2018 Online Trust Audit & Honor Roll

Recognizing excellence in security, consumer protection, and responsible privacy practices

OTA
Online Trust Alliance
an **Internet Society** initiative

TABLE OF CONTENTS

Overview & Background

This 2018 Online Trust Audit and Honor Roll, which takes a snapshot of best practice adoption as of the end of 2018, represents the 10th year the Online Trust Alliance (OTA) has conducted benchmark research to promote security best practices, data stewardship and responsible privacy practices. The primary goals of this work include raising the level of data security and privacy, and recognizing organizations that have demonstrated security and privacy excellence. In addition to the Honor Roll status (Appendix D), this Audit includes a "Top of Class" list representing the top 50 organizations based on their total score (Appendix C).

Recent headline news regarding business email compromise ($123M extracted from Facebook and Google), large breaches (383 million records from Marriott) and questionable handling of users' data (series of revelations regarding Facebook), as well as the commencement of the EU's General Data Protection Regulation (GDPR), reinforce the need for organizations to embrace best practices in all areas – email security, site security and privacy practices. The 2018 CIGI-Ipsos Global Survey on Internet Security and Trust continues to paint a bleak picture of the state of online trust. More than half of those surveyed are more concerned about privacy than the year before, and the majority have a high level of distrust of social media platforms, search engines and Internet technology companies.[1] [2] [3] [4] [5]

In many areas, business practices are moving out of alignment with consumer expectations. Left unchecked, mistrust in the privacy and security offered by organizations may have chilling effects. For the Internet economy to prosper, users need to be able to trust that their personal information will be secure, their preferences respected and their privacy protected.

The OTA recommendations and best practices evaluated in this Audit apply not only to email, websites and mobile applications, but increasingly to the expanded universe of Internet of Things (IoT) offerings. In addition to this Audit, IoT manufacturers should review OTA's IoT Trust Framework for recommendations specific to IoT offerings.[6] The 2018 Audit has been enhanced in several areas – additional subsectors, one major new sector (healthcare), and expanded criteria in each major category, which now totals more than 100 data attributes (Appendix B) – thus providing a more comprehensive view of online trust across a wider range of relevant organizations. New criteria have been added and weighting has been updated to reflect the evolving threat landscape, regulatory environment and globally accepted practices. In addition, high-level GDPR-related principles were captured to create a baseline for future Audits. To assist organizations, this report includes a Best Practices Checklist (Appendix E) and Implementation Resources (Appendix F).

It is important to note that the Audit is limited to a slice of time. Based on the dynamic nature of website and application configurations, organizations' scores may have changed since the Audit was completed. All analysis was done without the active participation of the sites being analyzed. Sites were selected based on their ranking within their individual sectors or public lists (or organizational membership in the Internet Society). In instances where a significant vulnerability was identified, OTA abided by coordinated disclosure practices and attempted to contact the "at-risk" entity providing them a chance to remedy the observed issue and be rescored before publication of this report.

Executive Summary & Highlights

The 2018 Online Trust Audit & Honor Roll assesses nearly 1,200 organizations, examining consumer protection, security and privacy protection practices.[7] Enhancements to the Audit include additions of new subsectors in the News/Media and Consumer sectors (sports news, video streaming and payment services) as well as a new sector – Healthcare. This sector includes top medical insurance companies, pharmacies, medical testing labs and hospital chains. The sectors examined and the associated top-ranked organizations include:

- 2018 Internet Retailer Top 500 (IR 100 & IR 500) [8]
- Top 100 Federal Reserve Banks (Bank 100) [9]
- Top 100 U.S. Federal government organizations (Federal 100)
- Top 100 Consumer Services companies (Consumer 100) [10]
- Top 100 News and Media organizations (News 100)
- Top 100 ISPs, Carriers & Hosters (ISP/Hosts 100)
- Top 100 Healthcare organizations (Health 100)
- OTA (Internet Society) Member organizations (OTA) [11]

> *"We are pleased to see more and more organizations satisfy the criteria for the Online Trust Alliance Honor Roll over time as they rise to meet society's growing demand for a safer Internet." – Neil Daswani, Senior Vice President, Consumer Chief Information Security Officer, Norton LifeLock*

While the majority of segments remain the same, the actual list of organizations audited each year changes based on revenue/traffic ranking and market consolidation. This year, with the addition of the Healthcare sector and additions or shifts in organizations on the ranked lists, approximately 30% of organizations are new to the Audit.

As in previous years, 100 baseline points can be earned in each of the three major assessment categories (consumer protection, site security and privacy). Bonus points are applied for emerging best practices and penalty points are applied for breaches, legal settlements and observed vulnerabilities. A minimum score of 60 is required in each of the three categories. Bonus points are limited to a maximum of 20% of the baseline score. Sites qualify for the Honor Roll by achieving a score of 80% or higher overall with no failures in any one of the three core categories.

2018 has seen record achievement, with 70% of organizations earning Honor Roll status (the previous high was 52% in the 2017 Audit). Given that the methodology was updated to "raise the bar" in all three scoring categories, this is impressive. Scores of former OTA members are not incorporated in the results (except the overall top scores) since they would skew the results (98% achieved Honor Roll status).

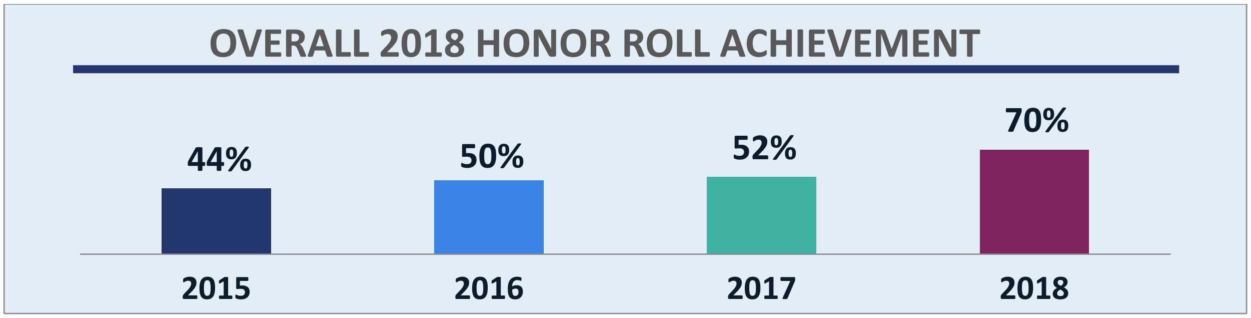


Figure 1 – Overall Honor Roll Achievement by Year, 2015-2018

As illustrated in Figure 2, Honor Roll achievement grew in all sectors despite more stringent criteria in this year's Audit.[12] The Federal 100 outscored all sectors with 91% achievement, overtaking the Consumer 100, which has been the top sector for six consecutive years. U.S. federal government entities were also most improved, followed closely by the Bank 100 and News 100. The newly added Healthcare sector had 57% Honor Roll achievement, lagging all other sectors.

