2015 Online Trust Audit & Honor Roll
Email Practices Deep Dive

July 7, 2015

Mike Jones
Director
Agari

Brian Westnedge
Sr. Director, Client Services
Return Path

Craig Spiezle
Executive Director & President
Online Trust Alliance

Jeff Wilbur
VP Marketing
Iconix

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.

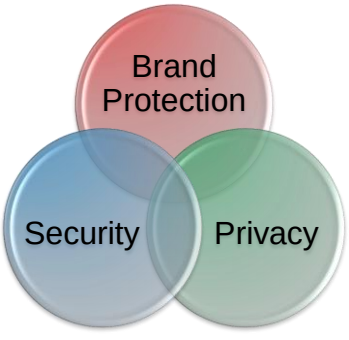
Online Trust Audit & Honor Roll

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** *Italics* = new in 2015
  - 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

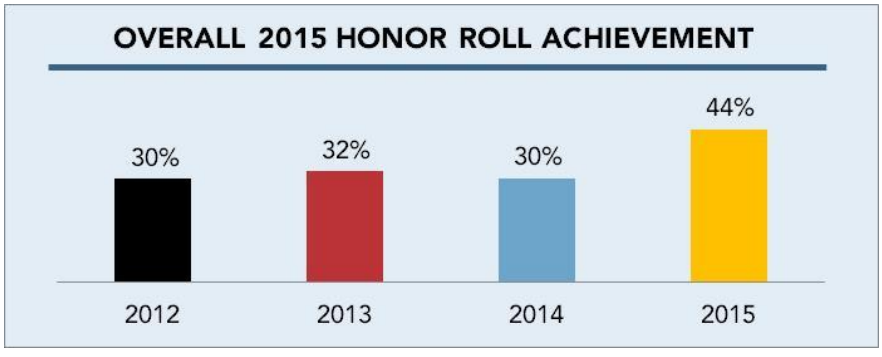


Collaborative & Open Process

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

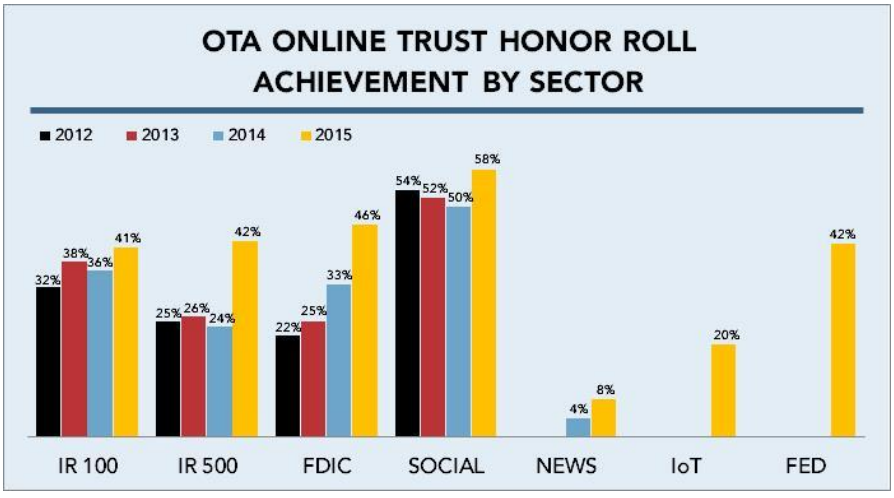
- *Powered in part by leading companies including;*
  - Agari, AVG Technologies, DigiCert, Disconnect
  - Distil Networks, Ensighten, GlobalSign, High-Tech Bridge SA
  - IID, Microsoft, Return Path, SiteLock, SSL Labs, Symantec,
  - ThreatWave, TRUSTe & VERISIGN

