



2016 Online Trust Audit

Webinar Will Start Shortly

*Webinar will be recorded
Presentation will be posted at
<https://otalliance.org/HonorRoll>*

UNDERWRITERS



LEARN • INNOVATE • COLLABORATE



2016 Online Trust Audit



Madelon Smith
VP, Director of Strategic Initiatives

UNDERWRITERS



LEARN • INNOVATE • COLLABORATE



2016 Online Trust Audit Review



Craig Spieze
Executive Director & President

Jeff Wilbur
VP, Industry Insights & Research

June 28, 2016



LEARN • INNOVATE • COLLABORATE

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 user awareness and preference**
- **Support calls for objective ranking and scoring of security & privacy practices**



LEARN • INNOVATE • COLLABORATE

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

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 5 

LEARN • INNOVATE • COLLABORATE

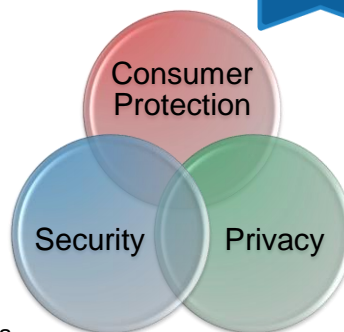
Honor Roll Overview

• 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

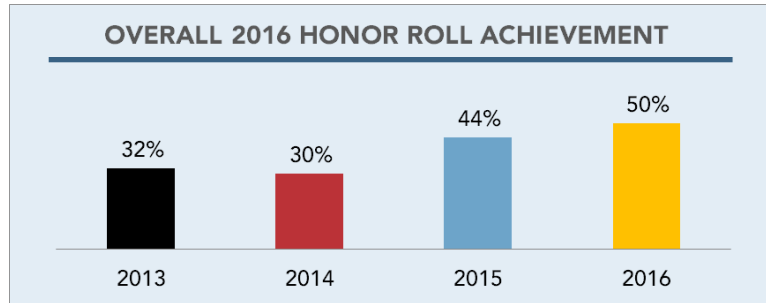


© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 6 

LEARN • INNOVATE • COLLABORATE

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%+

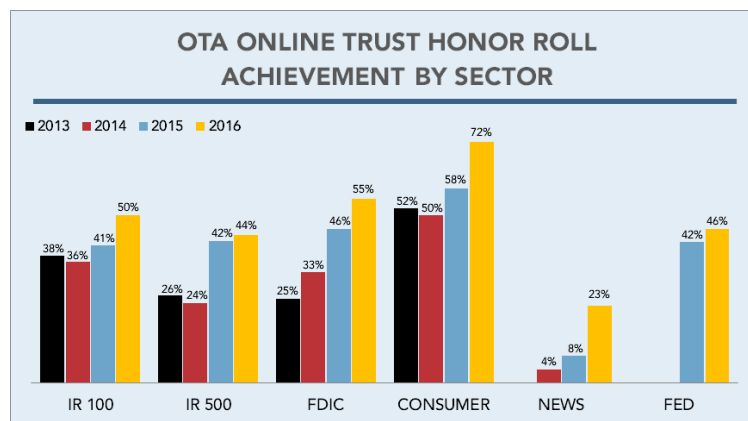
© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 7



LEARN • INNOVATE • COLLABORATE

Growth in All Sectors



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

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 8



LEARN • INNOVATE • COLLABORATE

Top of The Class in 2016



Ranked #1
of all sites across all sectors



Online Retailers



Consumer

HealthCare.gov

Federal

IBERIABANK

Banking

Google

News

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 9

LEARN • INNOVATE • COLLABORATE

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 All rights reserved. Online Trust Alliance (OTA)

Slide 10



LEARN • INNOVATE • COLLABORATE

2016 Online Trust Audit Report

EXECUTIVE SUMMARY & HIGHLIGHTS

The primary goal of this audit and report is to help drive the adoption of best practices and provide transparency to consumers regarding their security, data protection and privacy practices. The secondary goal is to recognize companies who have demonstrated a commitment to online trust and consumer best practices.

Now, in its 8th year, the report is available worldwide as a free resource (with no download) to help consumers adopt best practices.

