2016 Online Trust Audit & Honor Roll Methodology

March 23, 2016

Jeff Wilbur
Chairman, OTA

Craig Spiezle
Executive Director & President, OTA

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

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 awareness and preference for best practices**

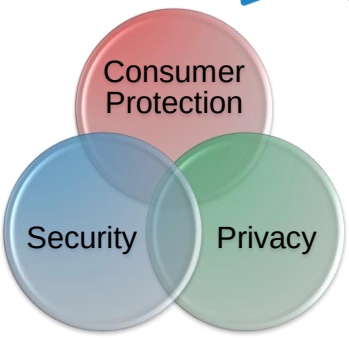
© 2016 All rights reserved. Online Trust Alliance (OTA)

LEARN • INNOVATE • COLLABORATE

© 2015. All rights reserved. Online Trust Alliance (OTA)

Honor Roll Overview

- **Audit of 1,000 web sites** *Italics* = new in 2016
  - FDIC Banking 100
  - Internet Retailer 500
  - Top 50 Social *(rename and expand to 100)*
  - Top 50 News/Media
  - Top 50 Federal Gov't
  - OTA Members
  - IoT 50 (Home automation, Wearables)
  - 2016 Presidential Candidates
- **Scoring**
  - Up to 100 points in each category
  - 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



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

Online Trust Alliance
LEARN • INNOVATE • COLLABORATE

Expanding the Social 50

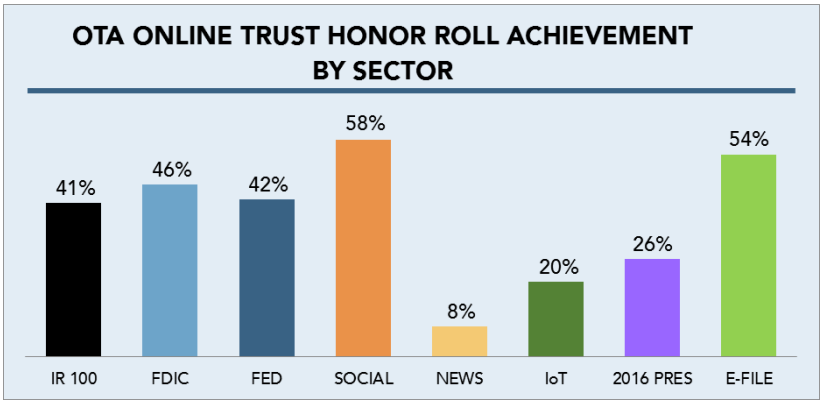
- Renaming to "Consumer Services" or something similar
- Expanding to 100, including top sites in
  - Social networks
  - Image/file sharing
  - Dating
  - Gaming
  - Jobs/career
  - Review/reference
  - Free IRS e-file sites
  - ID theft/credit monitoring
  - Travel
  - Blogging
  - Other miscellaneous

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

Online Trust Alliance
LEARN • INNOVATE • COLLABORATE

© 2015. All rights reserved. Online Trust Alliance (OTA)

Where are We Today?



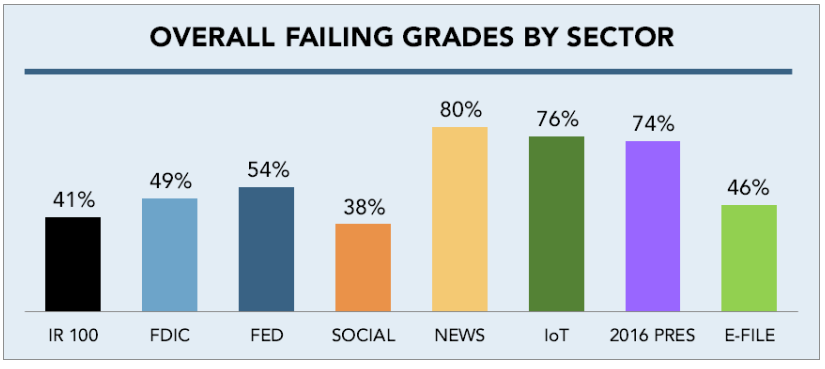
OTA members – 92.5%

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

Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Where are We Today?