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 Alliance

LEARN • INNOVATE • COLLABORATE

Top of The Class

Ranked #1
of all 800 sites across all sectors

AMERICAN GREETINGS
Online Retailers

Social

FDIC
Federal

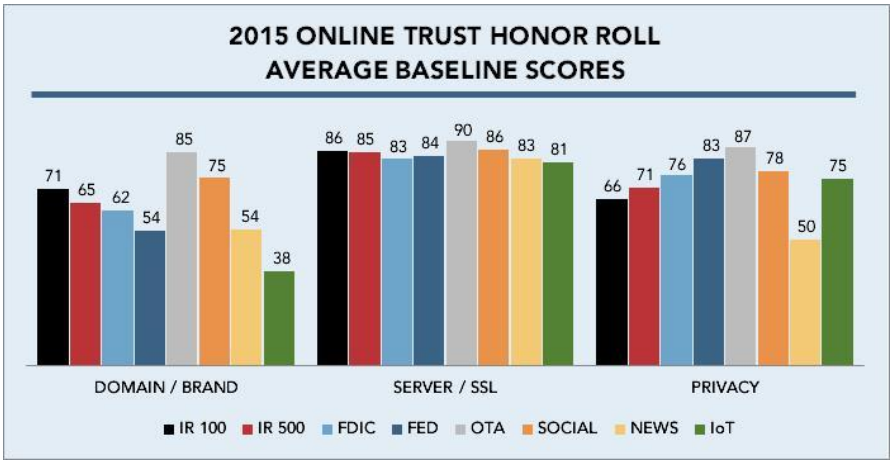
USAA
Banking

Bloomberg Businessweek
News

dropcam
IoT

LEARN • INNOVATE • COLLABORATE

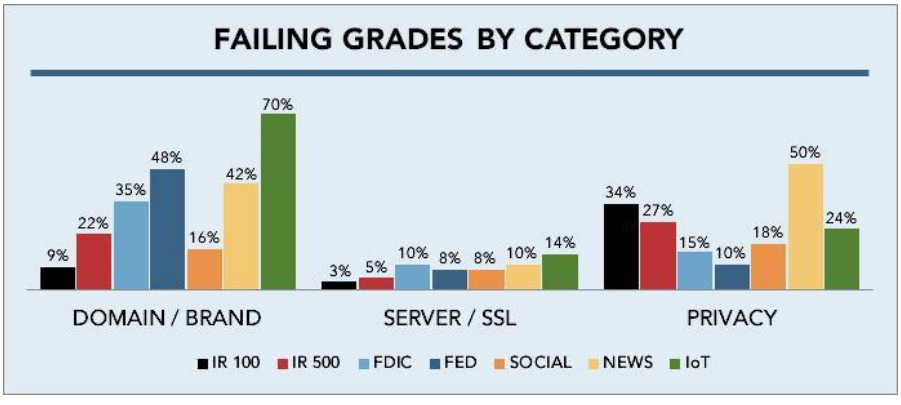
Baseline Category Scores



OTA Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Reasons for Failure

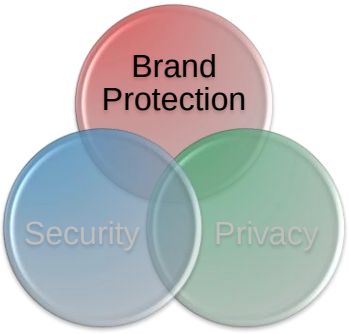


OTA Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Brand Protection

- Base points — *Italics* = new in 2015
  - 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)



Best practices to help detect and prevent malicious and spoofed email and protect corporate domains

OTA Online Trust Alliance

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)

OTA Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Transport Layer Security

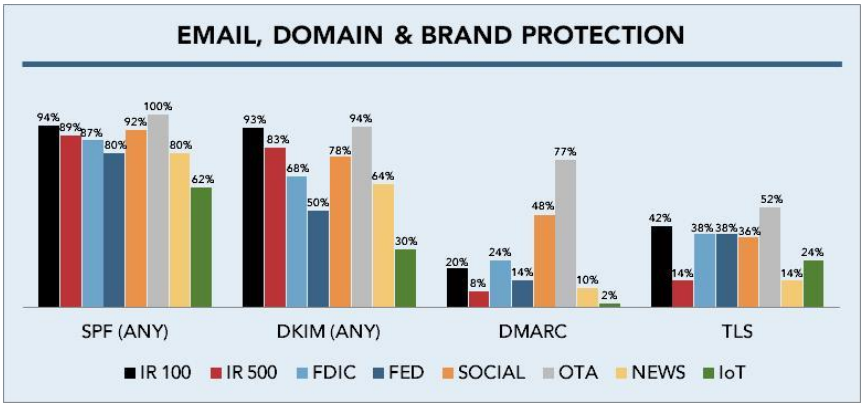
Rapidly being adopted standard for secure email.