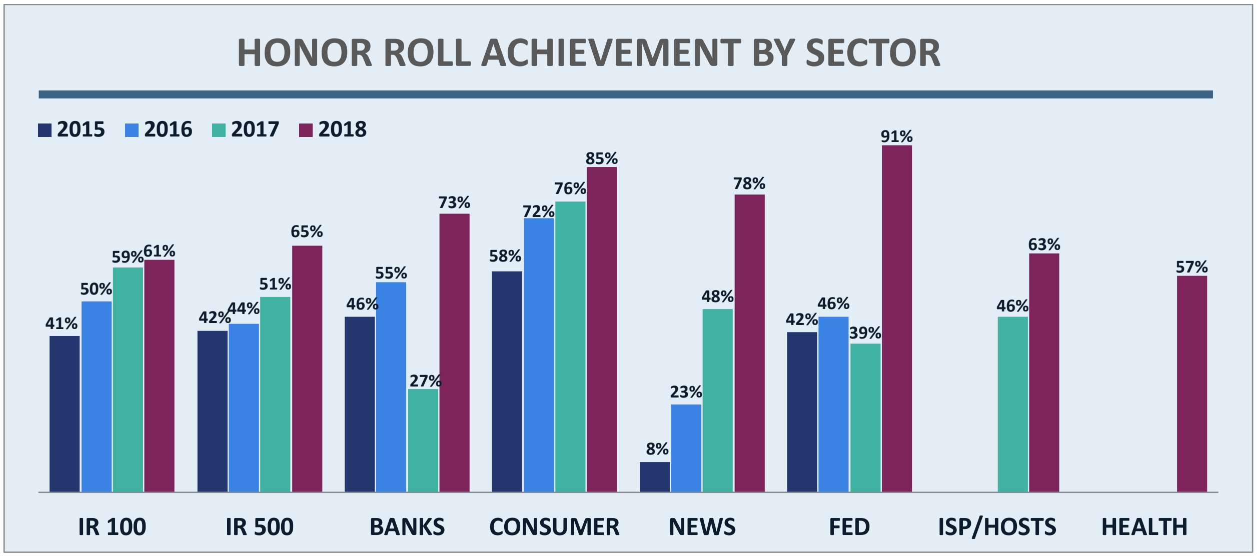


Figure 2 – Percent Achieving Honor Roll Status by Sector, 2015-2018

As in previous years, results were nearly bi-modal, with a majority of sites either qualifying for the Honor Roll or failing in one or more areas. As illustrated in Figure 3, only 3% overall neither failed nor qualified for the Honor Roll, ranging from 0% to 7% for individual sectors.

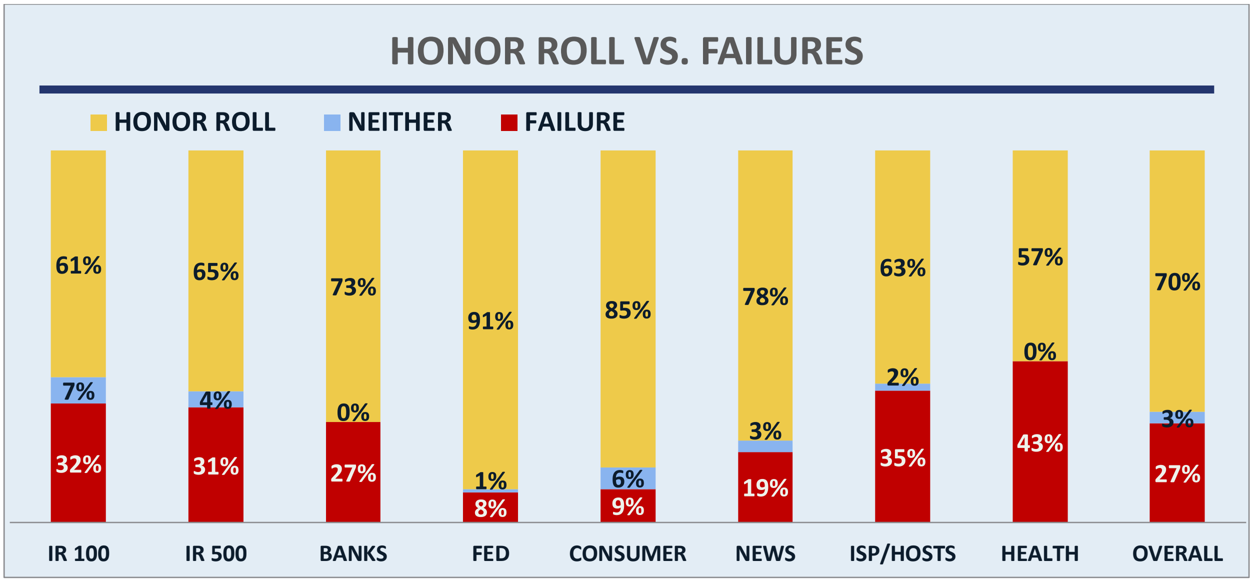


Figure 3 – Distribution of Honor Roll vs. Failures by Sector

In the 2017 Audit a "Top of Class" category was created, representing the top 50 (Top 50) overall scores. This year all sectors are represented in the Top 50, as shown in the table below (note that because several organizations are in multiple sectors, the total exceeds 100%). The biggest shift in the Top 50 was the Federal sector, which doubled from 12% in 2017 to 26% this year. The Bank sector, which had no presence in 2017, had three organizations in the Top 50 this year. A full listing of the Top 50 scoring organizations can be found in Appendix C.

TOP 50 SECTOR PERFORMANCE

Code	Sector	% of Top 50
C	Consumer Services	40%
F	US Federal Government	26%
R	Internet Retailers	14%
O	OTA (Internet Society) Members	12%
B	Banks	6%
H	Healthcare	4%
I	ISPs, Carriers & Hosters	4%
N	News/Media	4%

Figure 4 – Top 50 Performance by Sector

The top overall score in the Audit was earned by Google News, which was also the top score in the News/Media sector. Other sector winners were 23andMe (Healthcare), Federal Emergency Management Agency – FEMA (US Federal Government), First National Bank of Omaha (Banks), Google Cloud (ISP/Hosts), Google Play (Internet Retailers), Online Trust Alliance (OTA Internet Society members), and PayPal (Consumer).