2016 Executive Summary Top 100 - Honor Roll

APPENDIX A - 2016 HONOR ROLL RECIPIENTS

2016 Executive Summary Top 100 - Honor Roll	
1. 100.com	101. 100.com
2. 100.com	102. 100.com
3. 100.com	103. 100.com
4. 100.com	104. 100.com
5. 100.com	105. 100.com
6. 100.com	106. 100.com
7. 100.com	107. 100.com
8. 100.com	108. 100.com
9. 100.com	109. 100.com
10. 100.com	110. 100.com
11. 100.com	111. 100.com
12. 100.com	112. 100.com
13. 100.com	113. 100.com
14. 100.com	114. 100.com
15. 100.com	115. 100.com
16. 100.com	116. 100.com
17. 100.com	117. 100.com
18. 100.com	118. 100.com
19. 100.com	119. 100.com
20. 100.com	120. 100.com
21. 100.com	121. 100.com
22. 100.com	122. 100.com
23. 100.com	123. 100.com
24. 100.com	124. 100.com
25. 100.com	125. 100.com
26. 100.com	126. 100.com
27. 100.com	127. 100.com
28. 100.com	128. 100.com
29. 100.com	129. 100.com
30. 100.com	130. 100.com
31. 100.com	131. 100.com
32. 100.com	132. 100.com
33. 100.com	133. 100.com
34. 100.com	134. 100.com
35. 100.com	135. 100.com
36. 100.com	136. 100.com
37. 100.com	137. 100.com
38. 100.com	138. 100.com
39. 100.com	139. 100.com
40. 100.com	140. 100.com
41. 100.com	141. 100.com
42. 100.com	142. 100.com
43. 100.com	143. 100.com
44. 100.com	144. 100.com
45. 100.com	145. 100.com
46. 100.com	146. 100.com
47. 100.com	147. 100.com
48. 100.com	148. 100.com
49. 100.com	149. 100.com
50. 100.com	150. 100.com

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 11

TA Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Failing vs Stewardship

HONOR ROLL VS. FAILURES

■ HONOR ROLL ■ NEITHER ■ FAILURE

Category	Honor Roll (%)	Neither (%)	Failure (%)
IR 100	50%	14%	36%
IR 500	44%	13%	43%
FDIC	55%	4%	41%
FED	46%	0%	54%
CONSUMER	72%	3%	25%
NEWS	23%	4%	73%

• 4 categories bi-modal (or nearly)

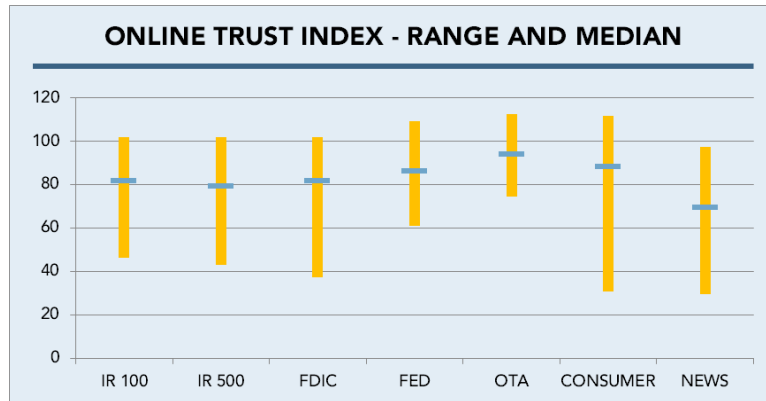
© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 12

TA Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Range & Median



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

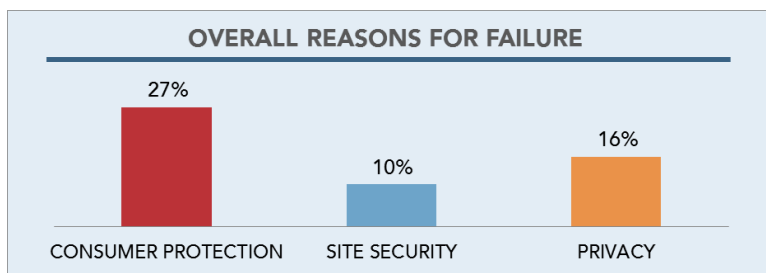
© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 13



