2017 Online Trust Audit – Find Out Who Made the Grade

Recognizing Excellence in Security, Privacy & Consumer Protection

2017 Online Trust Audit

Jeff Wilbur
Director, OTA Initiative
Internet Society

Craig Spiezle
Founder, Chair Emeritus
Online Trust Alliance
Objectives:
• Drive adoption and awareness of data security principles and responsible privacy practices
• Move organizations from a “compliance” mindset to embrace “stewardship”
• Incentivize businesses and developers to enhance their security, data protection and privacy practices
• Recognize leadership and excellence

9th Annual Audit Overview
• Over 1,000 web sites
  ▫ Internet Retailer Top 500
  ▫ Bank 100 (previously FDIC 100)
  ▫ Consumer Services 100
  ▫ News/Media 100
  ▫ Federal Gov’t 100
  ▫ ISP/Carriers/Hosters 100
  ▫ OTA Members

• Scoring
  ▫ 100 baseline points for each category
  ▫ Weighted composite analysis
  ▫ Bonus points for emerging practices
  ▫ Penalties for vulnerabilities, data loss incident & fines/settlements
  ▫ Honor Roll = 80% or higher overall, no failure(s)
  ▫ Failure for less than 60 points in each category
Record Achievement

- Record achievement despite a bar that continues to rise
- New criteria & shifts in additional requirements
- Minimum failure thresholds raised

OVERALL 2017 HONOR ROLL ACHIEVEMENT

<table>
<thead>
<tr>
<th>Year</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>30%</td>
<td>44%</td>
<td>50%</td>
<td>52%</td>
</tr>
</tbody>
</table>

2017 “Top of Class”
Sector Performance

- News/Media segment surge exponentially
- Retailers and Consumer have steady growth
- Banks plunge

Bi-Modal Results

- Over 60% of the Fed 100 and 65% of the Bank 100 fail!
- Effectively, sites embraced best practices or failed
Wide-Ranging Scores

- Many sectors clustered around 80% Honor Roll threshold

Causes of Failures

- Overlooking the basics & fundamentals
- 36% failed in one area, 11% failed in 2-3 areas
Failure Analysis

Failing Grades by Category

- **Consumer Protection** – Sites failing to counter phishing exploits
- **Security** – Insecure ciphers & protocols
- **Privacy** – Lack of full disclosures & excessive third-party trackers

Consumer Protection – 2017

- **Base points**
  - Email authentication
  - SPF and DKIM at top-level and subdomains (↑ TLD weight)
  - DMARC record and policy
  - DMARC reject/quarantine
    - Increased weight for reject
  - Invalid SPF / DMARC & “naked” DMARC records not counted

- **Bonus points**
  - TLS for email
  - DNSSEC
  - IPv6
  - Multi-factor authentication

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

- Italic = new for 2017

- 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?
Fighting Spearphishing

**SPF & DKIM Adoption**

- SPF & DKIM allow recipient to verify sender
- Recommend implementation for inbound & outbound email
- All domains – top-level and subdomains
- Observed many (>70) inaccurate / malformed SPF records

**DMARC Adoption**

- DMARC allows sender to get reports, tell receiver how to handle messages that fail authentication
- Federal sites lagging in protection from spoofed email
- Use of reject/quarantine policy growing, but far from adequate
Site Security – 2017

- **Base points**
  - Server & SSL/TLS implementation
  - Application / network security
  - IP reputation, patching cadence

- **Bonus points**
  - Extended Validation certificates
  - "HTTPS everywhere", HSTS
  - Web application firewall
  - *Vulnerability reporting mechanism*

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

Italics = new for 2017

---

Overall Security

- Encryption becoming the “norm”, jumping from 30% to 52%
- Extended Validation certs recognized for brand protection
Security Assessment Tools

- Bonus points (new in 2017)
  - Discoverable on the site
  - Discoverable via third-party reporting program
- Ties to NTIA, NIST and FTC recommendations
- 36% of Consumer sites support it
- Other segments <3%

Vulnerability / Bug Reporting
Privacy – 2017

- **Base points**
  - Privacy policy (55 pts)
    - Data sharing, retention, third-party sharing
    - DNT disclosure
    - Layered notices
    - Link on home page
    - COPPA
    - Date stamp on top of page
  - Third-party trackers on site (45 pts)

- **Bonus points**
  - Redline version archived
  - Use of Icons
  - Cross device tracking disclosure
  - Honoring DNT / Multi-lingual policy
  - Tag management 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

---

Example

Vulnerability Reporting Form

Note: Under Construction

OTA is committed to the adoption of security and privacy best practices. Recognizing the evolving threat landscape, we welcome responsible and coordinated disclosures to help improve the security of our site. Please allow 72 hours for an initial reply and initiate investigations and risk assessments. Note: unless requested otherwise by the submitting party, after investigation and resolution, we may provide recognition to confirmed and resolved reports.