OTA members – 3.1% due to inadequate email authentication practices

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

Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

© 2015. All rights reserved. Online Trust Alliance (OTA)

Top of The Class in 2015

Ranked #1
of all 800 sites across all sectors

Online Retailers

Social

Federal

Banking

News

IoT

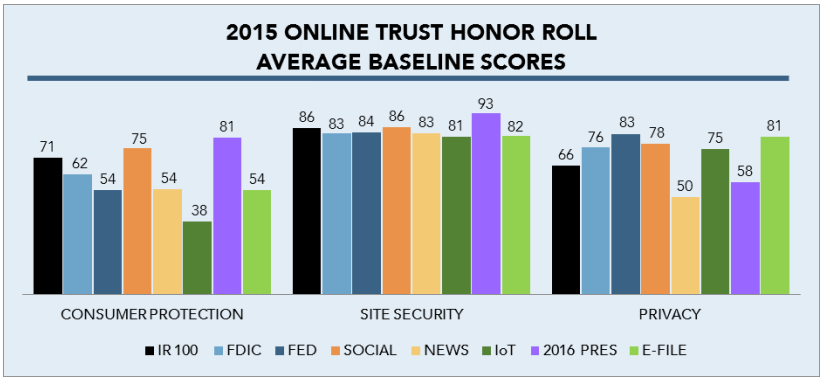
© 2016 All rights reserved. Online Trust Alliance (OTA)

Internet Retailer Top 10

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

© 2015. All rights reserved. Online Trust Alliance (OTA)

Average Baseline Scores



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

Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Summary of Changes

	Baseline	Bonus/Penalty
Consumer Protection	Increased weight of SPF/DKIM at TLD	
	Increased weight on DMARC reject	
		Bonus for IPv6 support
		Penalty for malvertising incident
		Assessing terms/display of “native” advertising
Site Security	Component failure in SSL assessment = overall failure	
		Penalty for DV cert
		Increased bonus for AOSSL
		Penalty for malvertising incident
Privacy	DNT disclosure part of baseline	
	Layered policy part of baseline	

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

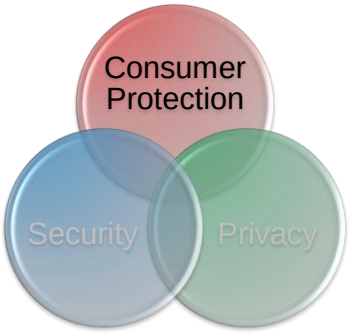
Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

© 2015. All rights reserved. Online Trust Alliance (OTA)

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?

- Will also assess delineation (terms/display) of "native" advertising

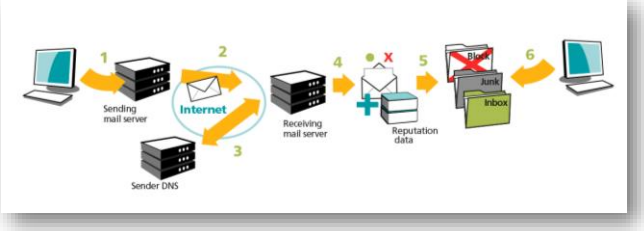
© 2016 All rights reserved. Online Trust Alliance (OTA)

Online Trust Alliance
LEARN • INNOVATE • COLLABORATE

Consumer Protection - Eauth

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)

Online Trust Alliance
LEARN • INNOVATE • COLLABORATE

© 2015. All rights reserved. Online Trust Alliance (OTA)

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)

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

Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Email Authentication Adoption

