RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Walking The Security & Privacy Talk

Moving from Compliance to Stewardship

02/28/2014

SESSION ID: DSP-F01

Craig Spiezle (moderator)
Executive Director & President, Online Trust Alliance

Rick Andrews
Senior Technical Director for Trust Services, Symantec

Mike Hammer
Web Operations Security, American Greetings

Jeff Wilbur
VP Marketing, Iconix Inc.

Online Trust Honor Roll

Objectives:

- ***Move from a "compliance" mindset to "stewardship"***
- **Recognize leadership of sites and apps that implement security and privacy practices protecting users' data**
- **Incentivize businesses and developers to enhance their security, data protection and privacy practices**
- **Increase awareness and preference for best practices**

Why Care?


Federal Trade Commission
Privacy Policy
Protecting America's Consumers
Home
News
Competition
Consumer Protection
Economics
General Counsel
Actions
About Public Affairs | Public Events | Speeches | Webcasts | Reporter Resources | Noticias en
For Release: 12/05/2013
Android Flashlight App Developer Settles FTC Charges It Deceived Consumers
'Brightest Flashlight' App Shared Users' Location, Device ID Without Consumers' Knowledge


Weak Server Side Controls
71%
of vulnerabilities resided on the web server

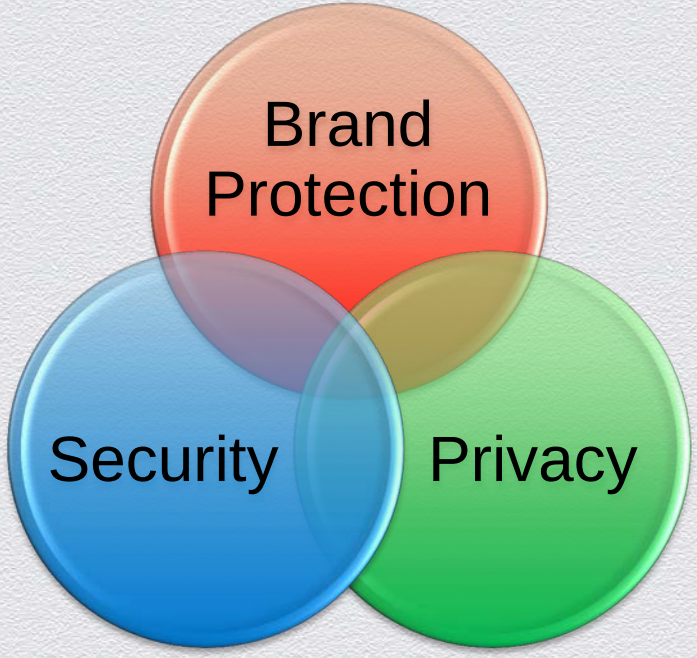

TARGET

Insecure Encryption & Data Storage
75%
of applications do not use proper encryption when storing data


The Telegraph
Home News World Sport Finance Comment Culture Travel Life Women Fashion
Technology News | Technology Companies | Technology Reviews | Video Games | Technology Video
HOME » TECHNOLOGY » INTERNET SECURITY
Four in five top Android and iOS apps 'have been hacked'
All of the top 100 paid Android apps and 56 per cent of the top 100 paid iOS apps have been compromised, according to new research

Honor Roll Overview

- **Analysis of ~800 web sites**
  - FDIC Banking 100
  - Internet Retailer 500
  - Top 50 Social, Gov't & OTA Members
- **Up to 100 points in each of the three major categories**
- **Bonus Points**
  - **Emerging practices**
- **Negative Scoring**
  - **Data loss incident**
  - **Fines or settlement**
  - **Other**



