2016 Online Trust Audit
Email Authentication Practices
Deep Dive & Reality Check

July 20, 2016

Craig Spiezle
Executive Director
Online Trust Alliance
https://otalliance.org/DMARC

Industry Panel

Mike Jones
Director, Product Management, Agari

Rob Holmes
General Manager, Fraud Protection, Return Path

Alexander García-Tobar
CEO, ValiMail

Jeff Wilbur
VP Marketing, Iconix
VP Research, Online Trust Alliance
Why Care?

- Rise in phishing attacks, precision, variety of methods
- Entry point for >90% of breaches

Honor Roll Overview

- Audit of 1,000 web sites
  - Internet Retailer Top 500
  - FDIC Banking 100
  - Top 100 Consumer Services
  - Top 100 News/Media
  - Top 50 Federal Gov’t
  - OTA Members

- Scoring
  - 100 baseline points for each category
  - Weighted composite analysis, ~50 criteria
  - Bonus points for emerging practices
  - Penalty points for
    - Vulnerabilities, privacy practices, data loss incident & fines/settlement
  - Honor Roll = 80% of total points, 55% or better in each category
Summary of Failures

OVERALL REASONS FOR FAILURE

- **CONSUMER PROTECTION**: 27%
- **SITE SECURITY**: 10%
- **PRIVACY**: 16%

- **Primary cause(s) of failure** –
  - Consumer protection – lack of DKIM at top-level domain
  - Site security – use of old ciphers, lack of latest protocol
  - Privacy – broad data sharing, many trackers that share data
- Sites can fail in more than one area

Consumer Protection

- **Base points**
  - Email authentication
    - SPF and DKIM at top-level and subdomains *(increased weight for TLD)*
  - DMARC record and policy
  - DMARC reject/quarantine
    - *(Increased weight for reject)*

- **Bonus points**
  - TLS for email
  - DNSSEC
  - IPv6

- **Penalty points**
  - Domain locking (not locked)
  - Malvertising incident in last year

*Italics = new for 2016*

- Can the app or website be spoofed, fooling a person to open/download an update, open an attachment or simply open an email with a drive-by exploit?
- Does the site or app exercise best practice to help prevent brand-jacking and domain abuse?
Email Authentication Overview

- **SPF**: *Path-based*. Sender publishes list of authorized servers. Email receiver checks if server is authorized to send for domain.

- **DKIM**: *Signature-based*. Sender inserts signature into email. Email receiver checks signature regardless of source.

- **DKIM+SPF** = Resilient email authentication infrastructure

Leveraging SPF and DKIM

**SPF**
- **Authenticates Message Path**
- Authorized senders in DNS

**DKIM**
- **Authenticates Message Content**
- Public encryption keys in DNS

**DMARC**

- **Consistency**: A method to leverage the best of SPF and DKIM
- **Policy**: Senders can declare how to process unauthenticated email
- **Visibility**: Reports on how receivers process received email
- **Aggregated Insights**: Telemetry into mail streams (RUA)
- **Failure & Spoofed email reports** (RUF)
Overall Adoption Trends

- Steady growth over time, exceeding 80% in many areas

2016 Snapshot by Sector

- Aids in protection from social engineering exploits including spearphishing & ransomware
- Overall adoption continues to rise, but still lacking at TLD
Reality Check

- Shows percent of organizations that support both SPF and DKIM at the TLD and have a DMARC record with a “reject” or “quarantine” policy
- Highlights need for increased focus across organizational “silos” to protect consumers, employees and brands

Top Sites Protecting Their Brand
Stumbling Blocks

- Lack of awareness of value
- Risk tolerance
- Organizational disconnects / ownership
- Technical knowledge

Common Mistakes – SPF & DKIM

General - Incomplete authentication

SPF
- Overly broad references in the record
- Exceeding the limit of 10 DNS queries
- Typos or syntax errors (e.g., ipv4 instead of ip4)
- Use of “?all” or “+all”
- Referencing records that are missing or ambiguous
- Multiple SPF records for the same domain
- Not publishing SPF for subdomains (SPF does not propagate to subdomains)