Overall failure results, as shown in Figure 5, show that privacy was the most prevalent cause of failure for all sectors at 15%, followed by consumer protection at 13% and site security at only 3%. Failures in the consumer protection category improved dramatically from 33% in 2017, primarily due to significantly higher adoption of DomainKeys Identified Mail (DKIM). Failures varied widely by sector (Figure 6). Overall, 27% of sites failed in one or more areas (down from 47% in 2017). The highest causes of failures were lack of email authentication in the Healthcare and ISP/Hosts sectors followed by inadequate privacy statements for the Internet Retailer and ISP/Hosts sectors. Conversely, the Federal and News sectors each had no failures in Site Security and the Federal and Consumer sectors led the way in privacy, with failures of only 2%.

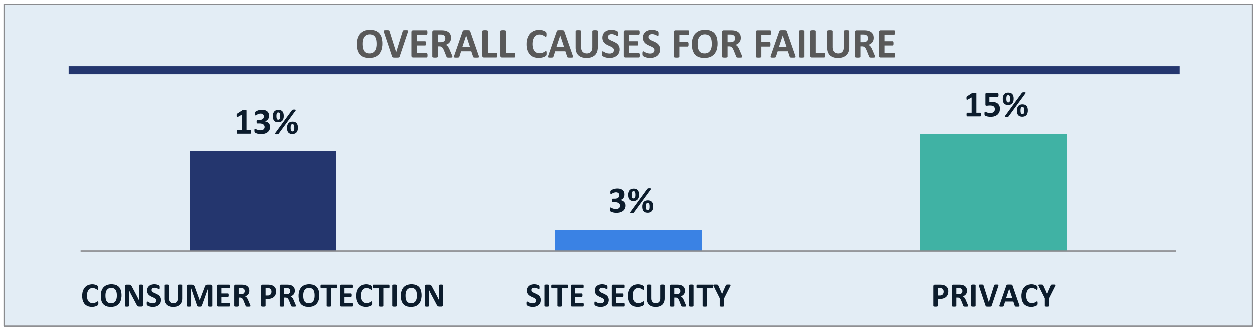


Figure 5 – Failures Causes by Audit Category

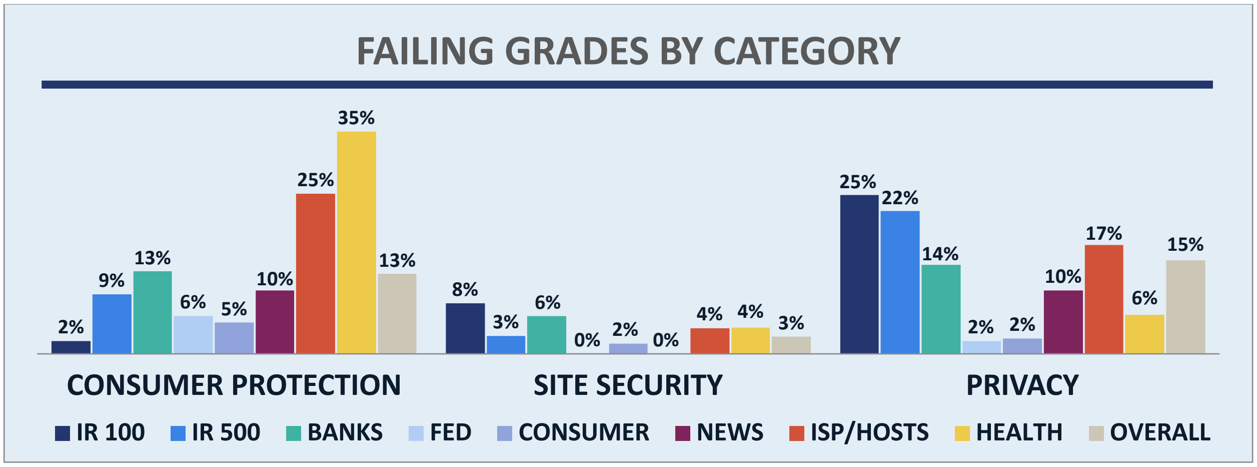


Figure 6 – Percent of Companies with Failing Grade by Sector and Category

Additional insight can be gained by normalizing the 300 baseline points to a 100-point scale (called the "Online Trust Index") and comparing the high, low and median index across sectors. For several years the median in most sectors hovered around the 80% Honor Roll threshold, meaning that many organizations were "on the bubble" of Honor Roll achievement. Figure 7 shows that the median for all sectors this year is above the 80% threshold, and the median for many exceeds 90%.

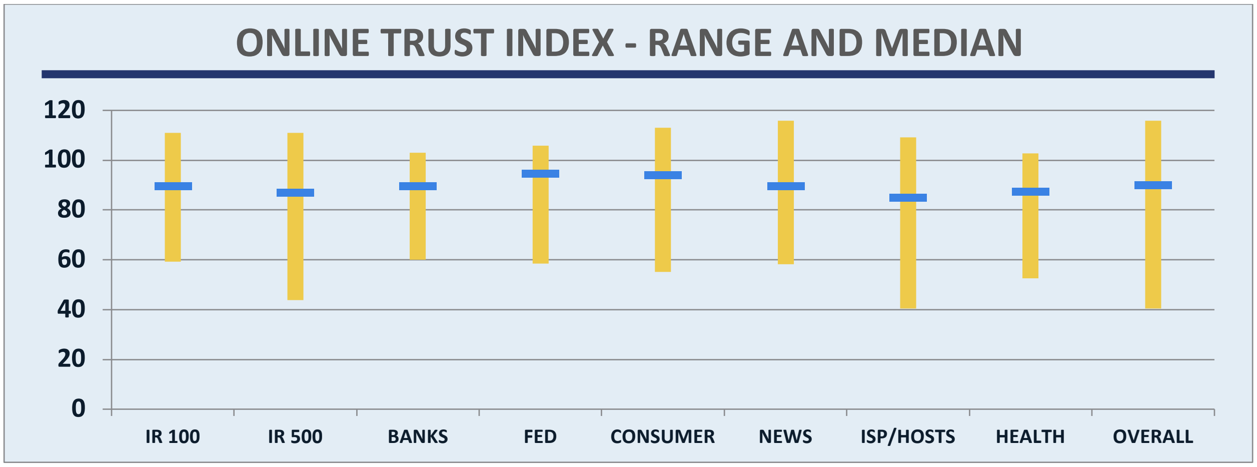


Figure 7 – Range and Median Online Trust Index Scores by Sector

Best Practices Highlights

The following is a summary of audited best practices advocated by OTA. Additional details are provided in the respective sections: 1) Domain, Brand & Consumer Protection, 2) Site, Server & Infrastructure Security, and 3) Privacy, Transparency & Disclosures.

Consumer Protection

Email Authentication –The methodology was updated in 2017 to ensure that Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting & Conformance (DMARC) records were in compliance with published specifications. Non-conformant records were either given partial credit or disqualified altogether. Across all organizations, 3% had an invalid SPF record and 13% had errors causing them to receive only partial credit. Likewise, 2% of DMARC records were deemed invalid. This underscores the need for sites to continually monitor their records to maximize brand and consumer protection. If left unmonitored, brands may have a false sense of security because some receiving networks and ISPs may disregard such "invalid" records.

