’s the simply definition: DMARC is an industry standard used to validate email senders and ensure that an email meets authentication requirements.
2. Here’s the complicated definition:
   a. DMARC stands for Domain-based Message Authentication, Reporting & Conformance.
   b. It is an email authentication, policy, and reporting protocol.
   c. It uses the Secure Policy Framework (SPF records) and DKIM (Domain Key Identified Mail) protocols.
3. DMARC is designed to detect and prevent email spoofing.
4. DMARC helps combat phishing and email spam.
5. DMARC has been adopted by UNC Charlotte.
6. See this FAQ for why DMARC is important.
7. See this FAQ about DKIM.
8. See this FAQ about testing for DMARC compliance.

Related FAQs

- How do I make sure mass email messages from 3rd party vendors will not be blocked or flagged as SPAM?
- Why is DMARC important?
- What is DMARC (Domain-based Message Authentication, Reporting and Conformance)?
- What is DKIM (Domain Key Identified Mail)
- How do I test for DMARC compliance when I am working with a third party vendor to send mass emails from an @uncc.edu account?