2016 Online Trust Audit

Webinar Will Start Shortly

Webinar will be recorded
Presentation will be posted at
https://otalliance.org/HonorRoll
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 user awareness and preference
- Support calls for objective ranking and scoring of security & privacy practices
Disclaimer

- Audit was conducted April 15 – May 15
- There is no perfect security or privacy
- “Snapshot” – sites and data may have changed
- Does not reflect an audit of business practices
- Is not an endorsement of any company or service
- Several sites advised OTA of updates. Where validated they were re-scored, impacting ranking

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, inadequate privacy practices, data loss incidents and/or regulatory fines/settlement
  - Honor Roll = 80% of total points, 55% or better in each category
Honor Roll Recap

- Record achievement despite a bar that continues to rise
- 12% qualified for 5 consecutive years
- Range of retailers #1 to #493, showing bar is achievable
- 10% qualified for the “Top of the class” 95%+

Growth in All Sectors

- Nearly three-fold increase in News, yet they still lag all sectors, primarily due to data sharing with limited controls
Top of The Class in 2016

Ranked #1 of all sites across all sectors

Online Retailers
Consumer
Federal

Banking
News

2016 Top Ten

1. Twitter (twitter.com)
2. HealthCare.gov (healthcare.gov)
3. Pinterest (pinterest.com)
4. The White House (whitehouse.gov)
5. Dropbox (dropbox.com)
6. FileYourTaxes (fileyourtaxes.com)
7. LifeLock (lifelock.com)
8. Instagram (instagram.com)
9. 1040.com (1040.com)
10. Gap Inc. (gap.com)
2016 Online Trust Audit Report

Failing vs Stewardship

4 categories bi-modal (or nearly)
Range & Median

- Retailers and FDIC banks median is at 80% Honor Roll bar
- Consumer and Fed sites outperform, while News lags

Summary of Failures

- 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
Primary Areas of Concern

- Lack of email authentication an issue in many sectors
- Low failure rate in site security – most sites have solid practices
- Overall privacy failures are low, but big issue for News 100

**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

- 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**
- 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)

Consumer Protection

- Aids in protection from social engineering exploits including spearphishing & ransomware
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><strong>64%</strong></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

DNSSEC and IPv6 Adoption

<table>
<thead>
<tr>
<th></th>
<th>DNSSEC ADOPTION</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Retailer Top 100</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>Internet Retailer Top 500</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>FDIC 100</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>Federal 50</td>
<td>88.0%</td>
<td>92.0%</td>
</tr>
<tr>
<td>Consumer 100</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>News 100</td>
<td>-</td>
<td>2.0%</td>
</tr>
<tr>
<td>OTA Members</td>
<td>7.6%</td>
<td>4.7%</td>
</tr>
</tbody>
</table>

- DNSSEC – miniscule adoption in all but the Federal 50
- IPv6 – Federal 50 has strong adoption, others just starting
Site Security

- Base points
  - Server & SSL implementation
  - *Major component failure = overall failure*

- Bonus points
  - EV SSL
  - AOSSL (*increased weight*)

- Penalty points
  - XSS / iFrame vulnerabilities
  - Malware
  - Malicious links
  - Bot risk
  - *DV certificate*

Italics = new for 2016

Best practices to secure data in transit and collected by websites, and prevent malicious exploits running against clients’ devices, including desktop, mobile and IoT devices.

Site & Data Security

- Overall average scores are tightly clustered, yet adoption of key standards advocated by the FDIC, IRS, OMB and industry varies widely

SITE & SERVER SECURITY

- SUMMARY SCORE
  - IR 100
  - IR 500
  - FDIC
  - FED
  - CONSUMER
  - NEWS

- EV SSL
  - 25%
  - 30%
  - 10%
  - 6%
  - 22%
  - 18%

- AOSSSL/HSTS
  - 81%
  - 50%
  - 50%

© 2016 All rights reserved, Online Trust Alliance (OTA)
OTA/Qualys SSL Tool

SSL Report: otalliance.org (67.192.183.74)
Assessed on: Wed, 27 Jan 2016 02:58:08 UTC (HIDENX) Scan now

Summary

Overall Rating

Certificate
Protocol Support
Key Exchange
Cipher Strength

Visit our documentation page for more information, configuration guides, and tools. Known issues are documented here.