2015/2016 AUDIT RESULTS BY SECTOR
CONSUMER PROTECTION ADOPTION

	IR100	FDIC	FED	SOCIAL	NEWS	IoT	2016 PRES	E-FILE
SPF (any)	94%	87%	80%	92%	80%	62%	100%	69%
SPF (TLD)	85%	73%	70%	92%	62%	52%	91%	62%
DKIM (any)	93%	68%	50%	78%	64%	30%	100%	62%
DKIM (TLD)	31%	30%	28%	56%	16%	14%	78%	38%
SPF and DKIM	90%	63%	48%	76%	56%	30%	100%	62%
DMARC Record	20%	24%	14%	48%	10%	2%	4%	38%
DMARC (R or Q)*	15%	21%	14%	58%	20%	0%	0%	20%
TLS	42%	38%	38%	36%	14%	24%	57%	31%
DNSSEC	0%	1%	90%	0%	4%	4%	0%	0%
Domain Lock	100%	97%	100%	94%	92%	88%	96%	92%

- Increasing weight on support of SPF and DKIM at top-level domain

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

Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

© 2015. All rights reserved. Online Trust Alliance (OTA)

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://otalliance.org/best-practices/transport-layered-security-tls-email

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

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

IPv6 Support

- Encryption and integrity-checking used in current VPNs is a standard component in IPv6, available for all connections and supported by all compatible devices and systems.
- Widespread adoption of IPv6 will therefore make man-in-the-middle attacks significantly more difficult.

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

© 2015. All rights reserved. Online Trust Alliance (OTA)

Assessing Native Advertising

Conceptual Framework - Display & Search Advertising		
Acceptable	**Possibly Unclear**	**Unacceptable**
	⟷	
Ad		Promoted
Advertisement		Promoted Stories
Paid Advertisement		Suggested content
Sponsored Advertising Content		Ad icon embedded with no words
Paid Post (or Positing)		Featured Content
		Promoted Content
Presented by		Sponsored Topics
Brought to you by		
Promoted by		
Sponsored by		
(variations of these)		(variations of these)

- Assess terms per the framework above
- Is it “clear and conspicuous”?

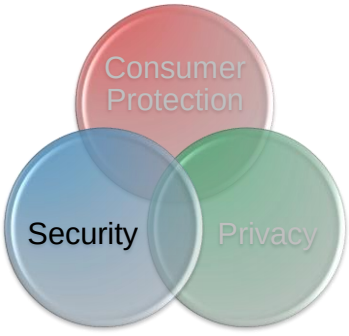
© 2016 All rights reserved. Online Trust Alliance (OTA)

Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Site Security

- Base points — *Italics* = new for 2016
  - Server & SSL implementation
  - *Component failure = overall failure*
- Bonus points
  - EV SSL
  - AOSSL *(increased weight)*
- Penalty points
  - XSS / iFrame vulnerabilities
  - Malware
  - Malicious links
  - Bot risk
  - *DV certificate*



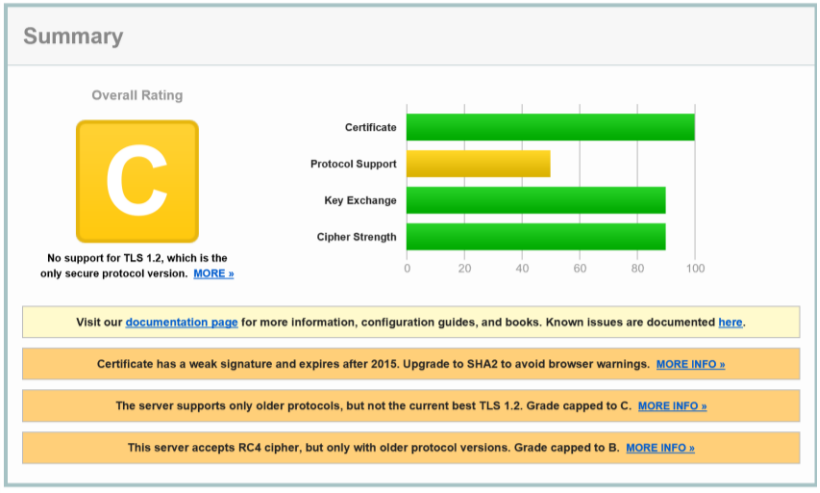
© 2016 All rights reserved. Online Trust Alliance (OTA)

Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

© 2015. All rights reserved. Online Trust Alliance (OTA)

Component Failure = Fail



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

Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

AOSSL – Bonus Points

Always On SSL (AOSSL)

- Helps secure sensitive data, especially for users of public Wi-Fi hot spots. Counters sidejacking which allows hackers to intercept cookies (typically used to retain user-specific information such as username, password and session data) when they are transmitted without the protection of SSL encryption.
- https://otalliance.org/resources/always-ssl-aossl
- Increased weight in 2016

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

Online Trust Alliance

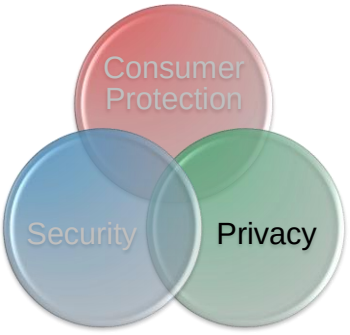
LEARN • INNOVATE • COLLABORATE

© 2015. All rights reserved. Online Trust Alliance (OTA)

Privacy

Italics = new for 2016

- Base points
  - Privacy policy
  - Third-party trackers on site
  - *DNT disclosure*
  - *Layered notices*
- Bonus points
  - Use of Icons
  - Tag mgmt or privacy solution
  - Honoring DNT
- Penalty points
  - WHOIS (if Private vs Public)
  - Data Breach Incidents
  - FTC / State Settlements



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

OTA Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Do Not Track – DNT

- Required disclosure in California as of 1/1/14
- The standard has moved through the W3C process
- Baseline points if disclosure is visible on the privacy page
- Added points if sites state they honor the setting and do not collect or share any data with third parties
  - 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)

OTA Online Trust Alliance

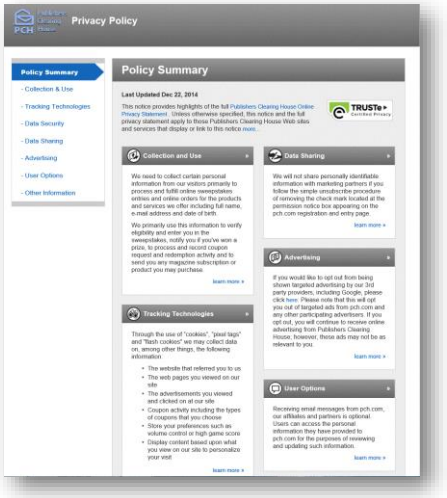
LEARN • INNOVATE • COLLABORATE

© 2015. 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



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

Privacy Policy Disclosures

- Data Collection
- Data Retention
- Data Usage
- Data Sharing
- Layered / Short Notice
- Tracking of Revisions & Date Stamping
- DNT Disclosure
- Notification of Sharing
- **Total possible 50 points**

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

© 2015. All rights reserved. Online Trust Alliance (OTA)

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)

Sharing with Third Parties

- Except as otherwise described in this statement, personal information you provide will not be shared outside of XYZ without your permission. To the extent we are legally permitted to do so, we will take reasonable steps to notify you in the event that we are required to provide your personal information to third parties as part of legal process

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

© 2015. All rights reserved. Online Trust Alliance (OTA)

Timing

- Next 30 days
  - Review methodology
  - Engage your teams and optimize your site, domain and policies
- April 15 – Begin testing
- Mid-June – Release report

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

Tools & Resources

- Online Trust Honor Roll https://otalliance.org/HonorRoll
  - Methodology, past reports and related resources https://otalliance.org/initiatives/2016-methodology
- 2016 Data Protection & Breach Readiness Guide https://otalliance.org/Breach
- Email Security https://otalliance.org/eauth
- Always On SSL SSL Best Practices https://otalliance.org/aossl

OTA +1 425-455-7400

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

© 2015. All rights reserved. Online Trust Alliance (OTA)