2015 Online Trust Audit & Honor Roll
Email Practices Deep Dive
July 7, 2015

Mike Jones
Director
Agari

Craig Spiezle
Executive Director & President
Online Trust Alliance

Who Is OTA?

Mission - To enhance online trust and empowering users, while promoting innovation and the vitality of the internet.

- Goal to help educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity.
- OTA supports collaborative public-private partnerships, benchmark reporting, meaningful self-regulation and data stewardship.
- IRS approved 501c3 tax-exempt charitable organization
  - Supported by over 100 leading brands, advertisers, marketers, technology leaders, non-profits and government agencies.

Brian Westnedge
Sr. Director, Client Services
Return Path

Jeff Wilbur
VP Marketing
Iconix
Online Trust Audit & Honor Roll

Objectives:

• Move from a “compliance” mindset to “stewardship”
• Recognize leadership brands, sites & apps that implement security and privacy practices protecting users’ data
• Incentivize businesses and developers to enhance their security, data protection and privacy practices
• Make security & privacy part of a brand’s value proposition
• Increase awareness and preference for best practices

Honor Roll Overview

• Analysis of ~1,000 web sites
  ▫ FDIC Banking 100
  ▫ Internet Retailer Top 500
  ▫ Top 50 Social
  ▫ Top 50 News/Media (introduced in 2014)
  ▫ Top 50 Federal Gov’t
  ▫ OTA Members
  ▫ IoT 50 (Home automation, Wearables)

• Scoring
  ▫ Up to 100 points in each category
  ▫ Bonus points for emerging practices
  ▫ Penalty points for
    • Data loss incident, fines/settlement
    • Inadequate practices
  ▫ Honor Roll = 80% of total points, 55% or better in each category
Collaborative & Open Process

- November 14 – Methodology Call for comments
- February 15 - Published methodology
- March 15 - Hosted webinars and tools to aid companies

*Powered in part by leading companies including;*
  - Agari, AVG Technologies, DigiCert, Disconnect
  - Distil Networks, Ensighten, GlobalSign, High-Tech Bridge SA
  - IID, Microsoft, Return Path, SiteLock, SSL Labs, Symantec,
  - ThreatWave, TRUSTe & VERISIGN

Overall Achievement

- Record level of Honor Roll achievement, despite more stringent criteria
- Primarily due to many organizations near threshold raising score with simple improvements
- Most consistent increase was in privacy policy scores
Overall Achievement by Sector

OTA ONLINE TRUST HONOR ROLL ACHIEVEMENT BY SECTOR

<table>
<thead>
<tr>
<th>Sector</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR 100</td>
<td>41%</td>
<td>34%</td>
<td>42%</td>
<td>54%</td>
</tr>
<tr>
<td>IR 500</td>
<td>35%</td>
<td>26%</td>
<td>42%</td>
<td>60%</td>
</tr>
<tr>
<td>FDIC</td>
<td>25%</td>
<td>25%</td>
<td>32%</td>
<td>56%</td>
</tr>
<tr>
<td>SOCIAL</td>
<td>44%</td>
<td>22%</td>
<td>54%</td>
<td>52%</td>
</tr>
<tr>
<td>NEWS</td>
<td>4%</td>
<td>8%</td>
<td>4%</td>
<td>20%</td>
</tr>
<tr>
<td>IoT</td>
<td>20%</td>
<td>20%</td>
<td>20%</td>
<td>42%</td>
</tr>
<tr>
<td>FED</td>
<td>20%</td>
<td>20%</td>
<td>20%</td>
<td>42%</td>
</tr>
</tbody>
</table>

Top of The Class

Ranked #1 of all 800 sites across all sectors

Online Retailers
Social
Federal
Banking
News
IoT
Baseline Category Scores

2015 ONLINE TRUST HONOR ROLL
AVERAGE BASELINE SCORES

Reasons for Failure

FAILING GRADES BY CATEGORY
Brand Protection

- **Base points**
  - Email authentication
    - SPF and DKIM at top-level and subdomains
  - DMARC record and policy
    - Policy=Reject for max points

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

- **Penalty points**
  - Domain locking (not locked)

Email Authentication Overview

**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)
Transport Layer Security

Rapidly being adopted standard for secure email.