DKIM
- Truncated DKIM records or bad characters in the key
- Key management (e.g., key rotation, key length, signing with the wrong key, etc.)
- Signing at the wrong point in the mail flow (e.g., signing at an internal hop before an outbound gateway modifies content)
- Email Service Providers adding a second DKIM signature

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=mail.mail.com; s=google; b=VQxhu613umJFZiNM8R0v32gbv3yQMtD8o2pmOz9tPgR5v5x1+ UrDAfj1qJrhCr0 punish9jD/3LjxWM8+eJb/k2l6Xc/...
Common Mistakes – DMARC

• Typos or syntax errors
  ▫ Incorrect tag delimiters
  ▫ Use of "_"
  ▫ p=monitor instead of p=none

• Publishing a p=none with no RUA or RUF address

• Inappropriate use of sp=none

• Publishing unspecified or incorrect RUA/RUF domains/addresses

• Publishing multiple addresses in RUA/RUF tags

• Publishing a record without an understanding of what to do with feedback data

_dmarc.returnpath.com. 600 IN TXT
"v=DMARC1; p=reject; fo=1; rua=mailto:dmarc_agg@auth.returnpath.net; ruf=mailto:dmarc_afrf@auth.returnpath.net; rf=afrf; pct=100"

Other Considerations

• Inbound protection

• Protecting “parked” or non-emailing domains

• Dealing with third parties

• Managing changes

• Low volume senders/departments

• Ongoing monitoring
What Now?

- Self-assessment – inventory, stakeholders, etc.
- Get help – OTA, industry resources
- Build a business case
- Implement and put processes in place

Tools & Resources

OTA
- Email Security  https://otalliance.org/eauth
- DMARC  https://otalliance.org/dmarc
- Resources  https://otalliance.org/eauth/resources
- TLS  https://otalliance.org/tls
- Online Trust Audit & Honor Roll  https://otalliance.org/HonorRoll
- Contact  admin@otalliance.org  +1 425-455-7400

OTA Members
- Agari  https://www.agari.com/resources/
- Dmarcian  https://dmarcian.com/
- Return Path  https://www.returnpath.com/StopEmailFraud/
- ValiMail  http://www.valimail.com/
## SPF Adoption

**CONSUMER PROTECTION**

**SPF ADOPTION**

<table>
<thead>
<tr>
<th></th>
<th>2013 Top Level Domains</th>
<th>2014 Top Level Domains</th>
<th>2015 Top Level Domains</th>
<th>2016 Any SPF</th>
<th>2016 Top Level Domains</th>
<th>2016 Any SPF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Retailer Top 100</td>
<td>77%</td>
<td>78%</td>
<td>85%</td>
<td>94%</td>
<td>80%</td>
<td>96%</td>
</tr>
<tr>
<td>Internet Retailer Top 500</td>
<td>69%</td>
<td>75%</td>
<td>77%</td>
<td>89%</td>
<td>78%</td>
<td>93%</td>
</tr>
<tr>
<td>FDIC 100</td>
<td>62%</td>
<td>68%</td>
<td>73%</td>
<td>87%</td>
<td>77%</td>
<td>91%</td>
</tr>
<tr>
<td>Federal 50</td>
<td>60%</td>
<td>62%</td>
<td>70%</td>
<td>80%</td>
<td>80%</td>
<td>94%</td>
</tr>
<tr>
<td>Consumer 100</td>
<td>94%</td>
<td>94%</td>
<td>92%</td>
<td>92%</td>
<td>92%</td>
<td>95%</td>
</tr>
<tr>
<td>News 100</td>
<td>-</td>
<td>58%</td>
<td>62%</td>
<td>80%</td>
<td>81%</td>
<td>93%</td>
</tr>
<tr>
<td>OTA Members</td>
<td>98%</td>
<td>95%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