For more information please refer to the OTA Privacy Policy. Related information on coordinated vulnerability and bug-reporting best practices. OTA blog [iapp](https://www.iapp.org)

First Name * 
Last Name *

Organization or Company *
Email Address *

Country
- None
- Name
- Year
- Month
- Day

Where are you located?
Phone Number *

Only add numbers or special characters

URL of Observed Vulnerability *
Additional URL (optional)
Overall Privacy

- In 2017, shifted more weight on the privacy policy disclosures
- Shifting from compliance to stewardship
- Driving towards GDPR

Tracking Tags / Calls

- Analysis of third party tracking, sharing, retargeting
- Does not apply to trackers used for anonymous site metrics
- Ranged from 0 to over 59 on a single site!
- Average of 25 unique trackers per News/Media site (down from 40 in 2016)
- Use of multiple tools
  - OTA tools
  - Disconnect
  - Ensighten
Transparency

- Beyond compliance, advancing transparency
Version Tracking

Updates: Privacy Policy

We want to be as transparent as possible about the changes we make to our Privacy Policy. In this archive you can see the previous versions of the policy. We've also included a page that compares the current policy to the previous version to make it as easy as possible to see what has changed.

- Current version
- Comparison
- March 1, 2017
- Comparison
- August 29, 2016
- Comparison
- June 29, 2016
- Comparison
- March 25, 2016
- Comparison
- August 19, 2015

Privacy Policy

This is an archived version of our Privacy Policy. View the current version or all past versions.

Last modified: 2017-08-29 15:01 (new archived version)

There are many different ways you can use our services - to search for and share information, to communicate with other people or to create new content. When you share information with us, for example by creating a Google Account, we can make those services even better - to show you more relevant search results and ads, to help you connect with people or to make sharing with others quicker and easier. As you use our services, we want to be clear how we're using information - the ways in which you can protect your privacy.

Our Privacy Policy explains:
- What information we collect and why we collect it.
- How we use that information.
- The choices we offer, including how to access and update information.

Example

For example, if someone is already a contact, Google will autocompleate their name if you want to add them to a message in Gmail.

Learn more
Readability

- Complexity vs Comprehendible?
- Is English the primary language of all of your users?

Layered Notices
Layered Notice

Basic Privacy Settings & Tools

Selecting an Audience for Stuff You Share

When I post something, how do I choose who can see it?

You'll find an audience selector tool most places you share status updates, photos and other things you post. Click the tool and select who you want to share something with.

© 2017 All rights reserved. The Internet Society

Use of Icons

© 2017 All rights reserved.
Data Handling

- Control on the sharing and usage of user data
- “If you do not retain it you can not lose it”

What Have We Learned

- Need to move beyond compliance
- Requires ongoing commitment & vigilance
- Everyone’s job within an organization
- Need to think beyond the US legal framework
- Responsible privacy practices enhance trust
- Learn from others’ mistakes
Checklist & Resources

- Evaluate your own site
- [https://otalliance.org/TrustAudit](https://otalliance.org/TrustAudit)
  - Methodology
  - Checklists
  - Listing of free public tools
  - Recorded webinars

Next Steps

- Evaluate your own site & use the checklist
- Possible new segments
  - Healthcare / Top 100 hospitals / medical center
  - EU & APAC segments
- Tentative Timing
  - September open call for comments
  - January / February publish new criteria and enhancements
  - April / May testing
  - June – Release of 2018 Audit
- Updates at [https://otalliance.org/TrustAudit](https://otalliance.org/TrustAudit)
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)
DMARC – Emerging Standard

DMARC ADOPTION

<table>
<thead>
<tr>
<th>Sector</th>
<th>2015 Record</th>
<th>2016 Record</th>
<th>2017 Any Record</th>
<th>2017 Valid Record</th>
<th>R or Q*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Retailer Top 100</td>
<td>20%</td>
<td>30%</td>
<td>51%</td>
<td>50%</td>
<td>22%</td>
</tr>
<tr>
<td>Internet Retailer Top 500</td>
<td>8%</td>
<td>21%</td>
<td>35%</td>
<td>33%</td>
<td>13%</td>
</tr>
<tr>
<td>Bank 100</td>
<td>24%</td>
<td>33%</td>
<td>42%</td>
<td>39%</td>
<td>10%</td>
</tr>
<tr>
<td>Federal 100</td>
<td>14%</td>
<td>20%</td>
<td>23%</td>
<td>20%</td>
<td>11%</td>
</tr>
<tr>
<td>Consumer 100</td>
<td>48%</td>
<td>64%</td>
<td>68%</td>
<td>62%</td>
<td>34%</td>
</tr>
<tr>
<td>News 100</td>
<td>10%</td>
<td>21%</td>
<td>35%</td>
<td>29%</td>
<td>11%</td>
</tr>
<tr>
<td>ISP/Hosts</td>
<td>-</td>
<td>-</td>
<td>29%</td>
<td>25%</td>
<td>12%</td>
</tr>
</tbody>
</table>