LEARN • INNOVATE • COLLABORATE

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

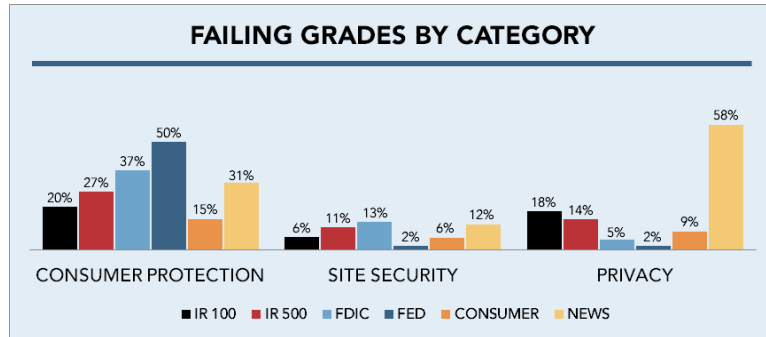
© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 14



LEARN • INNOVATE • COLLABORATE

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

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 15



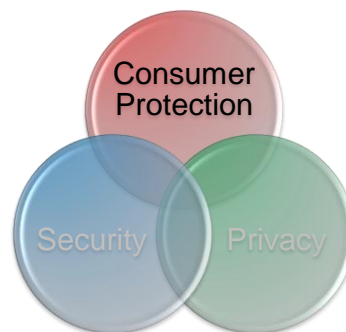
LEARN • INNOVATE • COLLABORATE

Consumer Protection

- Base points *Italics = new for 2016*
 - 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?

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 16



LEARN • INNOVATE • COLLABORATE

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

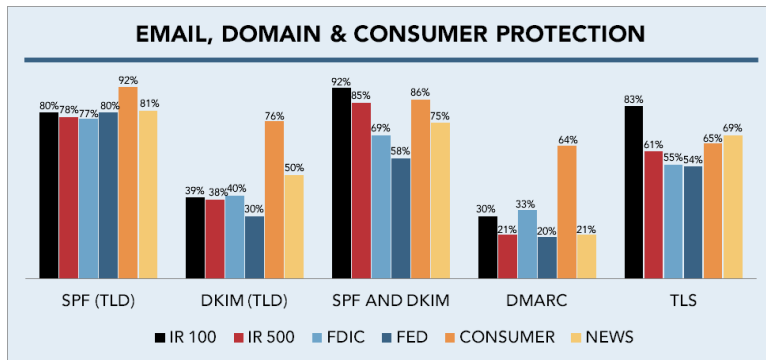


Aggregated Insights
Telemetry into mail streams (RUA)



Failure & Spoofed email reports (RUF)

Consumer Protection



- Aids in protection from social engineering exploits including spearphishing & ransomware

DMARC Adoption

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

* As % of sites with a DMARC record

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 19  Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

DNSSEC and IPv6 Adoption

	DNSSEC ADOPTION				IPv6
	2013	2014	2015	2016	2016
Internet Retailer Top 100	0.0%	0.0%	0.2%	0.0%	1.0%
Internet Retailer Top 500	0.0%	0.0%	0.4%	0.6%	1.6%
FDIC 100	0.0%	0.0%	1.0%	2.0%	0.0%
Federal 50	88.0%	92.0%	90.0%	88.0%	84.0%
Consumer 100	0.0%	0.0%	0.0%	0.0%	9.7%
News 100	-	2.0%	4.0%	2.0%	3.0%
OTA Members	7.6%	4.7%	4.7%	7.4%	13.2%

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

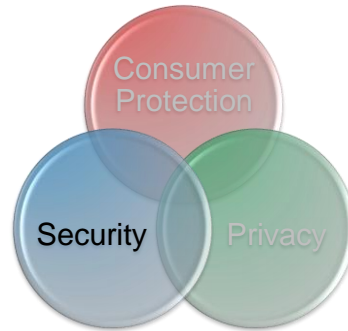
© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 20  Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Site Security

- Base points *Italics = new for 2016*
 - 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*