- Overall SPF grew in most sectors (especially Fed, News)
- SPF at TLD grew in nearly all sectors – big jumps in News, Fed; dip in top 100 retailers
- Retailers, banks, Fed and News sites still have room for improvement

## DKIM Adoption

**CONSUMER PROTECTION**

**DKIM ADOPTION**

<table>
<thead>
<tr>
<th></th>
<th>2013 Top Level Domains</th>
<th>2014 Top Level Domains</th>
<th>2015 Top Level Domains</th>
<th>2015 Any DKIM</th>
<th>2016 Top Level Domains</th>
<th>2016 Any DKIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Retailer Top 100</td>
<td>26%</td>
<td>33%</td>
<td>31%</td>
<td>93%</td>
<td>39%</td>
<td>96%</td>
</tr>
<tr>
<td>Internet Retailer Top 500</td>
<td>18%</td>
<td>27%</td>
<td>27%</td>
<td>83%</td>
<td>38%</td>
<td>89%</td>
</tr>
<tr>
<td>FDIC 100</td>
<td>30%</td>
<td>27%</td>
<td>30%</td>
<td>68%</td>
<td>40%</td>
<td>71%</td>
</tr>
<tr>
<td>Federal 50</td>
<td>22%</td>
<td>20%</td>
<td>28%</td>
<td>50%</td>
<td>30%</td>
<td>58%</td>
</tr>
<tr>
<td>Consumer 100</td>
<td>62%</td>
<td>56%</td>
<td>56%</td>
<td>78%</td>
<td>76%</td>
<td>90%</td>
</tr>
<tr>
<td>News 100</td>
<td>-</td>
<td>14%</td>
<td>16%</td>
<td>64%</td>
<td>50%</td>
<td>77%</td>
</tr>
<tr>
<td>OTA Members</td>
<td>58%</td>
<td>73%</td>
<td>78%</td>
<td>94%</td>
<td>93%</td>
<td>99%</td>
</tr>
</tbody>
</table>

- “Any DKIM” grew in all sectors, with large jumps in Consumer, News
- DKIM at TLD grew significantly in nearly all sectors, but still lags “Any DKIM” by 38% overall
## DMARC Adoption

### DMARC ADOPTION

<table>
<thead>
<tr>
<th></th>
<th>2013 Record</th>
<th>2014 Record</th>
<th>2015 Record</th>
<th>2016 Record</th>
<th>R or Q*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Retailer Top 100</td>
<td>5%</td>
<td>15%</td>
<td>20%</td>
<td>30%</td>
<td>17%</td>
</tr>
<tr>
<td>Internet Retailer Top 500</td>
<td>3%</td>
<td>6%</td>
<td>8%</td>
<td>21%</td>
<td>14%</td>
</tr>
<tr>
<td>FDIC 100</td>
<td>13%</td>
<td>21%</td>
<td>24%</td>
<td>33%</td>
<td>24%</td>
</tr>
<tr>
<td>Federal 50</td>
<td>4%</td>
<td>6%</td>
<td>14%</td>
<td>20%</td>
<td>40%</td>
</tr>
<tr>
<td>Consumer 100</td>
<td>22%</td>
<td>36%</td>
<td>48%</td>
<td>64%</td>
<td>29%</td>
</tr>
<tr>
<td>News 100</td>
<td>-</td>
<td>10%</td>
<td>10%</td>
<td>21%</td>
<td>14%</td>
</tr>
<tr>
<td>OTA Members</td>
<td>44%</td>
<td>59%</td>
<td>77%</td>
<td>75%</td>
<td>25%</td>
</tr>
</tbody>
</table>

* As % of sites with a DMARC record

- Use of DMARC records grew in all sectors, led by retailers and Consumer, but is still a fraction of overall authentication levels
- Use of DMARC policy assertions also grew, but is still in early stages