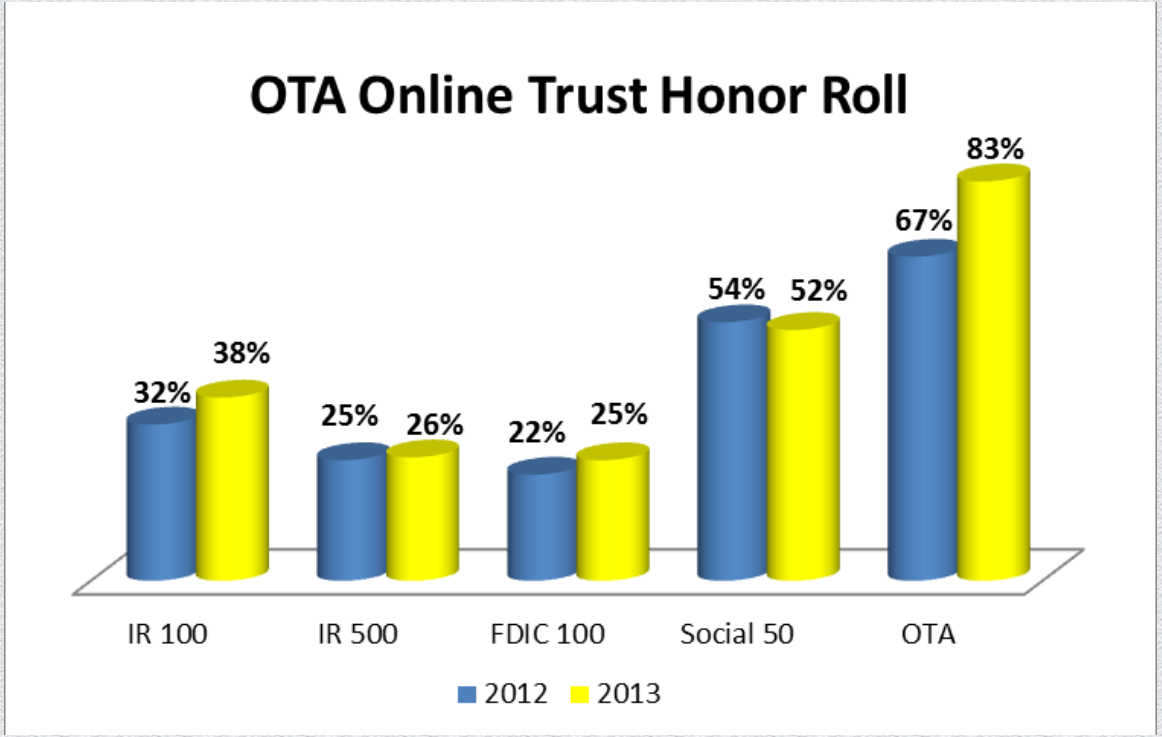
OTA ONLINE TRUST HONOR ROLL 2013 RECIPIENT

OTA Online Trust Alliance

#RSAC

RSACONFERENCE2014

Honor Roll Achievement by Segment

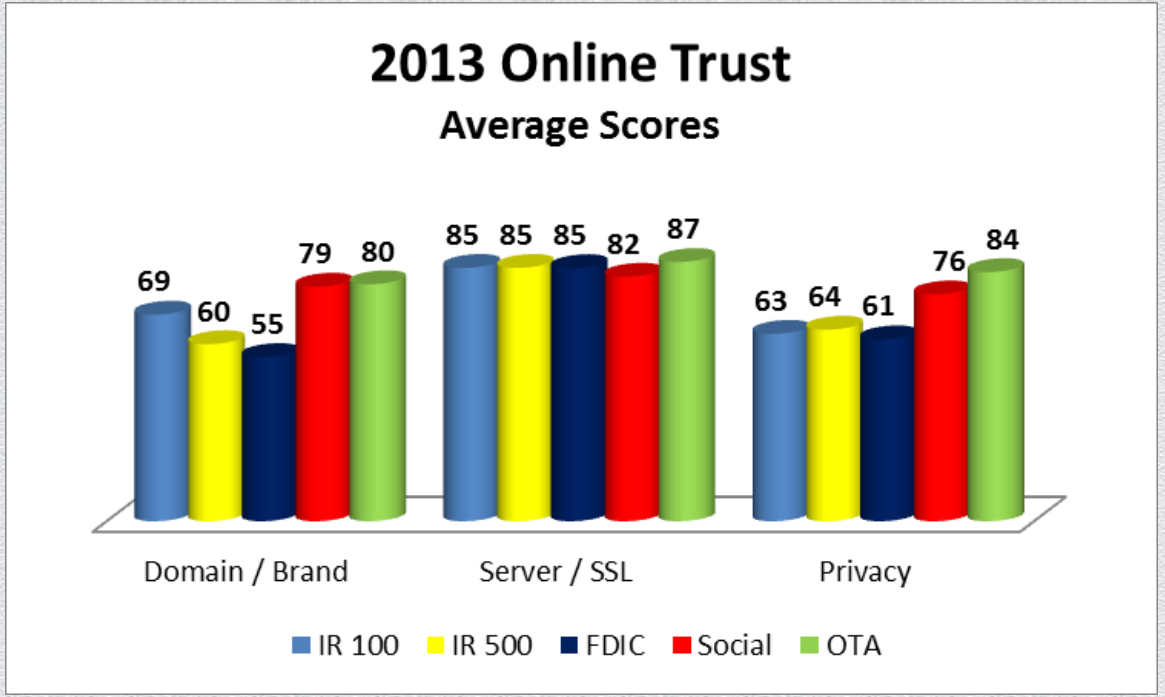


Internet Retailer 500 “Top 10”