- Overall, use of email authentication has reached record levels. SPF adoption at the top-level domain jumped from 77% to 89%, while adoption of DKIM at the top-level domain grew even more dramatically, from 56% to 83%.
- Use of DMARC records grew from 34% to 50%. DMARC is used in conjunction with SPF and DKIM to defend against spoofed and forged email used in spearphishing and business email compromise attacks.
- Adoption of DMARC reject or quarantine records at the top-level domain grew from 15% to 24% overall. This "enforcement" policy tells email receivers to quarantine or block messages that fail authentication, protecting consumers from fraudulent email.

Opportunistic TLS – This encrypts messages between mail servers, and adoption continued to grow, from 65% to 73%. (Bonus Points)

Domain Name System Security Extensions (DNSSEC) – Adoption dropped slightly, from 12% to 10%, which can be entirely attributed to changes in the sector lists. (Bonus Points)

IPv6 – Adoption dropped slightly, from 14% to 12%, mainly due to more stringent criteria (websites had to be reachable via IPv6 – in prior years only the name service had to be IPv6 compliant). Even with this higher bar, some sectors grew in adoption (Banks from 0% to 6%, Consumer from 12% to 15% and Internet Retailers from 5% to 7%). (Bonus Points)

Site Security

HTTP Strict Transport Security (HSTS), Always on SSL, or HTTPS Everywhere – This element became part of baseline scoring this year (it previously earned bonus points). Adoption took another large jump, growing to 93% (from 30% in 2016 and 52% in 2017). Growth is attributed to increased attention on online encryption as the "norm" for Internet communication based on concerns of third-party and government monitoring of web activities. In prior Audits, 99% of sites supported encryption but it often applied only to login or financial transaction pages instead of the entire web session.

Overall Site Security Scores – Overall scores dropped slightly from 91 to 89 (out of 100), entirely due to increased weighting on IP reputation, software patching and website header security scores. Many sites are still not setting a content security policy and limiting exposure to vulnerabilities introduced by cookies and other third-party content by configuring web security headers. The bulk of the Site Security score is still tied to SSL/TLS configuration, and scores actually improved 2% in this aspect, since more sites are using proper configurations of protocols and cipher suites. Sites with failing scores had the same issues observed in prior years: weak or insecure cipher suites, use of insecure protocols and incomplete certificate chains leading to vulnerabilities to threats such as the ROBOT attack. Banks had the highest failure rate (6%). Use of newer TLS protocols continued to evolve – 29% of sites do not support protocols older than TLS1.2 and 7% of sites are already supporting TLS1.3, which was officially published by the Internet Engineering Task Force (IETF) in August 2018.[13]

Certificate Authority Authorization (CAA) – This allows sites to publish a list of certificate authorities allowed to issue certificates for their domain, thereby limiting abuse. This item was added to the 2018 Audit because the Certificate Authority/Browser (CA/B) Forum mandated that certificate authorities must check for CAA before issuing or renewing certificates starting in September 2017. Unfortunately, only 6% of sites overall are taking advantage of this capability, led by the Consumer and ISP/Hosts sectors at 20% and 13%, respectively. Adoption in all other sectors is less than 6%. (Bonus Points)

Vulnerability Disclosure Mechanisms / Programs – This was added in 2017 and is recognized as a best practice by the National Telecommunications and Information Administration (NTIA), National Institute of Standards and Technology (NIST), the Federal Trade Commission (FTC) and OTA. Adoption grew from 6% to 11% overall for sites that had a reporting mechanism visible on their site or listed with third-party "bug bounty" service providers. The Consumer sector outpaced all others with 43% adoption, followed by ISP/Hosts at 25%, News/Media at 9% and Banks at 6%. Having such mechanisms is critical to effectively respond to reports from third-party researchers and users and is relatively simple to implement. (Bonus Points)

> *"This is the most expansive OTA Audit to date and we have seen record jumps in adoption of key practices such as email authentication and end-to-end encryption," said Olaf Kolkman, Chief Internet Technology Officer, Internet Society. "This is encouraging and we hope this motivates all organizations to follow suit. The practices we audit enable consumer trust and increase confidence, not only in the individual organization, but also in the Internet as a whole."*

Cross Site Scripting (XSS) Vulnerabilities – After growing from 27% in 2016 to 50% in 2017, presence of XSS vulnerabilities dropped significantly to 21% in this Audit. News sites had the highest rate (43%) while Banks had the lowest (5%). Several sectors were near the overall average in the 21%-23% range.

Privacy Trends

Combined scores (privacy statement and use of third-party trackers) dropped this year, from 73 to 70, mainly due to more stringent scoring of some of the key privacy statement criteria.

Privacy Statement – Overall privacy statement scores dropped from 31 in 2017 to 27 in 2018. Significant shifts were observed in data retention language (dropped from 49% to 2% since it now requires a specific retention timeframe as in GDPR), layered statements (grew from 29% to 47%) and holding third-party vendors to the same privacy practices as the organization (grew from 48% to 57%). In addition, the data sharing criterium was broken into two pieces – basic sharing language (e.g., "we do not share data except with third parties who deliver the service" – 67% have such a statement, a modest increase from

63% in 2017) and "affiliate" language (e.g., "we do not share with affiliates or other third parties" – only 20% have such a restriction). This means that 80% are, or could be, sharing data with third parties. The concern with the affiliate sharing exception is that it often enables targeted marketing and other activity that may not be expected by the user.

For the first time, the display of privacy statement date stamps was captured in this year's Audit since they were deemed to be of interest in light of GDPR going into effect in May 2018. Overall, 31% of sites had no date stamp, 11% had a date prior to 2017, 11% had a date in 2017, and 47% had a date newer than January 1, 2018. The Consumer sector had the most "current" privacy statements (71% newer than January 1, 2018) while the Healthcare sector had the least current statements (only 19% newer than January 1, 2018).

GDPR Alignment – Because GDPR went into effect in mid-2018, various GDPR-related data was captured to create a baseline, and bonus points were awarded for organizations that included key GDPR-related principles in their privacy statement. Bonus (vs baseline) points were awarded since most of the audited organizations (and related sites) assessed are US-based, so GDPR does not necessarily apply. Analysis showed that:

- 32% of privacy statements were deemed easy to read (leaving nearly 70% with a clear need to improve),
- 95% of statements sufficiently articulated what data is being collected and for what reason,
- Less than 1% named the categories of third parties with whom that data is shared,
- 70% identified a means to contact the Data Protection Officer,
- Only 1% address how sensitive personal information (e.g., biometric data, racial or ethnic origin, political opinions, religious or philosophical beliefs, etc.) gathered from third parties is handled (this disclosure is only required if such data is handled), and
- 50% outline the process for users to request data the organization has collected about them.