- Growth in all sectors
- Real value when sites instruct ISPs / receivers to “reject” or “quarantine” unauthenticated email
- Note impact of invalid DMARC records (3% overall)

“Top of Class” – Top 50

<table>
<thead>
<tr>
<th>Sector</th>
<th>Site</th>
<th>Sector</th>
<th>Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Airbnb</td>
<td>C, O</td>
<td>Identity Guard</td>
</tr>
<tr>
<td>R, O</td>
<td>American Greetings Corp.</td>
<td>C</td>
<td>Indeed</td>
</tr>
<tr>
<td>C</td>
<td>Blogger</td>
<td>C</td>
<td>Instagram</td>
</tr>
<tr>
<td>C</td>
<td>Booking.com</td>
<td>C, O</td>
<td>LifeLock</td>
</tr>
<tr>
<td>C</td>
<td>Box</td>
<td>C, O</td>
<td>LinkedIn</td>
</tr>
<tr>
<td>R</td>
<td>BuildDirect Technologies Inc.</td>
<td>R</td>
<td>LivingSocial Inc.</td>
</tr>
<tr>
<td>G</td>
<td>Census Bureau</td>
<td>C</td>
<td>Meetup</td>
</tr>
<tr>
<td>R</td>
<td>Chewy Inc.</td>
<td>I, O</td>
<td>Microsoft Azure</td>
</tr>
<tr>
<td>R</td>
<td>Costco</td>
<td>I, O</td>
<td>Microsoft Outlook.com</td>
</tr>
<tr>
<td>G</td>
<td>Health &amp; Human Services (Healthcare.gov)</td>
<td>N, O</td>
<td>MSN</td>
</tr>
<tr>
<td>I</td>
<td>DigitalOcean</td>
<td>C, O</td>
<td>OneDrive</td>
</tr>
<tr>
<td>C</td>
<td>Dropbox</td>
<td>C</td>
<td>Pinterest</td>
</tr>
<tr>
<td>R</td>
<td>Etsy Inc.</td>
<td>C, O</td>
<td>Publishers Clearing House</td>
</tr>
<tr>
<td>G</td>
<td>Federal Communications Comm. (FCC)</td>
<td>C, N</td>
<td>Reddit</td>
</tr>
<tr>
<td>G</td>
<td>Federal Deposit Insurance Corp. (FDIC)</td>
<td>C</td>
<td>Snapchat</td>
</tr>
<tr>
<td>R</td>
<td>Fitbit Inc.</td>
<td>C</td>
<td>Spotify</td>
</tr>
<tr>
<td>C</td>
<td>Foursquare</td>
<td>I</td>
<td>Squarespace</td>
</tr>
<tr>
<td>R, O</td>
<td>Gap Inc.</td>
<td>R</td>
<td>The RealReal</td>
</tr>
<tr>
<td>C</td>
<td>Glassdoor</td>
<td>C, O</td>
<td>Twitter</td>
</tr>
<tr>
<td>C</td>
<td>Google Docs</td>
<td>G</td>
<td>U.S. Dept. of Education</td>
</tr>
<tr>
<td>I</td>
<td>Google Gmail</td>
<td>G</td>
<td>U.S. Postal Service</td>
</tr>
<tr>
<td>N</td>
<td>Google News</td>
<td>R</td>
<td>Under Armour Inc.</td>
</tr>
<tr>
<td>C</td>
<td>Google Play</td>
<td>C</td>
<td>UpWork</td>
</tr>
<tr>
<td>I</td>
<td>Google Sites</td>
<td>C</td>
<td>YouTube</td>
</tr>
<tr>
<td>C, I</td>
<td>iCloud</td>
<td>C</td>
<td>Zynga</td>
</tr>
</tbody>
</table>

Top 50 Segment Performance

<table>
<thead>
<tr>
<th>Code</th>
<th>Segment</th>
<th>% of Top 50</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Consumer Services</td>
<td>52%</td>
</tr>
<tr>
<td>R</td>
<td>Internet Retailers</td>
<td>20%</td>
</tr>
<tr>
<td>I</td>
<td>ISPs, Carriers &amp; Hosters</td>
<td>14%</td>
</tr>
<tr>
<td>G</td>
<td>Government</td>
<td>12%</td>
</tr>
<tr>
<td>N</td>
<td>News &amp; Media</td>
<td>6%</td>
</tr>
<tr>
<td>F</td>
<td>FDIC 100</td>
<td>0%</td>
</tr>
</tbody>
</table>