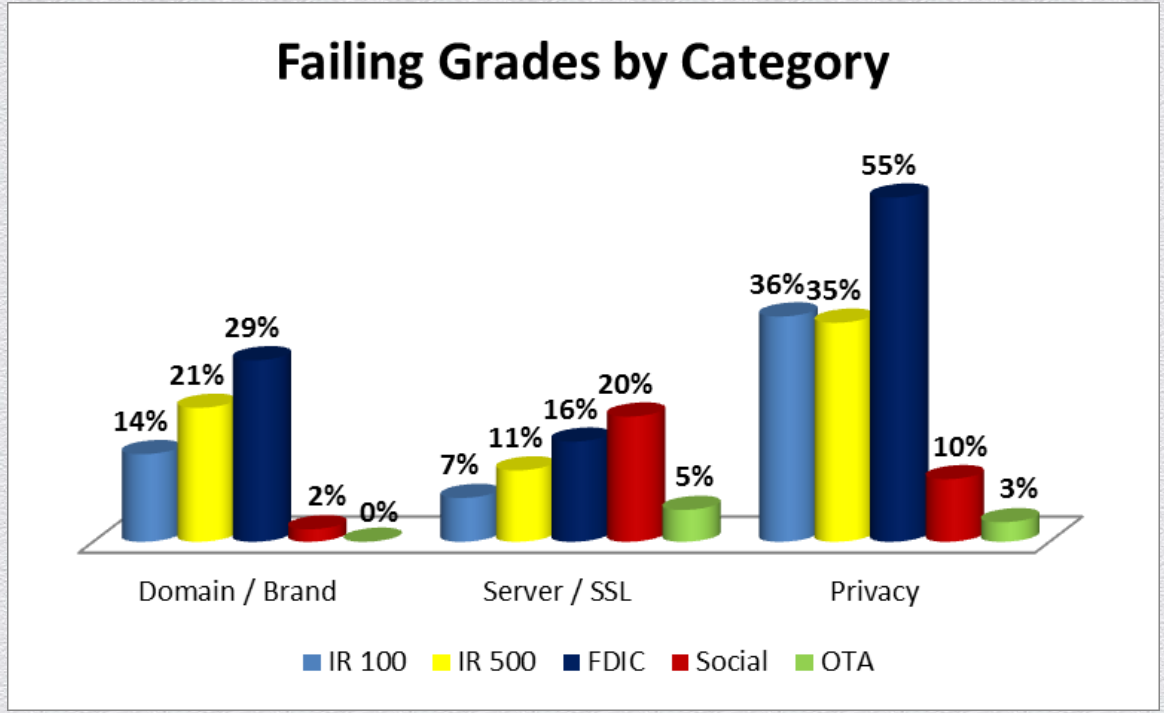
#1 Amazon to #453 BAMM.com based on revenues

