DMARC (Domain based Message Authentication, Reporting and Conformance)

Introduction

> DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol. It is designed to give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing. The purpose and primary outcome of implementing DMARC is to protect a domain from being used in business email compromise attacks, phishing emails, email scams and other cyber threat activities. source

Description

The owner of a domain can, by means of a DNS record, publish a policy that states how to handle e-mail (deliver, quarantine, reject) which is not properly authenticated using SPF (Sender Policy Framework) and/or DKIM (DomainKeys Identified Mail).

Read More

Example

As an example, `swigg.net` is setup with the following DNS record.

Domain	Type	Value

_dmarc	TXT	v=DMARC1; p=quarantine; rua=mailto:dustin@swigg.net; ruf=mailto:dustin@swigg.net; sp=quarantine; ri=86400

This rule can be read as telling MTA (Mail Transfer Agents) the following.

Component	Description
p=quarantine	treat mail that fails DMARC check as suspicious
rua=mailto:dustin@swigg.net	send aggregated reports to `dustin@swigg.net`
ruf=mailto:dustin@swigg.net	send forensic reports to `dustin@swigg.net`
sp=none	treat mail that fails DMARC check as suspicious for subdomains
ri=86400	send reports every 24 hours (86400 seconds)

Revision #3
Created 29 October 2020 18:39:59 by dustin@swigg.net
Updated 2 April 2021 14:04:16 by dustin@swigg.net