- TLS uses Public Key Infrastructure (PKI) to encrypt messages between mail servers. This encryption makes it difficult for hackers to intercept and read messages.

- TLS supports the use of digital certificates to authenticate the receiving servers. Authentication of sending servers is optional. This process verifies receivers (or senders) are who they say they are, which helps to prevent spoofing.


https://www.google.com/transparencyreport/saferemail/

Email/Brand Protection Summary
Overall Authentication Adoption

- Minimum adoption is to support at least one authentication method
- Adoption of “either” nearing 100% in many sectors – Fed, News and IoT are lagging

<table>
<thead>
<tr>
<th>DOMAIN &amp; BRAND PROTECTION</th>
<th>EITHER SPF OR DKIM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2012</td>
</tr>
<tr>
<td>Internet Retailer Top 100</td>
<td>97%</td>
</tr>
<tr>
<td>Internet Retailer Top 500</td>
<td>91%</td>
</tr>
<tr>
<td>FDIC 100</td>
<td>69%</td>
</tr>
<tr>
<td>Federal 50</td>
<td>58%</td>
</tr>
<tr>
<td>Social 50</td>
<td>96%</td>
</tr>
<tr>
<td>OTA Members</td>
<td>99%</td>
</tr>
<tr>
<td>News 50</td>
<td>-</td>
</tr>
<tr>
<td>IoT 50</td>
<td>-</td>
</tr>
</tbody>
</table>

- Best practice is to support both SPF and DKIM
- Adoption of both grew in all sectors

SPF Adoption Analysis

<table>
<thead>
<tr>
<th>DOMAIN &amp; BRAND PROTECTION</th>
<th>SPF ADOPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2012 Top Level Domains</td>
</tr>
<tr>
<td>Internet Retailer Top 100</td>
<td>67%</td>
</tr>
<tr>
<td>Internet Retailer Top 500</td>
<td>63%</td>
</tr>
<tr>
<td>FDIC 100</td>
<td>60%</td>
</tr>
<tr>
<td>Federal 50</td>
<td>50%</td>
</tr>
<tr>
<td>Social 50</td>
<td>96%</td>
</tr>
<tr>
<td>OTA Members</td>
<td>99%</td>
</tr>
<tr>
<td>News 50</td>
<td>-</td>
</tr>
<tr>
<td>IoT 50</td>
<td>-</td>
</tr>
</tbody>
</table>

- Overall SPF grew in most sectors (especially Fed, News and FDIC) – IoT still lags significantly
- SPF at TLD grew in nearly all sectors – still room for improvement in IoT, News, Fed and FDIC
### DKIM Adoption Analysis

<table>
<thead>
<tr>
<th></th>
<th>2012 Top Level Domains</th>
<th>2013 Top Level Domains</th>
<th>2014 Any DKIM</th>
<th>2015 Top Level Domains</th>
<th>2015 Any DKIM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Retailer Top 100</td>
<td>23%</td>
<td>26%</td>
<td>33%</td>
<td>92%</td>
<td>31%</td>
</tr>
<tr>
<td>Internet Retailer Top 500</td>
<td>16%</td>
<td>18%</td>
<td>27%</td>
<td>81%</td>
<td>27%</td>
</tr>
<tr>
<td>FDIC 100</td>
<td>27%</td>
<td>30%</td>
<td>27%</td>
<td>58%</td>
<td>30%</td>
</tr>
<tr>
<td>Federal 50</td>
<td>16%</td>
<td>22%</td>
<td>20%</td>
<td>28%</td>
<td>28%</td>
</tr>
<tr>
<td>Social 50</td>
<td>56%</td>
<td>62%</td>
<td>56%</td>
<td>76%</td>
<td>56%</td>
</tr>
<tr>
<td>OTA Members</td>
<td>46%</td>
<td>58%</td>
<td>73%</td>
<td>84%</td>
<td>78%</td>
</tr>
<tr>
<td>News 50</td>
<td>-</td>
<td>-</td>
<td>14%</td>
<td>56%</td>
<td>16%</td>
</tr>
<tr>
<td>IoT 50</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>14%</td>
<td>30%</td>
</tr>
</tbody>
</table>