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

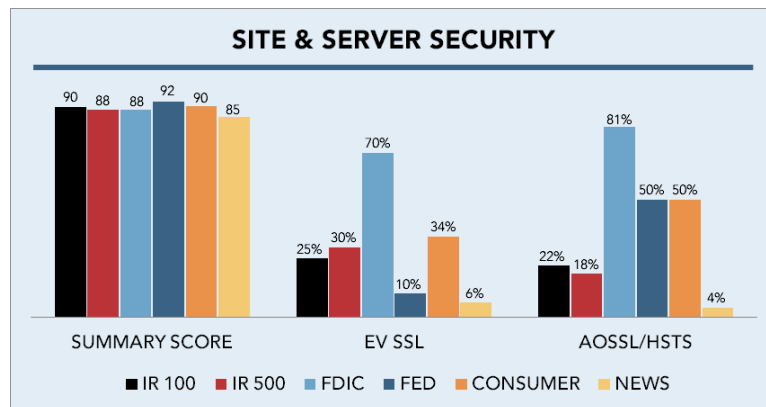
© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 21



LEARN • INNOVATE • COLLABORATE

Site & Data Security



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


© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 22




LEARN • INNOVATE • COLLABORATE

OTA/Qualys SSL Tool



Online Trust Alliance



Powered by
QUALYS SSL LABS

SSL Report: otalliance.org (67.192.153.74)

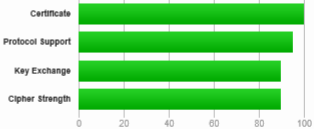
Assessed on: Mon, 27 Jun 2016 21:36:56 UTC | HIDDEN | [Clear cache](#)

[Scan Another >](#)

Summary

Overall Rating

A



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).


Invalid or incomplete HPKP information supplied. More information available below.

Server sent invalid HSTS policy. See below for further information.

<https://ota.ssllabs.com>


© 2016 All rights reserved. Online Trust Alliance (OTA)

LEARN • INNOVATE • COLLABORATE



Slide 23

High-Tech Bridge SSL Tool




High-Tech Bridge
INFORMATION SECURITY SOLUTIONS

Geneva: +41 (22) 723 2424 | San Francisco: +1 (415) 635 3784 | sales@htbridge.com

COMPANY • IMMUNIWEB • SERVICES • CONTACTS • Q

High-Tech Bridge > Free SSL Server Test > otalliance.org | 67.192.153.74:443

Free SSL Server Test

powered by 

SSL/TLS Security | Web Server Security | Domain Security Radar

SSL/TLS Security Test by High-Tech Bridge

Test SSL/TLS implementation of any service on any port for compliance with industry best-practices, NIST guidelines and PCI DSS requirements.

Web Server: just enter your website URL

Email Server: enter your mail service IP:Port

Other Server: enter IP:Port of the service

Do not display test results in statistics Provided "as is" without any warranty of any kind

Summary of otalliance.org SSL/TLS Security Test

FINAL GRADE

A+

COMPLIANT WITH

PCI DSS

HOST

SERVER IP /PORT
67.192.153.74:443

DATE OF TEST
June 27th 2016, 23:48 CEST

OPTIONS

Download PDF

Refresh results

The server prefers cipher suites supporting Perfect-Forward-Security Good configuration


The server provides HTTP Strict Transport Security Good configuration

Consider reviewing the set of supported cipher suites Non-compliant with NIST guidelines

<https://www.htbridge.com/ssl>

© 2016 All rights reserved. Online Trust Alliance (OTA)

LEARN • INNOVATE • COLLABORATE



Slide 24

Security Score Trends

SITE & SERVER SECURITY SITE SECURITY SCORES

	2013	2014	2015	2016
Internet Retailer Top 100	85.3	81.9	85.7	89.6
Internet Retailer Top 500	85.1	83.3	85.3	88.3
FDIC 100	85.0	86.5	83.0	88.3
Federal 50	73.2	70.5	83.6	91.6
Consumer 100	82.1	86.2	86.1	89.9
News 100	-	83.2	83.0	85.0
OTA Members	87.1	86.8	89.8	92.1