Third Party Trackers – Overall, the scores related to problematic trackers remained flat, increasing slightly from 42.0 in 2017 to 42.4 in 2018. These are trackers known to share data with third parties (not including data captured for anonymous or pseudonymous site metrics). The number of unique trackers observed on all sites ranged from 0 to 40. The News/Media sector had more than double the overall sector average, reflecting their dependence on advertising and re-targeting of site users.

Data Loss Incidents & Breaches – Measured from June 2017 through December 2018, 15% of sites had one or more incidents (up from 12% in 2017). The Consumer sector had the highest rate (34%) followed by the Healthcare sector (30%). Banks, which had the highest rate in the 2017 Audit, were next at 20%. Organizations with breaches of more than 1000 records received a penalty, and this year the penalty was scaled in proportion to the size of the breach.[14]

Regulatory Fines & Settlements – Eighteen organizations received a penalty for suits or settlements this year (down from 21 in 2017), with the Consumer sector having the most (14). Data includes actions from the Consumer Financial Protection Bureau (CFPB), individual state Attorney General offices, class action suits and international agencies as well as the Federal Trade Commission (FTC). For purposes of Audit assessment, the focus is on consumer protection actions related to security and privacy and does not include settlements pertaining to mergers and acquisitions or labor issues.

Domain, Brand & Consumer Protection

By utilizing email authentication (SPF and DKIM), organizations can help protect their brands and prevent consumers from receiving spoofed and forged email. Email authentication allows senders to specify who is authorized to send email on their behalf. Building on email authentication protocols, DMARC adds a policy assertion providing receivers direction on how to handle messages that fail authentication.

Opportunistic TLS provides a means to encrypt messages between mail servers, protecting both the brand and consumer. Domain locking ensures that domain ownership cannot be transferred without the owner's permission. Domain Name System Security Extensions (DNSSEC) adds security and integrity to the DNS, helping to prevent "Man-in-the-Middle" (MitM) attacks, cache poisoning and related DNS attacks. IPv6 expands the number of unique IP addresses, thereby supporting the growth of the Internet, including demand for new IP addresses driven by IoT.[15] [16]

Best practices include:

- Implement both SPF and DKIM for top-level domains, "parked" domains (not used for email) and any major subdomains seen on websites or used for email.
- Optimize SPF records with no more than 10 DNS lookups.
- Implement DMARC, initially in "monitor" mode to get receiver feedback and verify accuracy of email authentication, and eventually move to "enforcement" (signal a "reject" or "quarantine" policy to receivers).
- Mandate the use of DMARC reporting capabilities with RUA (aggregate) and RUF (message-specific forensic) reports.
- Implement inbound email authentication checks and DMARC on all networks to help protect against malicious email and spear phishing purporting to come from legitimate senders.
- Implement opportunistic TLS to protect email in transit between mail servers.
- Ensure that domains are locked to prevent domain takeovers.
- Implement DNSSEC to help protect a site's DNS infrastructure.
- Deploy IPv6.
- Implement Distributed Denial of Service (DDoS) mitigation technologies and processes.
- Implement multi-factor authentication.

Email Authentication

Authentication technologies, namely SPF and DKIM, help prevent phishing and spam. OTA recommends the use of email authentication at the top-level (or "corporate") domain (TLD) as well as any other domains used for sending email or that might be used to fool consumers. Additional telemetry was added in the 2017 Audit to assess the validity of SPF and DMARC records. Authentication at the TLD received increased weighting for the third year in a row.

Figure 8 shows adoption of SPF and DKIM at the corporate top-level domain (TLD) and combined use of SPF and DKIM at any level including subdomains. In general, SPF adoption is higher than DKIM which we conclude is primarily due to its ease of implementation, though the gap continues to narrow. Using both SPF and DKIM best enables receivers to detect and block malicious email, while reducing the risk of false positives.

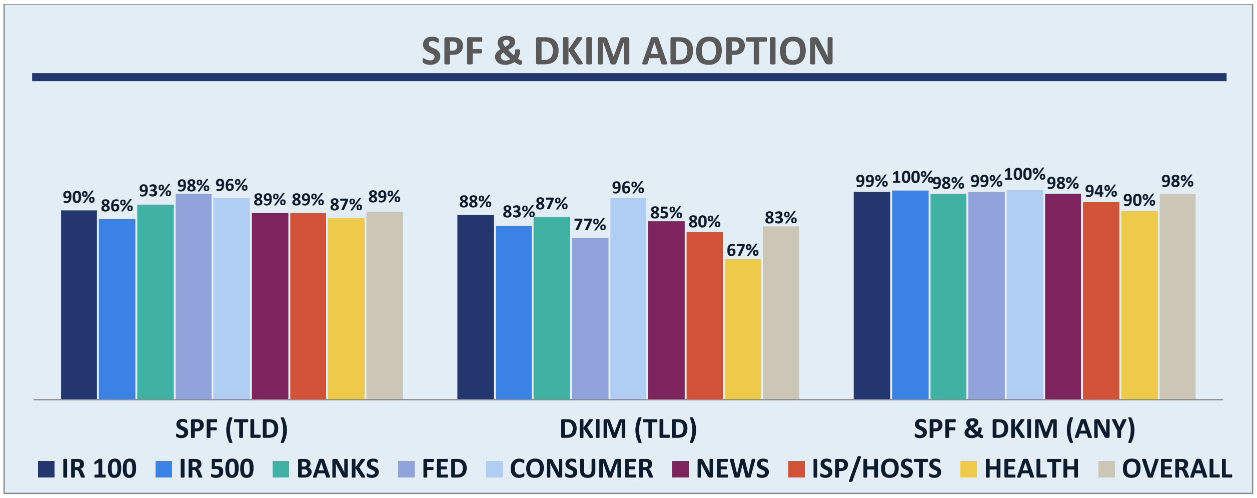


Figure 8 – Email Authentication & DMARC Adoption by Sector

As seen in Figure 9, growth was seen in all sectors, and many are approaching 100% adoption. Significant jumps were seen in the Federal sector (from 46% to 94%, attributed largely to DHS Directive 18-01) and the Bank sector (60% to 87%).[17] The Healthcare and ISP/Hosts sectors lag at 65% and 75% respectively. Though the gaps are closing, in some sectors there is still a significant lack of email authentication support at the top-level domains (note the gap between "DKIM TLD" and "SPF and DKIM" in Figure 8 above). This underscores that additional efforts are needed to drive DKIM implementation to protect top-level and corporate top-level domains from abuse.

