Online Trust Alliance

OTA 2013 Online Trust Audit Highlights

https://otalliance.org/2013HonorRoll.html

Background

- Goal – Highlight best practices in sites security, brand protection and privacy
- Audit covered 750 web sites, including over 10,000 web pages and 500 million emails.
- To qualify for the OTA Honor Roll, companies had to achieve 80% of the total available points across three major categories, and score at least 55% in each category;
  - Domain, Brand & Consumer Protection
  - Site, Server & Infrastructure Security
  - Data Protection, Privacy & Transparency

Honor Roll

- 32% of companies analyzed made the 2013 Honor Roll, up from 30% last year.
- Nearly half of the companies that made the Honor Roll are two-year consecutive recipients.
- More than 20% of companies who made the Honor Roll last year did make the list this year; indicating the importance of continually monitoring and maintaining site security and privacy.
- 83% of OTA member made the Honor Roll; the Social 50 had second highest recipients (52%).
- 71% of FDIC banks had failing scores in one or more categories; followed by the IR 500 (53%) failing in one or more categories.

Specific Areas

- Adoption of email authentication continues to rise across all sectors
  - Significant jump in adoption of both SPF and DKIM – 56% to 76% for IR 100, 34% to 49% for FDIC 100, Federal 50 doubled from 10% to 20%.
  - DMARC is gaining steam with 10% adoption overall (ranges from 3% to 44%) and organizations in all sectors asserting a “reject” or “quarantine” policy for email that fails authentication.
  - While adoption rose, average scores for email authentication were still low (65.2) due to heavier weighting on adoption at the top-level domain and use of DMARC.
- Average SSL scores improved nearly 10% in all sectors, despite tightened criteria that capped scores based on vulnerability to common attacks.
- FDIC 100 leads all sectors in adoption of EV SSL (60%) and AOSSL (61%) – next closest adopters are 35% and 10% respectively.
- Privacy scores negatively impacted all of many sectors, with 33.7% receiving failing scores. The FDIC 100 had the highest failure rate (55%), followed by the IR 500 (35%).
- Do Not Track (DNT) adoption is nearly zero, only one company to-date (Twitter) has made a public commitment to honor it.
- 88% of the Federal 50 adopted DNSSEC; the next closest sector had an adoption rate of only 8%.
- Federal 50 significantly lags behind all sectors in adopting best practices to help protect consumers from forged and deceptive email and securing their sites from known vulnerabilities.