OTA Online Trust Alliance
ONLINE TRUST HONOR ROLL
2013 RECIPIENT

Category Scores by Segment



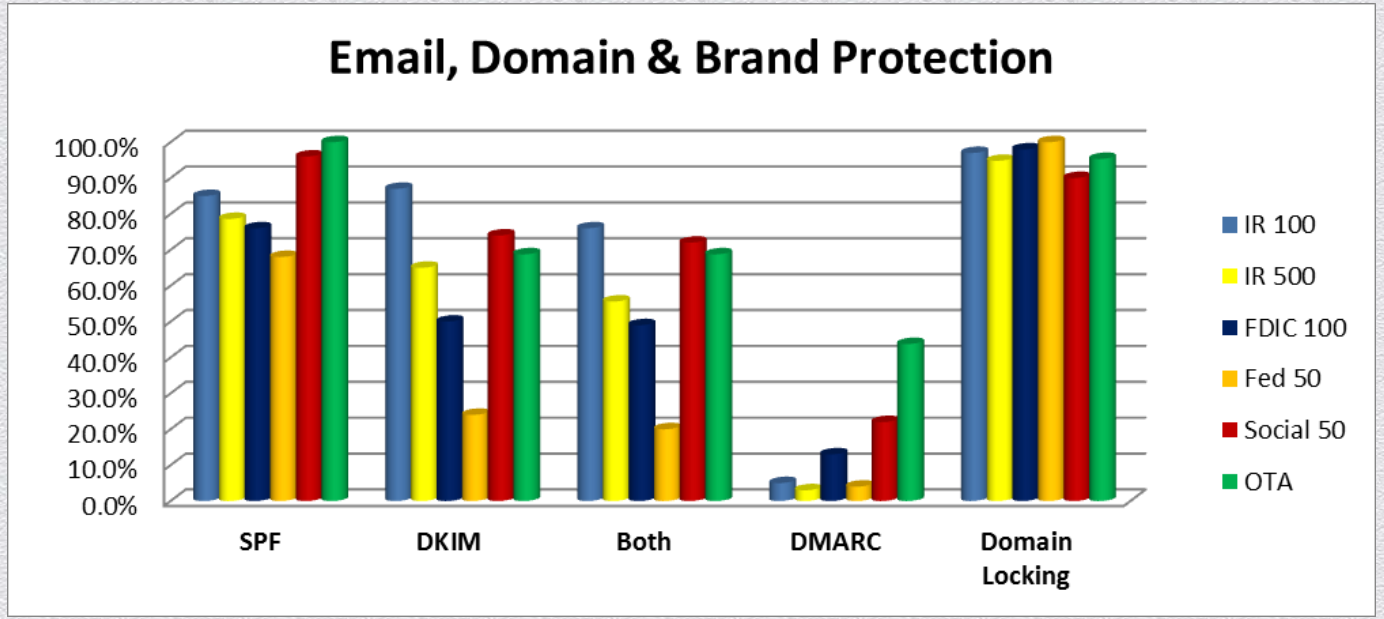
Failing Grades



Domain, Brand & Email Protection

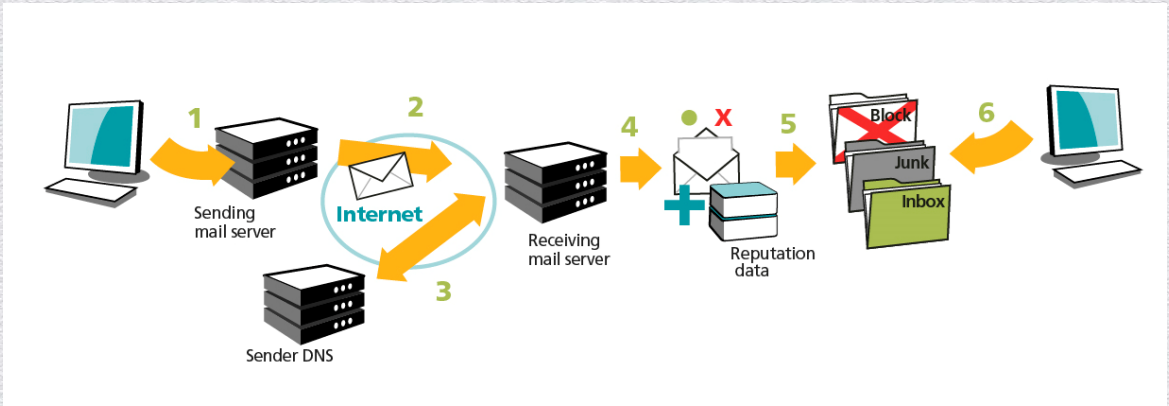
Critical Issues

- Parent or TLD vs delegated subdomains (i.e. email.foo.com)
- Parked Domains
- Ongoing Management



DKIM & SPF: Better Together

- **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



DMARC

- 2 years since release
- High adoption by ISPs and email marketers
- Low adoption by segments most phished
- “Reject & Quarantine” policy assertions lagging

DMARC Adoption				
	May/2013		Feb/2014	
	DMARC	R / Q	DMARC	R / Q
FDIC 100	13.0%	15.4%	16.0%	18.8%
Interent Retailer 500	3.0%	26.7%	4.0%	30.0%