Invalid or incomplete HSTS information provided. More information available below.

Server certificate invalid (HSTS). See below for further information.

https://ota.ssllabs.com

High-Tech Bridge SSL Tool

Free SSL Server Test

SSL/TLS Security Test by High-Tech Bridge
Test SSL/TLS implementation of any service on any host for compliance with industry best practices, NIST guidelines and PCI DSS requirements.

Summary of otalliance.org SSL/TLS Security Test

https://www.htbridge.com/ssl
### Security Score Trends

#### SITE & SERVER SECURITY

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Retailer Top 100</td>
<td>85.3</td>
<td>81.9</td>
<td>85.7</td>
<td>89.6</td>
</tr>
<tr>
<td>Internet Retailer Top 500</td>
<td>85.1</td>
<td>83.3</td>
<td>85.3</td>
<td>88.3</td>
</tr>
<tr>
<td>FDIC 100</td>
<td>85.0</td>
<td>86.5</td>
<td>83.0</td>
<td>88.3</td>
</tr>
<tr>
<td>Federal 50</td>
<td>73.2</td>
<td>70.5</td>
<td>83.6</td>
<td><strong>91.6</strong></td>
</tr>
<tr>
<td>Consumer 100</td>
<td>82.1</td>
<td>86.2</td>
<td>86.1</td>
<td>89.9</td>
</tr>
<tr>
<td>News 100</td>
<td>-</td>
<td>83.2</td>
<td>83.0</td>
<td>85.0</td>
</tr>
<tr>
<td>OTA Members</td>
<td>87.1</td>
<td>86.8</td>
<td>89.8</td>
<td>92.1</td>
</tr>
</tbody>
</table>

### What Is Malvertising?

- Malware + Advertising
- Malicious computer code with seemingly harmless ads.
- Draw a user to harmful or deceptive content through ‘click-baiting’ or misleading content.

OR

- May directly infect a device with malware damaging data, steal PII and/or take control of the device.
- Drives key loggers, malware, ransomware & ID theft.

Source: Anti-Malvertising.com
Malvertising

• Audit of the News 100 from Oct 2015 – May 2016
• Only tracked malvertising with malware; did not include deceptive pop-up, warnings or social engineered exploits; so data under-reports the real impact.
  ▫ 17% had at least one incident
  ▫ 10% pubs had 2 or more incidents
  ▫ 54 incidents observed serving 1.1 Billion malicious impressions

• Sites with malvertising had a slightly higher than average failure rate, so they suffer from other issues as well

Concerns – Certificate Type

• Recommend OV or EV for increased trust/transparency
• Rise in fraudulent/lookalike sites that typically use DV certs
Privacy

- **Base points**
  - Privacy policy (50 pts)
    - Data sharing, retention, third party sharing
    - DNT disclosure
    - Layered notices
    - Link on home page
    - COPPA
  - Third-party trackers on site (50 pts)

- **Bonus points**
  - Date stamp, version archive
  - Use of icons
  - Honoring DNT
  - Multi-lingual policy
  - Tag mgmt or privacy solution

- **Penalty points**
  - WHOIS (if private vs public)
  - Data breach incidents
  - FTC / State settlements

Best practices providing users clear notice and control of the data being collected, tracked and shared with third parties

Privacy Policy Disclosures

- **Total of 50 points possible based on**
  - Data collection
  - Data retention
  - Data usage
  - Data sharing
  - Layered / short notice
  - DNT disclosure
  - Notification of sharing
  - Link on home page
Privacy – Missing Link