- Overall DKIM grew in all sectors, with significant growth in Fed, FDIC, News and OTA
- DKIM at TLD lags significantly and was ~flat in most sectors

### DMARC Adoption Analysis

<table>
<thead>
<tr>
<th></th>
<th>2012 Record</th>
<th>2013 Record</th>
<th>2014 Record</th>
<th>2015 R or Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Retailer Top 100</td>
<td>2%</td>
<td>5%</td>
<td>15%</td>
<td>20%</td>
</tr>
<tr>
<td>Internet Retailer Top 500</td>
<td>2%</td>
<td>3%</td>
<td>6%</td>
<td>8%</td>
</tr>
<tr>
<td>FDIC 100</td>
<td>1%</td>
<td>13%</td>
<td>21%</td>
<td>24%</td>
</tr>
<tr>
<td>Federal 50</td>
<td>0%</td>
<td>4%</td>
<td>6%</td>
<td>14%</td>
</tr>
<tr>
<td>Social 50</td>
<td>19%</td>
<td>22%</td>
<td>36%</td>
<td>48%</td>
</tr>
<tr>
<td>OTA Members</td>
<td>34%</td>
<td>44%</td>
<td>59%</td>
<td>77%</td>
</tr>
<tr>
<td>News 50</td>
<td>-</td>
<td>-</td>
<td>10%</td>
<td>10%</td>
</tr>
<tr>
<td>IoT 50</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2%</td>
</tr>
</tbody>
</table>

- Use of DMARC records grew in nearly all sectors, but is still a small fraction of overall authentication levels
- Use of DMARC policy assertions also grew, but is still in early stages
**Email Trust Scorecard**

- Shows percent of organizations that support **both** SPF and DKIM at the TLD and have a DMARC record
- Some sectors grew, some fell, mainly due to shifts in sector membership
- Overall level fell due to new sector (IoT) at 0%
- Low levels overall reflect opportunity for brand protection

**Concerns and Next Steps**

- Lack of DKIM at top-level domain
  - Only 31% overall though 76% have at least some DKIM
- Lack of DMARC record and policy assertion
  - Only 17% overall have a DMARC record though 92% support some form of authentication
- Protection of “parked domains” and non-email sending domain.
- Develop comprehensive authentication plan in conjunction with management, MTA vendors and others.
- Requires operational discipline.
- Responsibility of mail streams distributed throughout an organization and often “siloded”
2016 Methodology Under Review

- Shifting additional “bonus points” to core points
- Increased weighting for TLD protection?
- Increased scoring for DMARC records?
- Always On SSL
- Layered Notices
- Bi-Lingual Notices
- Do-Not-Track Disclosure
- Negative points of use of DV certificates
- ???

Tools & Resources

- Email Security [https://otalliance.org/auth](https://otalliance.org/auth)
- Resources [https://otalliance.org/resources/ota-spf-dmarc-resources-tools](https://otalliance.org/resources/ota-spf-dmarc-resources-tools)

- Online Trust Honor Roll [https://otalliance.org/HonorRoll](https://otalliance.org/HonorRoll)
  - Methodology, past reports and related resources
- SSL Server Test [https://ota.ssllabs.com](https://ota.ssllabs.com)
- Always On SSL (AOSSL) - [https://otalliance.org/aossl](https://otalliance.org/aossl)
- Internet of Things – [https://otalliance.org/IoT](https://otalliance.org/IoT)

More information – email jeffw@otalliance.org or call +1 425-455-7400