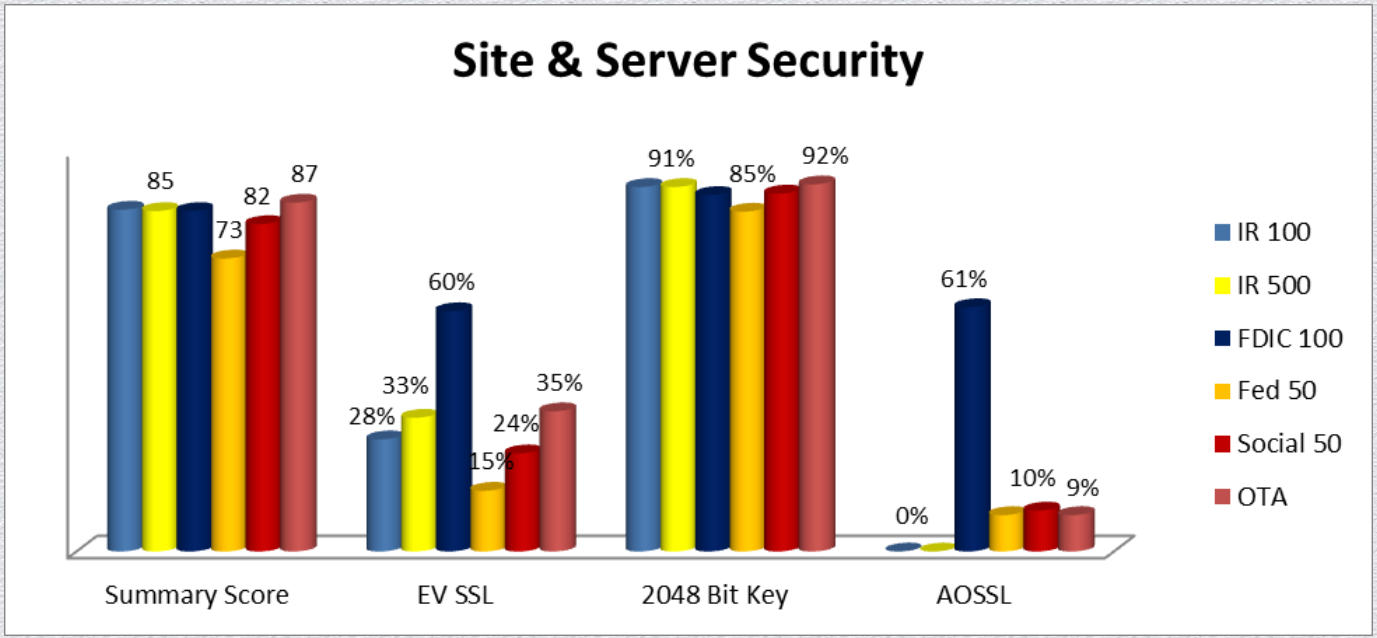
DMARC = Domain-based Message Authentication, Reporting & Conformance
https://otalliance.org/eauth.html

Spear Phishing & Brand Protection

- *"DMARC was eye-opening for **Twitter,"** said Josh Aberant, Postmaster. "We found massive amounts of abuse from both our domains and look alike domains we'd claimed. Using DMARC is a core component of how we protect our users."*

- *"DMARC has blocked over one hundred thousand messages, helping to protect the Publishers Clearing House brand and consumers from potential email threats," said Sal Tripi, Assistant Vice President of Digital Operations & Compliance at **Publishers Clearing House.** "DMARC is critical to future success of not only our business, but the vitality of the online marketplace in general."*

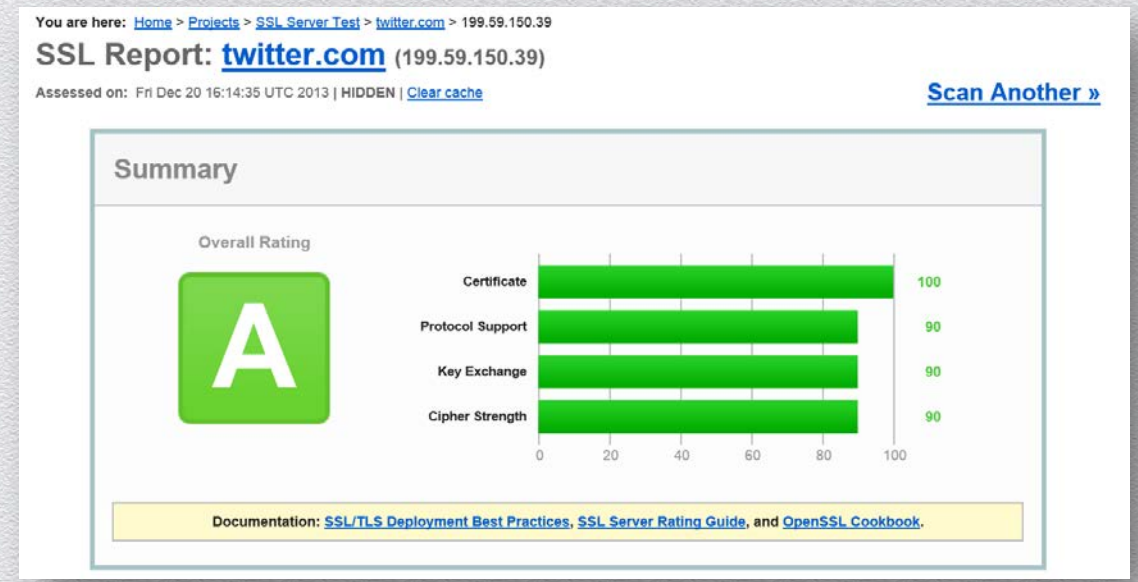
Site Security



Server Configuration Analysis

Common Issues

- Support of TLS 2.0
- “Beast Attack” vulnerabilities
- Mismatched certs
- Cross site scripting
- iframes exploits
- 1024 certs

