Domain-Based Message Authentication, Reporting and Conformance

Domain-Based Message Authentication, Reporting and Conformance (DMARC) is an email authentication policy that protects against bad actors using fake email addresses disguised to look like legitimate emails from trusted sources. DMARC makes it easier for email senders and receivers to determine whether or not an email legitimately originated from the identified sender. Further, DMARC provides the user with instructions for handling the email if it is fraudulent.

Why should State and Local Election Officials be interested in DMARC?

State and local election officials face a high volume of spam and phishing attacks on their internet accessible systems. Fraudulent emails are easy to design and cheap to send, which provides malicious actors incentive to use repeated email attacks. Unfortunately, employees are often the point of failure for these attacks, when they are forced to repeatedly determine whether emails are legitimate or fake. DMARC provides an automated solution to this issue, making it easier to identify spam and phishing messages before they ever reach an employee's inbox.

How does DMARC work?

DMARC removes guesswork from the receiver's handling of failed emails, limiting or eliminating the user's exposure to potentially fraudulent and harmful messages. A DMARC policy allows a sender to indicate that their emails are protected by Sender Policy Framework (SPF) and/or Domain Keys Identified Message (DKIM), both of which are industry-recognized email authentication techniques. DMARC also provides instructions on how the receiver should handle emails that fail to pass SPF or DKIM authentication. Options typically include sending the email to quarantine or rejecting it entirely. Lastly, DMARC provides the receiver with an email address to provide feedback to the sender. Potential feedback can include that the sender's email was rejected/quarantined by the receiver or that a bad actor is attempting to imitate the sender's domain.

How can I adopt DMARC on my Domain?

Adopting DMARC is not a seamless transition and will require IT departments to work with non-technical employees to ensure that everyone is receiving the messages they need. Below are a number of steps organizations can take to ease into DMARC over time.

1. Deploy DKIM & SPF. You have to cover the basics first.
2. Ensure that your mailers are correctly aligning the appropriate identifiers.
3. Publish a DMARC record with the "none" flag set for the policies, which requests data reports.
4. Analyze the data reports and modify your mail streams as appropriate.
5. Modify your DMARC policy flags from "none" to "quarantine" to "reject" as you gain experience.