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 25



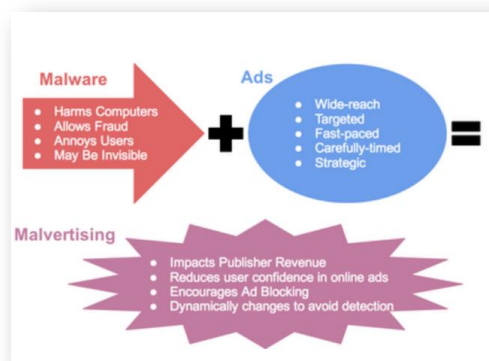
LEARN • INNOVATE • COLLABORATE

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

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 26



LEARN • INNOVATE • COLLABORATE

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

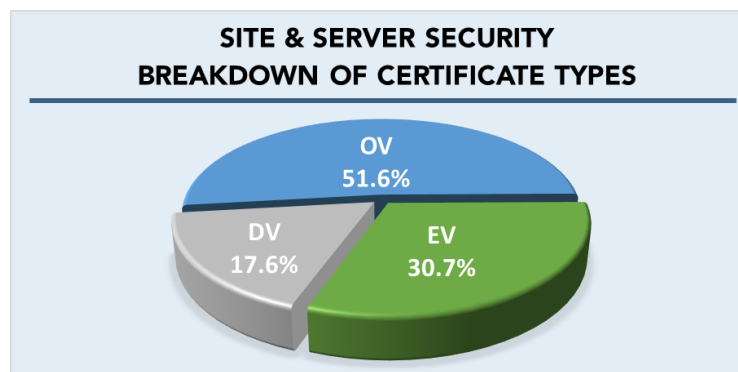
© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 27



LEARN • INNOVATE • COLLABORATE

Concerns – Certificate Type



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

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 28



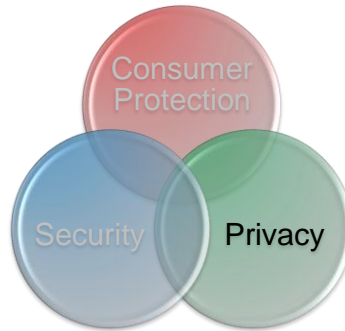
LEARN • INNOVATE • COLLABORATE

Privacy

- **Base points** *Italics = new for 2016*
 - 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

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 29



LEARN • INNOVATE • COLLABORATE

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

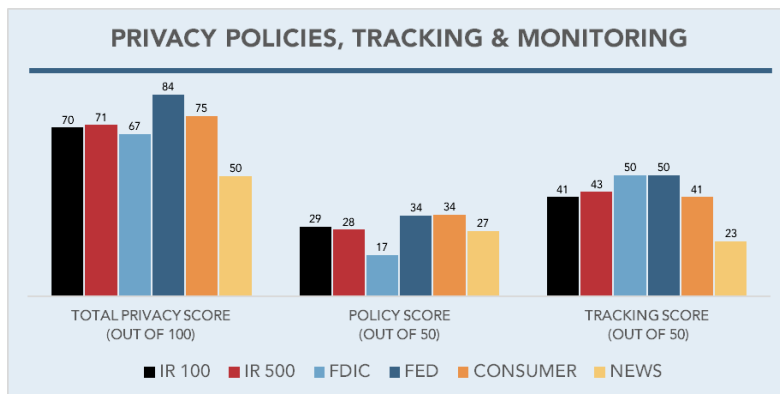
© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 30



LEARN • INNOVATE • COLLABORATE

Privacy – Missing Link

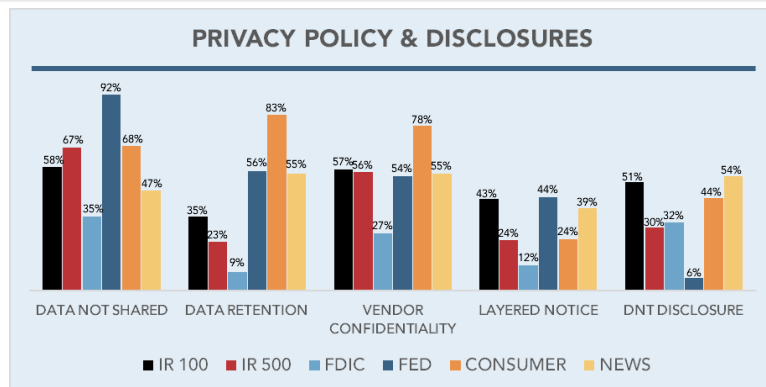


© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 31

LEARN • INNOVATE • COLLABORATE

Privacy – Missed Opportunities



Bonus items

- 1.3% include icons, 4.5% localize their policy
- 73.7% date stamp, yet only 4.1% post older revisions