BOTH SPF & DKIM

	2015	2016	2017	2018
Internet Retailer Top 100	90%	92%	92%	98%
Internet Retailer Top 500	78%	85%	83%	95%
Bank 100	63%	69%	60%	87%
Federal 100	48%	58%	46%	94%
Consumer 100	76%	86%	88%	95%
News 100	56%	75%	77%	94%
ISP/Hosts 100	-	-	55%	75%
Health 100	-	-	-	65%

Figure 9 – Adoption of Both SPF and DKIM by Sector

Starting in 2017, SPF records were analyzed more closely and received only partial credit or were considered invalid if they contained errors that would cause them to be unusable or ineffective. This impacted 16% of organizations overall and was most prevalent for retailers (20%). The Federal sector has the lowest error rate (4%). The top reasons for receiving only partial credit were excessive lookups and "include" references to non-existent or invalid SPF records of other domains.[18] Top reasons for deeming records invalid were use of multiple SPF records and syntax errors rendering the record useless. In addition, the use of a "+all" or "?all" directive was observed, which effectively instructs receivers (at ISPs and corporate networks) to allow any IP address to send mail or to ignore the record. These records were also deemed invalid. Many of these organizations may have a false sense of security, not knowing that their SPF records are ineffective in protecting their domain.

While outside the scope or capability of this Audit, all organizations should deploy inbound authentication checks and enforce DMARC policies. As a recommended risk mitigation practice, key vendors, business partners and service providers should be required to deploy end-to-end authentication including SPF, DKIM and DMARC.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

DMARC builds on SPF and DKIM results, provides a means for feedback reports and adds visibility for receivers on how to process messages that fail authentication. Added to baseline scoring in 2013, additional weight was given for use of DMARC reject and quarantine policies in 2016, with maximum points awarded to reject policies. Weighting was increased for use of the reject policy this year.

As illustrated in Figures 10 and 11, adoption of DMARC grew in most sectors, most notably in the Federal sector (20% to 93%, again directly due to Directive 18-01), Banks (39% to 70%) and News (29% to 50%). Invalid DMARC records were seen in nearly 2% of organizations overall, but most prominently in the ISP/Hosts sector (5%). The top reasons to invalidate a record were a "naked" record (p=none and no RUA or RUF reports) and pointing reports to domains unable to accept them.

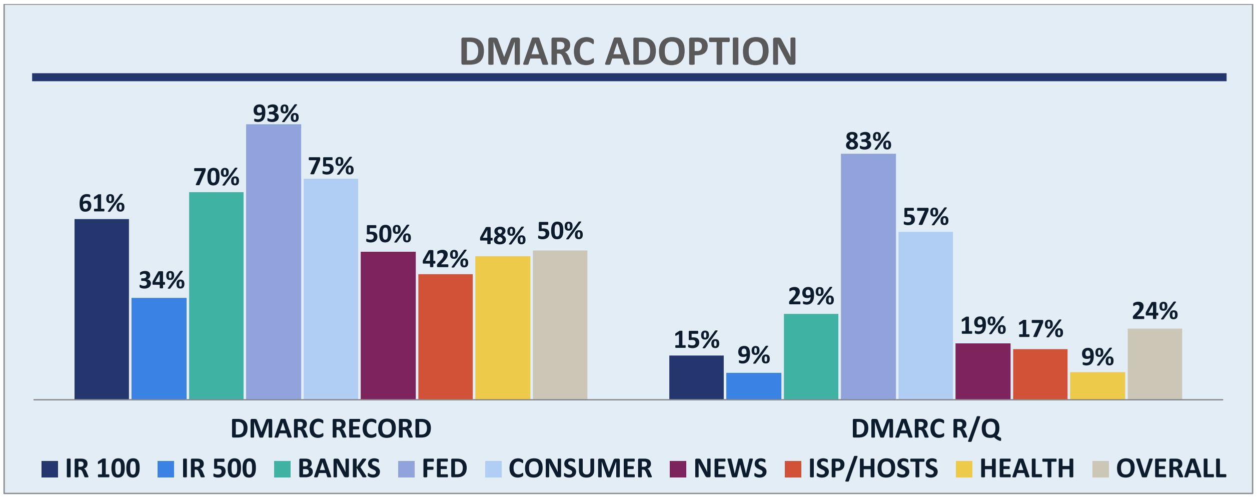


Figure 10 – DMARC Adoption & Policies

DMARC ADOPTION

	2015	2016	2017	2018		
	Record	Record	Record	Any Record	Valid Record	R or Q*
Internet Retailer Top 100	20%	30%	50%	61%	61%	15%
Internet Retailer Top 500	8%	21%	33%	34%	33%	9%
Bank 100	24%	33%	39%	70%	70%	29%
Federal 100	14%	20%	20%	93%	93%	83%
Consumer 100	48%	64%	62%	75%	74%	57%
News 100	10%	21%	29%	50%	48%	19%
ISP/Hosts 100	-	-	25%	42%	37%	17%
Health 100	-	-	-	48%	47%	9%

Figure 11 – DMARC Adoption by Sector. *R or Q = Reject policy or Quarantine policy

Opportunistic Transport Layer Security (TLS) for Email

Tracking of Opportunistic TLS for email was added in the 2015 Audit to help address mounting confidentiality concerns regarding monitoring of email in transit. TLS encrypts messages in transit from one server to another, seamlessly decrypting the messages before they are delivered to the user. TLS adoption is on a steady growth path, increasing from 65% in 2017 to 73% this year. The Federal sector continues to lag at 51%, while the Consumer and News sectors lead with 83% adoption. Growth is attributed to an overall call for encryption by dozens of organizations including the Internet Society, as well as Google and Twitter who provide data regarding use of Opportunistic TLS. Since early 2016, Gmail has also highlighted messages without TLS with an unlocked red padlock.[19]

Domain Locking

Domain locking became a scoring element in 2013 due to its importance in prevention of domain takeovers (a penalty is assigned if the domain is not locked). More than 95% of organizations across all sectors lock their domains. The Federal sector leads with 100% adoption followed closely by Consumer (98%) and Healthcare (97%). Retailers, Banks, News and ISP/Hosts sectors are all in the 93%-94% range.

Domain Name System Security Extensions (DNSSEC)

DNSSEC adds security to the DNS lookup. It is designed to help combat "Man-in-the-Middle" (MitM) attacks and cache poisoning by authenticating the origin of DNS data and verifying its integrity while moving through the Internet. DNSSEC is now deployed in the .com, .gov, .org, .net and over 135 other TLDs, potentially supporting more than 90 million domain name registrations worldwide in the .com domain alone.[20] DNSSEC adoption dropped from 12% in 2017 to 10% this year due to changes in the list of audited organizations. The Federal sector leads adoption (87%) largely due to a mandate in 2008, followed by Banks (10%) and ISP/Hosts (8%).[21] Broader implementation of DNSSEC continues to be hampered by legacy systems and lack of ecosystem infrastructure.

