DMARC

DMARC requires SPF & DKIM to be setup first for most effect

DMARC Deployment Checklist

7 December 2015

- 0
- 0

If you're at a large organization looking to deploy DMARC, view the video on dmarcian's deployment process. It's worth your time!

Here's a checklist you can use to get DMARC into place:

- Create a list of your domains.

Publish DMARC records to collect data for each of your domains.

- If you've created a dmarcian.com account, log in and view the instructions on how to publish a DMARC record.
- If you don't have a dmarcian account, create one because they're free.
- To roll your own DMARC record, this free tool is works great.

- Wait for data to roll in. DMARC report generators operate on a 24 hour cycle, and so you might as well check back in a day or two, or make yourself a really huge pot of coffee.
- Look at your DMARC reports to figure out what you need to do next.
  - dmarcian's Domain Overview does this work for you.
  - Or, learn how to interpret DMARC's XML reporting format. This route is no fun.
- Depending on who is sending your legitimate email, bring your sources of email into compliance with DMARC.
  - Capabilities of sources range from "easy" to "some setup required" to "difficult".
  - dmarcian tracks the capabilities of email sources to allow dmarcian users to quickly zero in on changes that need to happen.

    - DMARC uses SPF and DKIM to make email easy to identify. (A short video about SPF, and one for DKIM.)
- As each domain becomes compliant with DMARC to your satisfaction, you can put in place controls to disallow unauthorized use of your domain.
- You're done. Continue to monitor for DMARC compliance. When you get a new domain, just put it through these steps to maintain 100% DMARC compliance.

From <https://dmarcian.com/dmarc-deployment-checklist/>

Revision #2
Created 23 December 2023 04:13:50 by ColtM
Updated 7 August 2024 23:24:40 by ColtM