### PRIVACY POLICIES, TRACKING & MONITORING

<table>
<thead>
<tr>
<th>Category</th>
<th>IR 100</th>
<th>IR 500</th>
<th>FDIC</th>
<th>FED</th>
<th>CONSUMER</th>
<th>NEWS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Privacy Score (Out of 100)</td>
<td>75</td>
<td>71</td>
<td>67</td>
<td>67</td>
<td>76</td>
<td>50</td>
</tr>
<tr>
<td>Policy Score (Out of 50)</td>
<td>6</td>
<td>29</td>
<td>26</td>
<td>17</td>
<td>36</td>
<td>34</td>
</tr>
<tr>
<td>Tracking Score (Out of 50)</td>
<td>43</td>
<td>41</td>
<td>50</td>
<td>50</td>
<td>41</td>
<td>23</td>
</tr>
</tbody>
</table>

Privacy – Missed Opportunities

### PRIVACY POLICY & DISCLOSURES

<table>
<thead>
<tr>
<th>Disclosure</th>
<th>IR 100</th>
<th>IR 500</th>
<th>FDIC</th>
<th>FED</th>
<th>CONSUMER</th>
<th>NEWS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Not Shared</td>
<td>72</td>
<td>67</td>
<td>60%</td>
<td>47%</td>
<td>76%</td>
<td>59%</td>
</tr>
<tr>
<td>Data Retention</td>
<td>56%</td>
<td>35%</td>
<td>27%</td>
<td>27%</td>
<td>37%</td>
<td>39%</td>
</tr>
<tr>
<td>Vendor Confidentiality</td>
<td>83%</td>
<td>73%</td>
<td>54%</td>
<td>44%</td>
<td>53%</td>
<td>44%</td>
</tr>
<tr>
<td>Layered Notice</td>
<td>12%</td>
<td>24%</td>
<td>24%</td>
<td>24%</td>
<td>12%</td>
<td>12%</td>
</tr>
<tr>
<td>DNT Disclosure</td>
<td>6%</td>
<td>6%</td>
<td>6%</td>
<td>6%</td>
<td>6%</td>
<td>6%</td>
</tr>
</tbody>
</table>

**Bonus items**

- 1.3% include icons, 4.5% localize their policy
- 73.7% date stamp, yet only 4.1% post older revisions
Do Not Track – DNT

- Required disclosure in California as of 1/1/14
- Moved through W3C to “release candidate” status
- Baseline points if disclosure is visible on the privacy page
- Bonus for sites honoring DNT
  - Data limited to first party collection & usage
  - Permitted usage would allowed for analytics, measurement purposes, frequency capping and related anonymous analytics
  - Permitted use for fraud detection and security purposes

General Observations

- Record Honor Roll achievement levels
- Significant increase in proactive engagement
- Failures due to inadequate email authentication places users at unnecessary risk levels
- Lack of continuous monitoring of site / servers raises risk of exploits and breaches
- Attempts to contact sites failed due to lack of vulnerability reporting mechanisms
- Privacy policies still exhibit poor readability and excessive language that is not user friendly
- High levels of data collection and sharing via use of tracking tags, ranging from 0 to 125 per site
Possible Criteria Enhancements

- Multi-factor authentication – core or bonus?
- Deeper security assessments
  - Open ports / relays
  - Expand malvertising beyond drivebys across all sectors
- Increased focus on privacy disclosures
  - DNT move to penalty points for non disclosure
  - DNT no points for not honoring due to standards status.
- Consumer Protection
  - Increased weighting of DMARC reject or quarantine
  - Inadequate DMARC records with no reporting mechanisms
  - Increased weighting of SPF AND DKIM at TLD.
- Native advertising disclosures
- Abuse / vulnerability reporting capabilities