Internet Protocol Version 6 (IPv6)

IPv6 is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers across the Internet, and significantly expands the number of available addresses. OTA supports broader deployment, awarding bonus points for adoption. Adoption worldwide is growing with the Alexa Top 1000 websites currently reachable over IPv6 at over 26%, a 2% increase from 2017.[22] Overall adoption in the OTA Audit dropped from 14% in 2017 to 12% this year due to more stringent requirements – websites had to be reachable via IPv6, while in prior years only the name service had to be IPv6 compliant. The Federal sector leads with 46% adoption, followed by ISP/Hosts at 20% and Consumer organizations at 15%.

Multi-Factor Authentication (MFA)

Adding another layer of authentication on top of simple username and password is an effective step to help counter unauthorized account access, account takeover and password resets. Multi-factor authentication (MFA) requires additional credentials beyond username and password to gain access to an application, site, or data. In typical two-factor authentication, a one-time password or code is generated by a software or hardware token (something the user possesses) to verify account access authorization. Especially in light of the wave of credential stuffing attacks in 2018 and the massive database of breached username/password pairs, use of multi-factor authentication is a strongly recommended best practice.[23] [24] Multi-factor authentication data was collected in the 2017 Audit, but covered less than one-fourth of audited organizations. Due to incomplete data, MFA was not assessed in this Audit, though the intent is to make it part of the Audit methodology when sufficient data becomes available.

Site, Server & Infrastructure Security

A site's trustworthiness is largely defined by the security of the infrastructure as well as its associated privacy practices. Users need assurance that the site and its data are secure. Proper implementation of best practices in this category also protects the site itself from attack. The 2018 Audit has been expanded with deeper evaluation of DNS health, IP reputation, application security and patching cadence. In addition, the bar was raised this year in server security scoring by combining results from High-Tech Bridge (now ImmuniWeb), Qualys SSL Labs, Mozilla's Observatory and Sucuri's SiteCheck. Best practices include:

- Optimize SSL/TLS implementation using information gleaned from public tools, focusing on vulnerabilities that earn a letter grade of "F" or that have failure (60 points or less) in a major subcomponent of the scoring (which normally leads to an overall grade of "C"). [25] [26] This includes eliminating use of insecure ciphers and older, insecure protocols as well as vulnerabilities to the POODLE and ROBOT exploits.[27]
- Implement content security policy and associated headers for third-party content used on the site. This can prevent vulnerabilities introduced by outside content.[28] [29] [30]
- Review capabilities of certificate authorities to ensure that they meet your support requirements. Use EV SSL certificates for classes of sites that are frequently spoofed and where users need to be assured they are visiting and browsing a legitimate site.
- Implement Certification Authority Authorization (CAA) to prevent issuance of unauthorized certificates.[31]
- Implement HTTP Strict Transport Security (HSTS), also referred to as Always on SSL (AOSSL) or HTTPS everywhere, on all pages to maximize data security and online privacy. HSTS helps ensure that all data exchanged between the site and device is encrypted.
- Implement a Web Application Firewall to monitor HTTP conversations and block common attacks such as cross-site scripting (XSS) and SQL injections.
- Proactively scan sites for malicious links, iFrame exploits, malware and malvertising.[32]
- Implement bot detection and mitigation to help prevent brute force attacks, web scraping, account hijacking, unauthorized vulnerability scans, spam and man-in-the-middle attacks.
- Provide a discoverable and accessible vulnerability reporting mechanism for site visitors and third parties to report vulnerabilities.

> *"Consumers deserve to know what practices companies have in place to keep their data private and secure. The Online Trust Audit provides this transparency each year with its annual audit. This independent audit helps companies of all sizes understand which privacy and security best practices to apply to protect their customers and their businesses." – Ashutosh Agrawal, Sr. Manager, Security & Privacy Compliance, 23andMe*

As illustrated in Figure 12, summary security scores are in a relatively narrow range, while the adoption rate of key enhancements varies widely:

- Site security scores, which represent the bulk of the baseline score in this category, are tightly concentrated around the overall average of 89 (down from 92 in 2017), with the Federal sector leading at 94, followed by the Consumer and News sectors at 91. The drop in scores is entirely due to the increased weight put on other site security components – third-party content and security header implementation, patching cadence and IP reputation.
- Overall adoption of "Always On SSL" (now part of the baseline score) jumped significantly, to 93% (from 30% in 2016 and 52% in 2017), and the adoption gap across sectors has narrowed – ranging from 82% for the Healthcare sector to 100% in the Federal sector (vs a range of 26% to 91% in 2017). News sites showed the biggest growth, increasing from 26% to 93%.
- EV SSL adoption averages 25% but varies significantly across sectors – it is highest for Banks (71%, which outpaces all other sectors more than 2:1) and lowest for the News and Federal sectors (8%), followed closely by the Healthcare sector (9%).
- The newly added tracking of CAA showed that only 6% of sites overall have taken advantage of this capability, which allows domain owners to publicize the list of certificate authorities allowed to issue certificates on their behalf, thereby limiting abuse. Adoption was highest in the Consumer (20%) and News (13%) sectors, and lowest for online retailers (2%).