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 32

LEARN • INNOVATE • COLLABORATE

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

© 2016 All rights reserved. Online Trust Alliance (OTA)



LEARN • INNOVATE • COLLABORATE

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

© 2016 All rights reserved. Online Trust Alliance (OTA)



LEARN • INNOVATE • COLLABORATE

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

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 35



LEARN • INNOVATE • COLLABORATE

Next Steps

- Email Authentication Deep Dive – July 20
<https://attendee.gotowebinar.com/register/1141334127128392450>
- 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>

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 36



LEARN • INNOVATE • COLLABORATE

Back Up Slides

UNDERWRITERS



© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 37



LEARN • INNOVATE • COLLABORATE

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

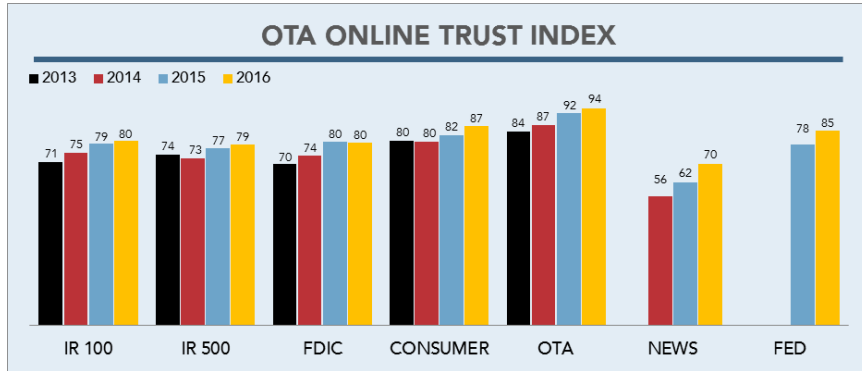
© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 38



LEARN • INNOVATE • COLLABORATE

Trust Index Trends

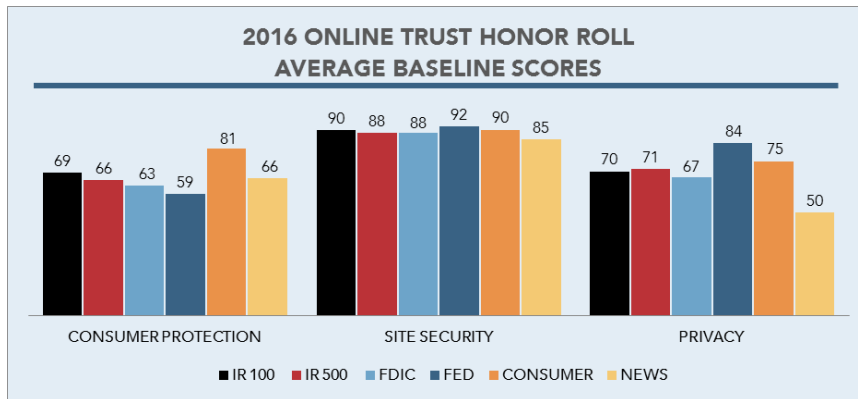


© 2016 All rights reserved. Online Trust Alliance (OTA)