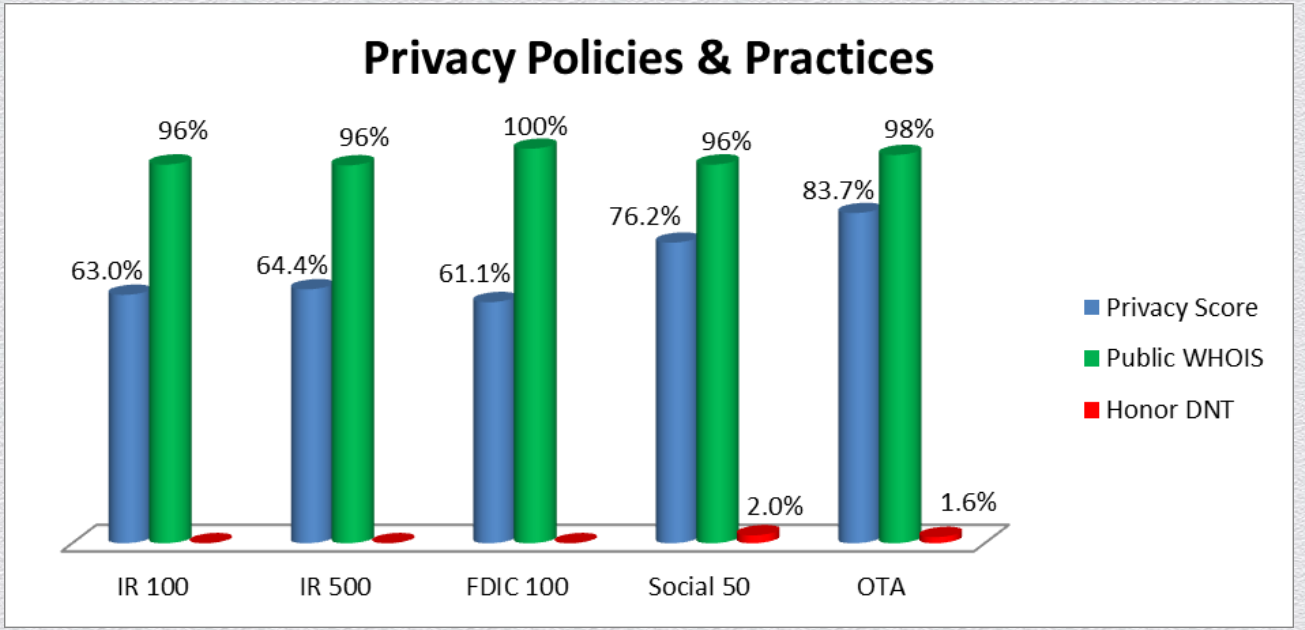


Data Sources: SSL Labs - https://www.ssllabs.com & High-Tech Bridge https://www.htbridge.com/

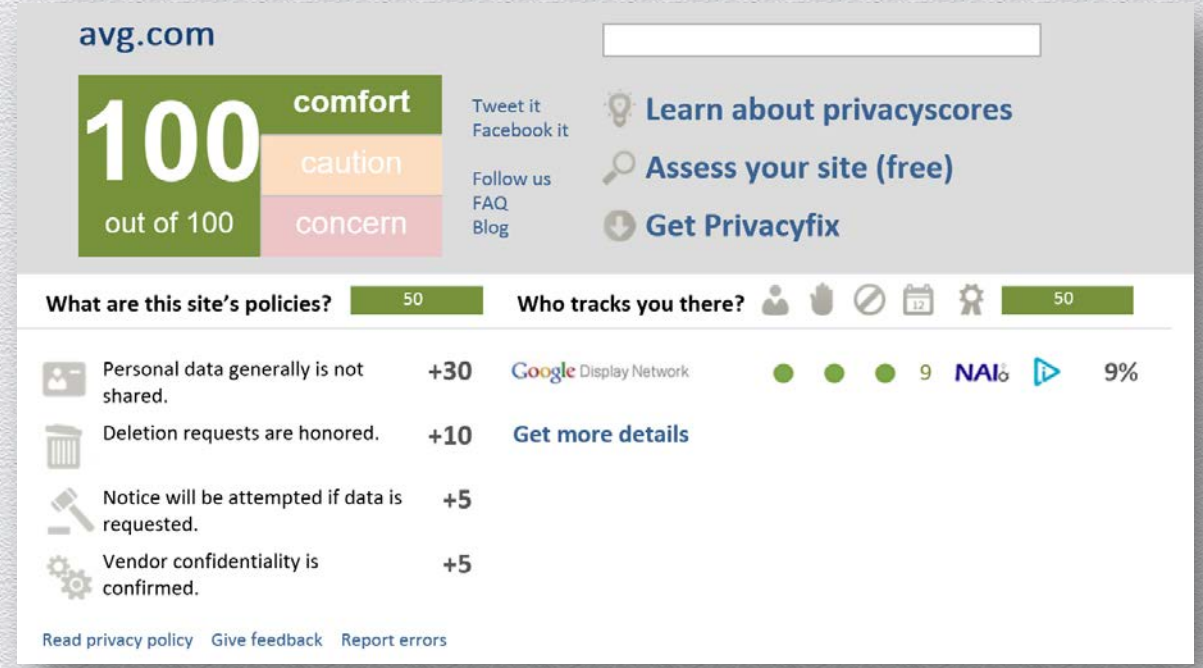
Privacy Policies & Practices

Common Issues

- Policies do not match data collection
- 3rd parties and analytics practices conflict with privacy policies
- Policy not discoverable
- Lack of notification to users on legal disclosure



