2015 Online Trust Audit & Honor Roll Methodology

Jeff Wilbur
VP Marketing, Iconix

Craig Spiezle
Executive Director & President, OTA

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 ~800 web sites**  
  - FDIC Banking 100
  - Internet Retailer 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
  - Honor Roll = 80% of total points, 55% or better in each category
Internet Retailer Top 10

[Logos of American Greetings, Ancestry.com, Bam!, Big Fish, Jackthreads, Netflix, Newegg, Sony, Walmart, Zulily]
Top of The Class

AMERICAN GREETINGS

#1 of all Online Retailers

Ranked #1
of all 800 sites across all sectors

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

2014 ONLINE TRUST AVERAGE SCORES

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

- **Base points**
  - Email authentication
    - SPF and DKIM at top-level and subdomains
    - DMARC record and policy
  - **Bonus points**
    - TLS for email
    - DMARC reject policy
  - **Penalty points**
    - Domain locking (not locked)

**Italics = new in 2015**

- Can the app or web site be spoofed fooling a consumer to open or 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?

**Brand 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
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)

SPF & DMARC Query Tool

https://otalliance.org/resources/spf-dmarc-record-validator
SPF Record Validation

SPF & DMARC Tools & Record Validator

Tool to validate if SPF and DMARC records have been “published” in a domain’s DNS zone file. The tool will query the DNS of the respective domains and present the records found. Up to 500 domains may be entered.

Enter a list of domains, one per line below. Then select a record type to query. (SPF or DMARC). The tool will query the DNS of the respective domains and present the records found. Up to 500 domains may be entered.

(e.g. domain.com NOT @ example.com or www.domain.com)

DMARC Records

Domain: A
Submit Query

Pipe Delimited Data Output

DMARC Validation

DMARC Record for ast.com

DMARC Record for linkedin.com

DMARC Record for twitter.com

DMARC Record for yahoo.com

DMARC Record for google.com

DMARC Record for badoo.com

Lookup Results

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

SPF & DMARC Tools & Record Validator

Tool to validate if SPF and DMARC records have been "published" in a domain's DNS zone file. The tool will query the DNS of the respective domains and present the records found. Up to 500 domains may be entered.

Lookup Results

SPF Record for mail.com
mail.com. 3042 IN TXT "~spf1 pr whois.mail.com include=gmail.com; include=google.com; -all"
SPF Record for linkedin.com
1084644.in-addr.arpa. 3000 IN TXT "~spf1 pr whois.linkedin.com include=gmail.com,123.com; include=google.com,123.com; -all"
SPF Record for outlook.com
2562576.in-addr.arpa. 3000 IN TXT "~spf1 pr whois.outlook.com include=gmail.com,123.com; include=google.com,123.com; -all"
SPF Record for yahoo.com
yahoo.com. 3042 IN TXT "~spf1 pr whois.mail.yahoo.com include=gmail.com; include=google.com; -all"
SPF Record for youtube.com
youtube.com. 3042 IN TXT "~spf1 pr whois.mail.youtube.com include=gmail.com; include=google.com; -all"
SPF Record for bitcoin.com
bitcoin.com. 301 IN TXT "~spf1 pr whois.mail.bitcoin.com include=gmail.com; include=google.com; -all"

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://www.google.com/transparencyreport/saferemail/
Infrastructure Security

- **Base points**
  - Server & SSL implementation

- **Bonus points**
  - *DV Certs*
  - EV SSL
  - AOSSL
  - DNSSEC

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

SSL/TLS Deployment Best Practices

**Common Issues**
- Support of TLS 2.0
- “Beast Attack”
- Mismatched certs
- Cross site scripting
- iFrames exploits
- SHA1 depreciation - weak signature, need to upgrade to SHA2
- Servers accepting RC4 cipher
- FREAK Exploits
- Lack of support of Forward Secrecy with the reference browsers

Data Sources: SSL Labs - [https://www.ssllabs.com](https://www.ssllabs.com), High-Tech Bridge [https://www.htbridge.com](https://www.htbridge.com), Distil Networks and Sitelock
Enhanced SSL Criteria

- Two new grades, A+ (100 pts) and A- (90 pts), allow for finer grading.
- Support for TLS 1.2 required for an A. If not, grade is capped at B.
- Key lengths below 2048-bit capped at B (below 1024-bit receive an F)
- MD5 certificate signatures considered insecure, receive an F
- Warnings – servers with good configuration, but one or more warnings, are reduced to an A-
  - Servers not supporting Forward Secrecy 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 receive a warning

AOSSL – 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.

- [https://otalliance.org/resources/always-ssl-aossi](https://otalliance.org/resources/always-ssl-aossi)
HTTPS By Default

FTC.gov is now HTTPS by default

By: Ashkan Soltani, Chief Technologist | Mar 6, 2015 11:00AM

In another step to enhance the FTC’s website, I’m pleased to announce that our agency has enabled encryption by default (HTTPS) for FTC.gov, our primary public domain, and home of the Tech@FTC blog. Ironically, as I was preparing this post, the entire internet has been RidICulous about another vulnerability in SSL.

While we have long provided secure transport for FTC domains that handle sensitive consumer data, such as complaint data and email subscriptions, consumers will now browse our entire site more privately, and their browsers will automatically verify the identity of the website to which they’re connecting – an important step to mitigate attempts to impersonate the FTC.

Privacy

- **Base points**
  - Privacy policy
  - Third-party trackers on site
- **Bonus points**
  - Layered privacy policies
  - Bilingual policies
  - Use of Icons
  - Do Not Track status, policy
  - Tag mgmt or privacy solution
- **Penalty points**
  - WHOIS (if Private vs Public)
  - Data Breach Incidents
  - FTC / State Settlements

*italics = new in 2015*
Do Not Track – DNT

- Required disclosure in California as of 1/1/14
- Recognize the standard is evolving
- Bonus if the disclosure is visible on the Privacy Page
- Added points if they state they will Honor the setting and 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

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
Timing

• Next 30 days
  ▫ Review methodology
  ▫ Engage your teams and optimize your brand, domain and site.
• April 20 – Begin testing
• May 1 – All data due to OTA
• May 4 – Start data analysis & cross tabbing
• June 15 – Release report

Tools & Resources

• Online Trust Honor Roll https://otalliance.org/HonorRoll
  ▫ Methodology, past reports and related resources
• Email Security https://otalliance.org/eauth
• Always On SSL SSL Best Practices https://otalliance.org/aossi

OTA +1 425-455-7400