LEARN • INNOVATE • COLLABORATE

Baseline Scores

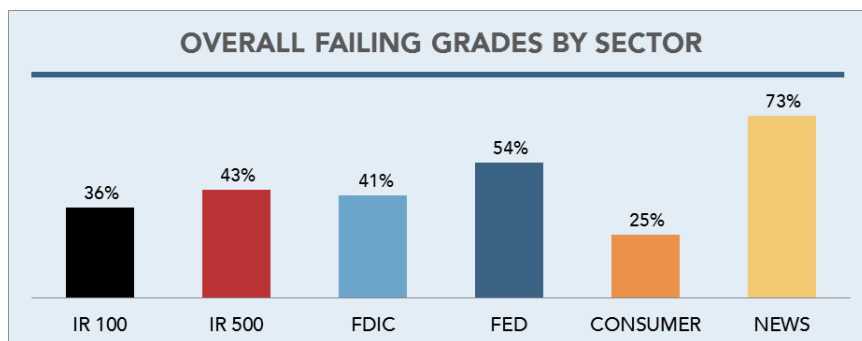


© 2016 All rights reserved. Online Trust Alliance (OTA)



LEARN • INNOVATE • COLLABORATE

Failing Grades By Sector



- Reasons for failure varied widely across sectors

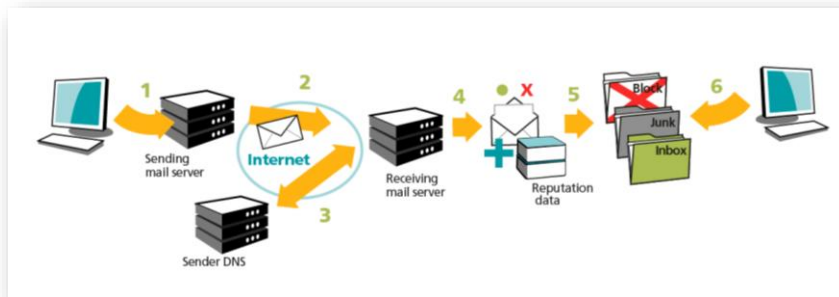
© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 41



LEARN • INNOVATE • COLLABORATE

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**

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 42



LEARN • INNOVATE • COLLABORATE

Email Authentication Adoption

CONSUMER PROTECTION BOTH SPF AND DKIM

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

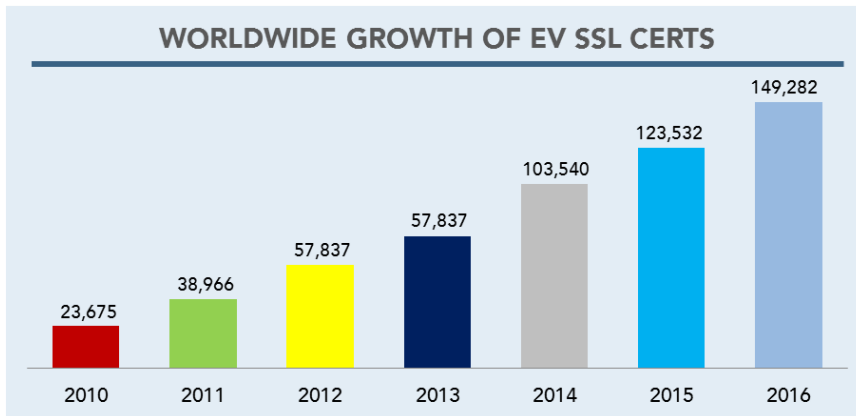
© 2016 All rights reserved. Online Trust Alliance (OTA)



LEARN • INNOVATE • COLLABORATE

SSL Growth

WORLDWIDE GROWTH OF EV SSL CERTS



© 2016 All rights reserved. Online Trust Alliance (OTA)

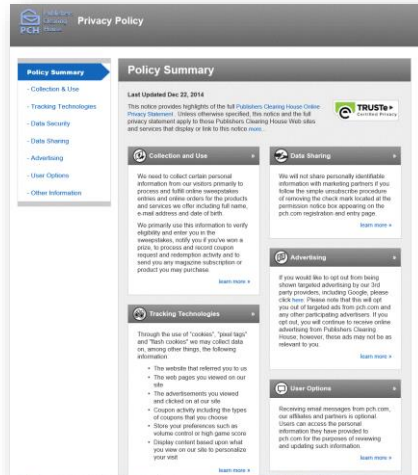


LEARN • INNOVATE • COLLABORATE

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



© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 45 Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

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.~~

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 46 Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

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 sites does not offer any persistent and universal provisions to opt-out of data collection, tracking and/or sharing.
- XYZ honors a DNT settings, 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.