Privacy Score



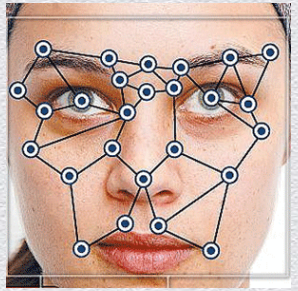
Data Sources: - http://privacyscore.com (AVG) and TRUSTe

Evolution of Threats & Draft 2014 Methodology

Enhanced Criteria, Bonus Points & Scoring

- Brand Protection
- Privacy - DNT, Facial Recognition, Geo Location
- Site Security

- DNS check?
- Bonus Points
- Reporting on Govt Disclosures?



Enhanced SSL Criteria

- Support for TLS 1.2 is required for an A. If not, the grade is capped at B.
- Keys below 2048 are capped at B. (below 1024 receive an F).
- MD5 certificate signatures are considered insecure, and receive an F.
- Two new grades, A+ and A-, to allow for finer grading.
- Warnings; servers with good configuration, one or more warnings, are reduced to an A-
  - Servers not supporting Forward Secrecy with our reference browsers receive a warning.
  - Servers that do not support secure renegotiation receive a warning.
  - Servers that use RC4 with TLS 1.1 or TLS 1.2 protocols receive a warning.

SSL Evolution

- Prepare for the deprecation of SHA-1 move to implement SHA-2
- Implement AOSSL (especially EV SSL and HSTS)
- Begin trials/evaluations/proof-of-concepts for
  - ECC (Elliptical Curve Cryptography)
  - PFS (Perfect Forward Secrecy)
  - CAA (Certification Authority Authorization)

Lessons Learned

Creating a Culture of Stewardship

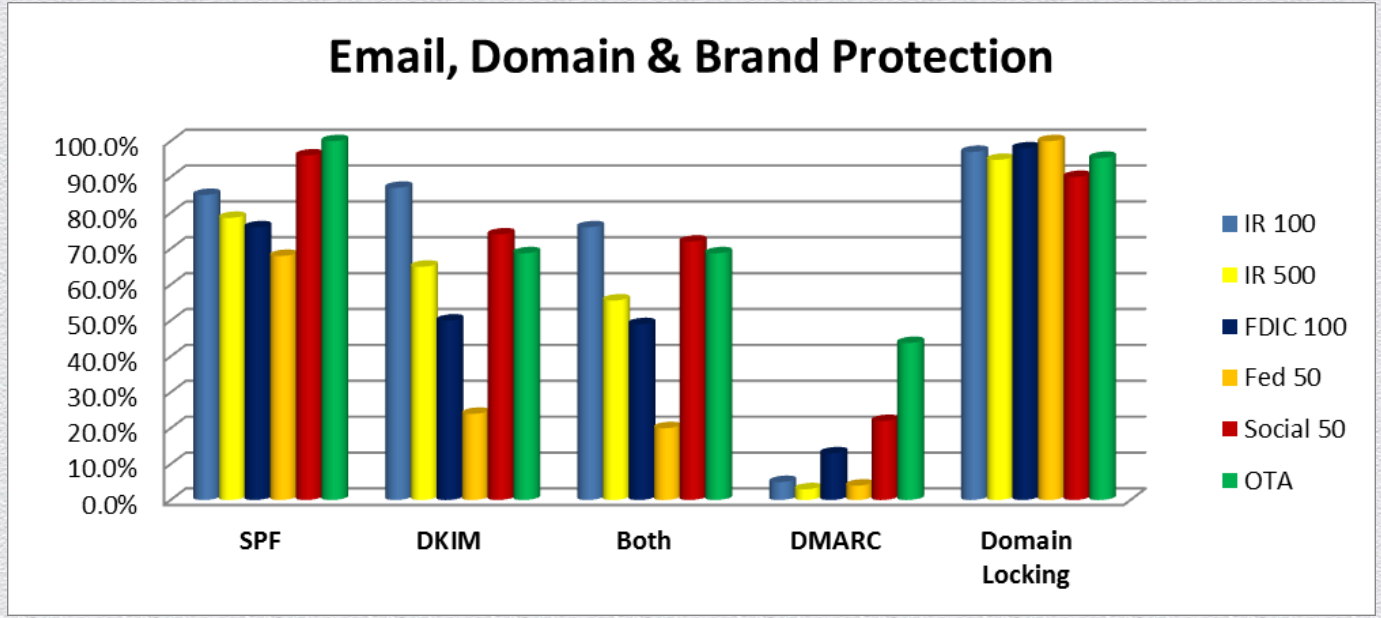
- Getting leadership and team(s) proactively embedded
- Involve subject matter experts
- Needs to be “evergreen”, a continual process
- Need to require rigor with evolving criteria including wish list
- Challenges
  - Visibility
  - Cadence; Momentum & Sustainability
  - Indoctrination of new hires, partners & new vendors