Next Steps

- Email Authentication Deep Dive – July 20
  https://attendee.gotowebinar.com/register/114134127128392450
- Input into 2017 methodology and scoring
  - Open call for comments – email admin@otalliance.org
- Under consideration
  - ISPs, cable providers and carriers
  - 50 States, focused on TBD core consumer agency(s)
  - State e-file sites
  - IoT devices & services
- Updates posted at https://otalliance.org/HonorRoll
Expanding the Social 50

- Renamed to “Consumer Services”
- Expanded to 100, including top sites in
  - Social networks
  - Image/file sharing
  - Dating
  - Gaming
  - Jobs/career
  - Review/reference
  - Free IRS e-file sites
  - ID theft/credit monitoring
  - Travel
  - Blogging
  - Other miscellaneous
Trust Index Trends

OTA ONLINE TRUST INDEX

2013 2014 2015 2016
IR 100 IR 500 FDIC CONSUMER OTA NEWS FED

Baseline Scores

2016 ONLINE TRUST HONOR ROLL AVERAGE BASELINE SCORES

CONSUMER PROTECTION SITE SECURITY PRIVACY

© 2016 All rights reserved. Online Trust Alliance (OTA)
Failing Grades By Sector

- Reasons for failure varied widely across sectors

What is Email Authentication?

- **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
Email Authentication Adoption

CONSUMER PROTECTION
BOTH SPF AND DKIM

<table>
<thead>
<tr>
<th></th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Retailer Top 100</td>
<td>76%</td>
<td>88%</td>
<td>90%</td>
<td>92%</td>
</tr>
<tr>
<td>Internet Retailer Top 500</td>
<td>56%</td>
<td>74%</td>
<td>78%</td>
<td>85%</td>
</tr>
<tr>
<td>FDIC 100</td>
<td>49%</td>
<td>49%</td>
<td>63%</td>
<td>69%</td>
</tr>
<tr>
<td>Federal 50</td>
<td>20%</td>
<td>22%</td>
<td>48%</td>
<td>58%</td>
</tr>
<tr>
<td>Consumer 100</td>
<td>72%</td>
<td>74%</td>
<td>76%</td>
<td>86%</td>
</tr>
<tr>
<td>News 100</td>
<td>-</td>
<td>50%</td>
<td>56%</td>
<td>75%</td>
</tr>
<tr>
<td>OTA Members</td>
<td>69%</td>
<td>83%</td>
<td>94%</td>
<td>99%</td>
</tr>
</tbody>
</table>

SSL Growth

WORLDWIDE GROWTH OF EV SSL CERTS

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>23,675</td>
<td>38,966</td>
<td>57,837</td>
<td>57,837</td>
<td>103,540</td>
<td>123,532</td>
<td>149,282</td>
</tr>
</tbody>
</table>

© 2016 All rights reserved. Online Trust Alliance (OTA)
Privacy – Bonus Points

Layered Notice & Icons

- Publishers Clearing House
  http://privacy.pch.com/
- Reduced word count from over 4,000 words to 475!
- Adds clarity, readability & transparency
- Added bonus points for icons

DNT Suggested Language

- XYZ respects enhanced user privacy controls. We support the development and implementation of a standard “Do Not Track” (DNT) browser feature, which had been designed to provide users control over the collection and use of information by third parties regarding their web-browsing activities. At this time, XYZ does not respond to DNT mechanisms. Once a standardized "do not track" feature is released, XYZ intends to adhere and respect the browser settings accordingly.
DNT is now a standard

- XYZ respects enhanced user privacy controls and Honors user browser Do Not Track setting.
  - Optional - As permitted by the DNT specification, we may collect data limited to site security and fraud prevention purposes as well as for anonymous site analytics.
- Xyz does not honor a user’s browser Do Not Track setting. This site does not offer any persistent and universal provisions to opt-out of data collection, tracking and/or sharing.
- XYZ honors a DNT setting, but third parties including ad networks, marketing partners and others may not honor this setting and continue to collect, share and use users tracking and personal data.