Implementing DMARC in the Federal Government

The key to eliminating phishing and safeguarding email communication

What is DMARC?

DMARC (Domain-based Message Authentication Reporting & Conformance) is an open email authentication protocol, established in 2012 by organizations including Google, Microsoft, Agari, PayPal, and others to protect the email channel. DMARC is the best way for email senders and receivers to determine whether or not a given message is legitimately from the sender, and what to do if it isn't.

"For 95% of breaches, email is the means of communication to the target."

Verizon Data Breach Digest 2017

"Phishing...continue[s] to present threats to both the federal government and public at large"

US Federal Information Security Management Act (FISMA)

Government agencies nationwide already adopting DMARC

U.S. Customs and Border Protection

THE PROBLEM

Email is the #1 way attackers target citizens and government employees.

WHY IT WORKS

Email lacks built-in authentication: Attackers can easily spoof or impersonate anyone in your organization using free tools

Attackers need to be right just once: With billions of emails hitting government inboxes, odds are in the attacker's favor

Email gateways can't solve the problem: Attackers rely on social engineering tactics and identity deception, not malicious content or URLs that traditional tools were built to detect

THE SOLUTION

DMARC functions like an 'identity check' for your agency. It prevents spammers and criminals from hijacking your valid organization domain names and brand for email.

.

BENEFITS OF DEPLOYING DMARC FOR YOUR AGENCY

Stop email phishing attacks using your agency's reputation: Agencies reduce the likelihood that their domains and brand will be used in an attack.

Reduce account takeover risk: By preventing delivery of phishing and malware-laden messages directed at your employees or constituents, you can reduce the number of account takeovers.

Increase email deliverability: By deploying DMARC, you ensure that legitimate email from your agency gets delivered and not blocked at the receiver.

Gain visibility Into cyberattack risk: Do you know every 3rd party company sends email on behalf of your agency? DMARC provides this critical visibility, allowing you to ensure that anyone sending on your behalf complies with email best practices.

THE FEDERAL PERSPECTIVE

Fact: **The Department of Homeland Security (DHS)** has mandated adoption of DMARC on all government agency email domains by January 14th, 2018. BOD 18-01 (https://cyber.dhs.gov/)

Fact: DMARC (and email authentication) is evolving into a key metric that impacts the **FISMA** scorecard against your agency.

Fact: **NIST** recommends using DMARC authentication tools to provide protection against phishing (SP 800-177, Trustworthy Email, Section 4.6).

A DMARC PRIMER

What Steps Does My Agency Need to Take to Use DMARC?

Implement Authentication Standards

The DMARC protocol builds on existing standards like Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM).

Authorize/Validate Approved Senders

You need to understand and authenticate all legitimate email messages and sources for your email-sending domains, including owned and third party domains. For example, it is crucial to ensure you don't block legitimate mail, such as communication from email service providers, such as sendgrid, that send on your behalf.

Set DMARC Enforcement Policy

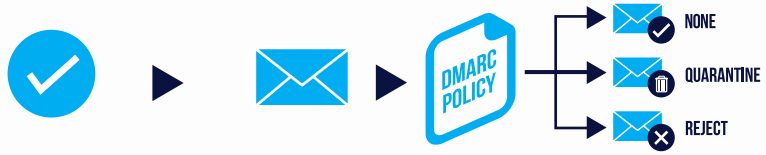
This is a key milestone in the DMARC journey. Publishing an explicit policy tells mailbox providers what to do with email messages that are determined not to be legitimate. This is how you can block all fraudulent emails before they reach employees, constituents, and citizens at large.

What is a DMARC Enforcement Policy?

When you set a DMARC policy for your agency you, as an email sender, are indicating that your messages are protected. The policy tells a receiver what to do if one of the authentication methods in DMARC passes or fails.

How it Works

When emails are received by the mailbox provider, the receiver checks if DMARC has been activated for your domain.



If **YES**, it checks if the email fails DMARC authentication.

If email fails DMARC verification, the control and visibility features of DMARC kick in, and the domain owner's policy is applied.

POLICIES:

1. If the policy is none, then the mail is delivered, and the mailbox providers run filters. However, statistics are still being compiled.
2. If quarantine, it sends email to junk folder.
3. If reject, email gets deleted and the end recipient never sees it.

If it returns a **"NO"** the mailbox provider runs its filters and email are allowed to continue on without any authentication.

What Does a DMARC Policy Look Like?

Here's a typical policy in DNS. Note that this domain is configured with a policy of "reject"

DMARC record for **agari.com**

```
v=DMARC1; p=reject; sp=reject; ri=3600; rua=mailto:agari-data@rua.agari.com;
ruf=mailto:agari-data@ruf.agari.com; fo=1
```

How Do I Get Visibility and Reporting from DMARC?

Once you DMARC is implemented, you will start to to receive thousands of reports every day, depending upon the number of emails your organization sends. Because it's difficult to process the reports manually (they are in XML format) you can work with a commercial vendor to display and process the data. Commercial vendors can help with DMARC implementation and 3rd party sender identification and alignment as you embark on your DMARC journey.

For more information on DMARC, visit https://dmarc.org/