Tools & Resources

- Online Trust Honor Roll https://otalliance.org/HonorRoll.html
- 2014 Data Protection & Breach Readiness Guide https://otalliance.org/Breach.html
- Always On SSL https://otalliance.org/AOSSL.html
- SSL Best Practices https://otalliance.org/ssl.html
- SSL Labs https://ssllabs.com
- Privacy Score http://privacyscore.com/
- Craigs@otalliance.org +1 425-455-7400

Appendix
Back Up Slides

Domain, Brand & Email Protection



Growth of SPF/DKIM Adoption

Either

2013 Domain & Brand Protection Either DKIM or SPF				
	2010	2011	2012	2013
IR 100	76%	84%	97%	96%
IR 500	54%	65%	91%	88%
FDIC 100	55%	59%	69%	77%
Fed 50	32%	38%	58%	72%
Social 50		92%	96%	98%
OTA Members	88%	95%	91%	100%

Both

2013 Domain & Brand Protection Both DKIM and SPF				
	2010	2011	2012	2013
IR 100	24%	42%	56%	76%
IR 500	14%	23%	43%	56%
FDIC 100	22%	23%	34%	49%
Fed Sites	2%	4%	10%	20%
Social 50	-	28%	63%	72%
OTA Members	36%	44%	59%	69%

DKIM Adoption Details

DomainKeys Identified Mail - Adoption Analysis						
	2010	2011	2012	2013		
	Any DKIM	Any DKIM	Any DKIM	Top Level Domains	Sub Domains	Any DKIM
IR 100	37.0%	55.0%	82.8%	**26%**	**81%**	**87%**
IR 500	22.8%	33.4%	69.5%	**18%**	**58%**	**65%**
FDIC 100	29.0%	34.4%	44.0%	**30%**	**38%**	**77%**
Fed 50	4.0%	6.0%	18.0%	**22%**	**6%**	**24%**
Social 50	-	52.0%	63.0%	**62%**	**42%**	**74%**
OTA Members	22.0%	34.5%	57.1%	**58%**	**28%**	**69%**

Methodology – Bonus Points

Always On SSL (AOSSL)

- A best practice to secure sensitive data, especially for users of public Wi-Fi hot spots. With the advent of widely available tools, criminals can "sidejack" cookies and data packets from unsuspecting users. Sidejacking 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.
- See https://otalliance.org/resources/AOSSL/index.html

Methodology – Bonus Points

Domain Name System Security Extension (DNSSEC)

- Testing for DNSSEC was completed using a custom-built tool from Internet Identity (IID) that directly queried DNSSEC records via "dig" requests. Accounting for the risk of DNS errors, the analysis was run twice during the test period.
- Sites adopting DNSSEC receive bonus points. https://otalliance.org/resources/dnssec.html

Methodology – Bonus Points

Do Not Track (DNT)

- Websites who affirm the status of honoring or not honoring the DNT signal asserting a user's request to not collect and share their online data will receive bonus points.
- Sites with no assertion supporting or ignoring the DNT signal composite score will not be impacted.
- As the standard is evolving with the W3C, it is recognized that many sites are reviewing their support. Currently support of DNT is voluntary, but draft legislation has been proposed to require sites to honor the preference.

Methodology – Negative Points

Domain Locking - A security enhancement offered by most registrars to help prevent unauthorized transfers of your domain to another registrar or web host by locking your domain name servers.

- When your domain is locked, you'll be substantially protected from unauthorized third parties who might try to misdirect your name servers or transfer your domain without your permission.
- Sites receive negative points if their domain is not locked.

Methodology – Negative Points

Who Is – Private Registration

- Private Domain Registration Sites that are registered by proxy or private registration received a negative score, reflecting a lack of transparency. While it is recognized that sites may choose to opt-in for private domain name registration, public facing sites are discouraged from doing so and consumers should exercise caution when interacting with sites that do not offer such transparency.