M³AAWG DMARC Training Series

Mike Adkins, Paul Midgen
DMARC.org
October 22, 2012
# M³AAWG DMARC Training Videos

(2.5 hours of training)

This is Segment 1 of 6
The complete series of DMARC training videos is available at: [https://www.m3aawg.org/activities/maawg-training-series-videos](https://www.m3aawg.org/activities/maawg-training-series-videos)

<table>
<thead>
<tr>
<th>Segment 1</th>
<th>Segment 2</th>
<th>Segment 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is DMARC? (about 20 minutes)</td>
<td>DMARC Identifier Alignment (about 20 minutes)</td>
<td>DMARC Policy Records (about 30 minutes)</td>
</tr>
<tr>
<td>Segment 4</td>
<td>Segment 5</td>
<td>Segment 6</td>
</tr>
<tr>
<td>DMARC Reporting (about 15 minutes)</td>
<td>DMARC Information for Mailbox Providers (about 20 minutes)</td>
<td>DMARC Information for Domain Owners and 3rd Parties (about 40 minutes)</td>
</tr>
</tbody>
</table>

M³AAWG 26th General Meeting | Baltimore, October 2012
What is DMARC?
DMARC Segment 1 – about 20 minutes

Mike Adkins, Paul Midgen, DMARC.org
October 22, 2012
Outline

Part 1

• Introduction to DMARC
  • Purpose and Goals
  • History
  • Roadmap

• DMARC Spec Overview
  • Identifier Alignment
  • DMARC Policy Records
  • Reporting

• Short Break

Part 2

• Information for Domain Owners
  • The Reporting and Compliance Process
    • Initial Record Publishing
    • 3rd Party Deployment Profiles
    • Report Processing and Analysis
    • Initial Policy Ramp-up
    • Ongoing Monitoring

• Information for Mailbox Providers
  • DMARC Policy Enforcement
  • Aggregate Reporting
  • Forensic Reporting

M3AAWG 26th General Meeting | Baltimore, October 2012
Things we won’t cover

- Why phishing is a problem.

- How DKIM, SPF, DNS, SMTP, or XML work.

- How to combat abuse of cousin domains or the display name field.

- Phishing website investigation or takedown services.
Who is in the audience?

• Mailbox providers?
• Domain owners?
• Domain owners who use 3rd party senders?
• 3rd party senders (ESPs, hosting providers, etc)?
Intro to DMARC

DMARC = Domain-based Message Authentication, Reporting, and Conformance

• Authentication – Leverage existing technology (DKIM and SPF)

• Reporting – Gain visibility with aggregate and per-failure reports

• Conformance – Standardize identifiers, provide flexible policy actions
Intro to DMARC – Purpose and Goals

• Open version of existing private mechanisms for preventing domain spoofing.

• Standardize use of authenticated identifiers.

• Provide insight into and debugging aids for your authentication practices.

• Incent wider adoption of SPF & DKIM.

• Encourage iteration toward aggressive authentication policy.
Intro to DMARC – Non-Goals

• Address cousin domain abuse
• Address display name abuse
• Provide MUA treatment advice
• An enterprise security solution
• An incident response tool
• Provide delivery reporting
Intro to DMARC - History

- Private Prototype between Paypal and Yahoo – 2007
- Vendors being offering similar functionality – 2009 to present
- First Prototype DMARC records published - Feb '11
- Draft specification released - Jan 30th 2012, revised April ‘12
Intro to DMARC - Roadmap

• Interop Event - July '12

• Produce a final draft

• Submit to the IETF
This has been the first of six DMARC video segments

View the entire

**M³AAWG DMARC Training Series**

from the public training video pages on the M³AAWG website at: https://www.m3aawg.org/activities/maawg-training-series-videos

Our thanks to Michael Adkins, Paul Midgen and DMARC.org for developing the material in this series and allowing M³AAWG to videotape it for professionals worldwide.

This video is presented by the

Messaging, Malware and Mobile Anti-Abuse Working Group
For information about M³AAWG:
www.m3aawg.org
www.facebook.com/maawg
www.twitter.com/maawg
www.youtube.com/maawg

Contact us at:
https://www.m3aawg.org/contact_form