- 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/

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

DOMAIN & BRAND PROTECTION
EITHER SPF OR DKIM

	2012	2013	2014	2015
Internet Retailer Top 100	97%	96%	100%	97%
Internet Retailer Top 500	91%	88%	98%	95%
FDIC 100	69%	77%	88%	92%
Federal 50	58%	72%	68%	82%
Social 50	96%	98%	96%	94%
OTA Members	99%	100%	98%	100%
News 50	-	-	78%	88%
IoT 50	-	-	-	62%

DOMAIN & BRAND PROTECTION
BOTH SPF AND DKIM

	2012	2013	2014	2015
Internet Retailer Top 100	56%	76%	88%	90%
Internet Retailer Top 500	43%	56%	74%	78%
FDIC 100	34%	49%	49%	63%
Federal 50	10%	20%	22%	48%
Social 50	63%	72%	74%	76%
OTA Members	59%	69%	83%	94%
News 50	-	-	50%	56%
IoT 50	-	-	-	30%

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

SPF Adoption Analysis

DOMAIN & BRAND PROTECTION
SPF ADOPTION

	2012 Top Level Domains	2013 Top Level Domains	2014 Top Level Domains	2014 Any SPF	2015 Top Level Domains	2015 Any SPF
Internet Retailer Top 100	67%	77%	78%	96%	85%	94%
Internet Retailer Top 500	63%	69%	75%	91%	77%	89%
FDIC 100	60%	62%	68%	79%	73%	87%
Federal 50	50%	60%	62%	62%	70%	80%
Social 50	96%	94%	94%	94%	92%	92%
OTA Members	99%	98%	95%	97%	100%	100%
News 50	-	-	58%	72%	62%	80%
IoT 50	-	-	-	-	52%	62%

- 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

DOMAIN AND BRAND PROTECTION DKIM ADOPTION	2012	2013	2014		2015	
	Top Level Domains	Top Level Domains	Top Level Domains	Any DKIM	Top Level Domains	Any DKIM
Internet Retailer Top 100	23%	26%	33%	92%	31%	93%
Internet Retailer Top 500	16%	18%	27%	81%	27%	83%
FDIC 100	27%	30%	27%	58%	30%	68%
Federal 50	16%	22%	20%	28%	28%	50%
Social 50	56%	62%	56%	76%	56%	78%
OTA Members	46%	58%	73%	84%	78%	94%
News 50	-	-	14%	56%	16%	64%
IoT 50	-	-	-	-	14%	30%

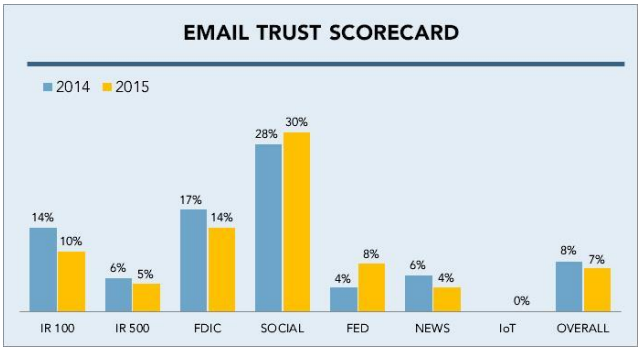
- Overall DKIM grew in all sectors, with significant growth in Fed, FDIC, News and OTA
- DKIM at TLD lags significantly and was ~flat in most sectors

DMARC Adoption Analysis

DOMAIN AND BRAND PROTECTION DMARC ADOPTION	2012	2013	2014	2015	
	Record	Record	Record	Record	R or Q
Internet Retailer Top 100	2%	5%	15%	20%	15%
Internet Retailer Top 500	2%	3%	6%	8%	22%
FDIC 100	1%	13%	21%	24%	21%
Federal 50	0%	4%	6%	14%	14%
Social 50	19%	22%	36%	48%	58%
OTA Members	34%	44%	59%	77%	12%
News 50	-	-	10%	10%	20%
IoT 50	-	-	-	2%	0%

- 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

OTA Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

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 “siloed”

OTA Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

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/eauth
- Resources https://otalliance.org/resources/ota-spf-dmarc-resources-tools
- TLS https://otalliance.org/best-practices/transport-layered-security-tls-email

- Online Trust Honor Roll https://otalliance.org/HonorRoll
  - Methodology, past reports and related resources
- SSL Server Test https://ota.ssllabs.com
- Always On SSL (AOSSL) - https://otalliance.org/aossl
- 2015 Data Protection & Breach Readiness Guide https://otalliance.org/Breach
- Internet of Things – https://otalliance.org/IoT

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