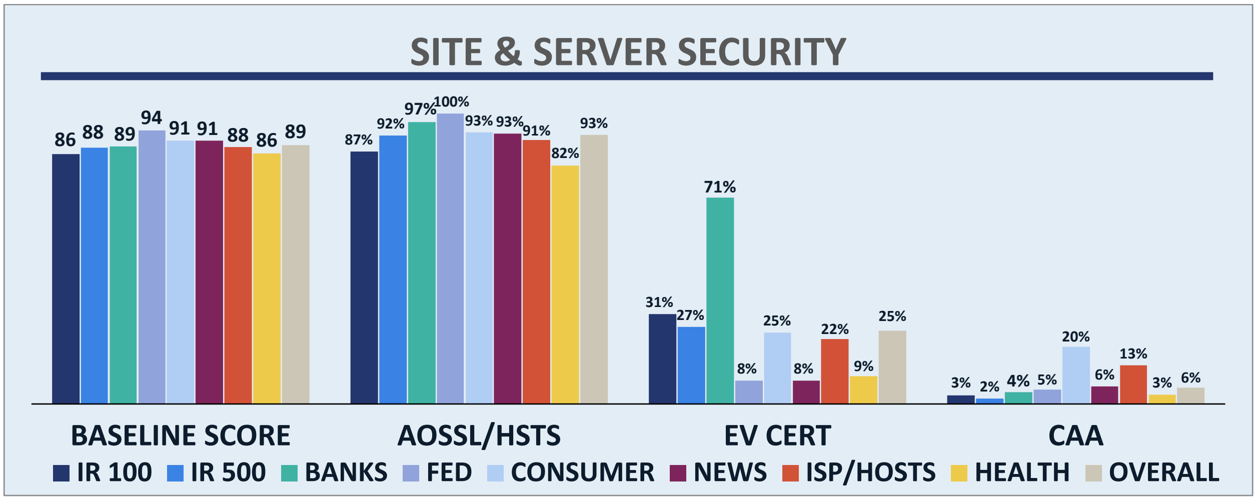


Figure 12 – Site & Server Security Scores/Adoption by Sector

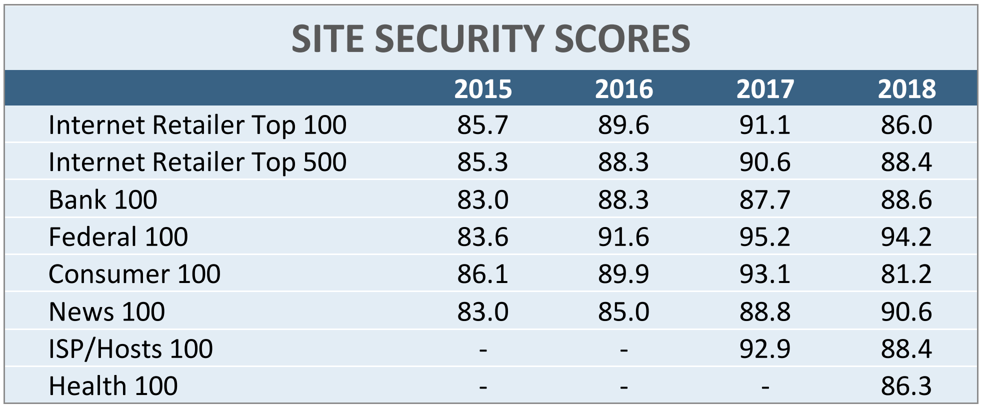
Server Implementation & Vulnerability Analysis

Ongoing SSL/TLS configuration monitoring and use of related security configurations is a fundamental requirement to optimize security and thwart vulnerabilities. The 2018 Audit has expanded the analysis with the addition of new tools, including those provided by ImmuniWeb, Internet.nl, Mozilla, Sucuri, Symantec and SSL Labs. Collectively the data was used to evaluate sites' SSL/TLS implementation, EV SSL adoption, CAA adoption, AOSSL adoption, third party content configuration, use of web application firewalls and vulnerability to cross-site scripting (XSS), iframe exploits, malware and malicious links.

As a reference to the overall state of SSL/TLS security, the March 2, 2019 monthly SSL Pulse report indicated that 66% of the 139,822 sites tested were considered secure, a continued increase from 58% in June 2017 and 43% in June 2016.[33] By comparison, 83% of sites in the OTA Audit are considered secure, indicating the Audit sample significantly outperforms the general population of websites. In the process of analyzing the site security scores, several trends were observed:

- Use of vulnerable key exchange parameters, ciphers and protocols decreased, but many sites still support older implementations. Commonly flagged issues were weak Diffie-Hellman parameters, RC4 ciphers, and use of SSL3 or TLS1.0 protocols (TLS1.0 was deprecated as part of the PCI standard as of June 2018).[34]
- 29% of sites support only TLS1.2 or later, which is the best practice recommendation. There are still some compatibility issues with older browsers that keep organizations from completely removing TLS1.0 and 1.1, but there has been a significant shift to remove protocols prior to TLS1.2. Seven percent of sites are supporting TLS1.3, which was officially published in August 2018, led by the ISP/Hosts and Healthcare sectors at 11%.
- Most sites are not setting a content security policy or taking advantage of headers that can limit vulnerabilities related to third-party content such as cookies. Specific results can be seen using the ImmuniWeb Website Security Test and Mozilla Observatory.

Malware was observed on 2% of sites overall and was most prevalent in Banks (10%). XSS/iframe vulnerabilities were observed on 21% of sites, a drop of more than half of the 50% observed in 2017. Sites were assessed with an XSS penalty if they had an occurrence in 2018 or have an unpatched XSS vulnerability reported prior to 2018.[35] Banks had the lowest presence of XSS/iframe vulnerabilities at 5%, but 43% of News sites and more than one-fifth of Consumer, Federal and News sites were vulnerable. Though the results are an improvement since 2017, the overall presence is still concerning and reinforces the need for organizations to continually monitor their sites and content management systems.



SITE SECURITY SCORES

	2015	2016	2017	2018
Internet Retailer Top 100	85.7	89.6	91.1	86.0
Internet Retailer Top 500	85.3	88.3	90.6	88.4
Bank 100	83.0	88.3	87.7	88.6
Federal 100	83.6	91.6	95.2	94.2
Consumer 100	86.1	89.9	93.1	81.2
News 100	83.0	85.0	88.8	90.6
ISP/Hosts 100	-	-	92.9	88.4
Health 100	-	-	-	86.3

Figure 13 – Site Security Score Average by Sector, 2015-2018

As shown in Figure 13, year-to-year security scores dropped in most sectors (Banks and News are the exceptions). Scores dropped entirely due to increased weight on non-SSL/TLS configuration factors, and mostly due to low scores seen in the ImmuniWeb Website Security Test and Mozilla Observatory. The Federal sector led for the third year in a row with a score of 94.2. As with XSS and malware, configuration and implementation of SSL/TLS and related site security elements requires continual monitoring since new vulnerabilities appear frequently. OTA's experience is that changes can usually be made quickly and inexpensively once decision makers are engaged.

SSL/TLS Certificate Types

Recognizing the importance of trust certificates and increasing concerns about certificate acquisition for fraudulent sites purporting to be popular consumer destinations, OTA started tracking certificate types in 2015. There are three major types of certificates – Domain Validation (DV), Organization Validation (OV) and Extended Validation (EV) – which have widely varying methods for validating the identity of the entity receiving the certificate. The official name and location of entities purchasing OV and EV certificates are verified and confirmed directly with the entity by certificate authorities and are included in the certificate. By contrast, DV certificates are typically verified through an automated process, making them more efficient and less expensive to acquire, leading to a large increase in the use of TLS. Following this trend, cybercriminals have also utilized them for phishing and look-a-like domains and content.[36] [37] [38]

EV SSL certificates provide a higher level of verification, requiring a comprehensive audit process. EV SSL provides differentiation by displaying the entity's name and a green visual trust indicator in the address bar or browser display, though differentiation has diminished in recent years and is not present in many mobile browser implementations. EV SSL certificates are mandated in some sectors (e.g., IRS free e-file providers).[39]

Recently there has been significant debate in the industry regarding the value of the different types of certificates, with some arguing that anything beyond the DV level adds no value.[40] Others argue that EV and OV certificates are worth the extra cost due to the differentiation in the browser (EV) or additional support in managing large batches of certificates or revoking compromised certificates.

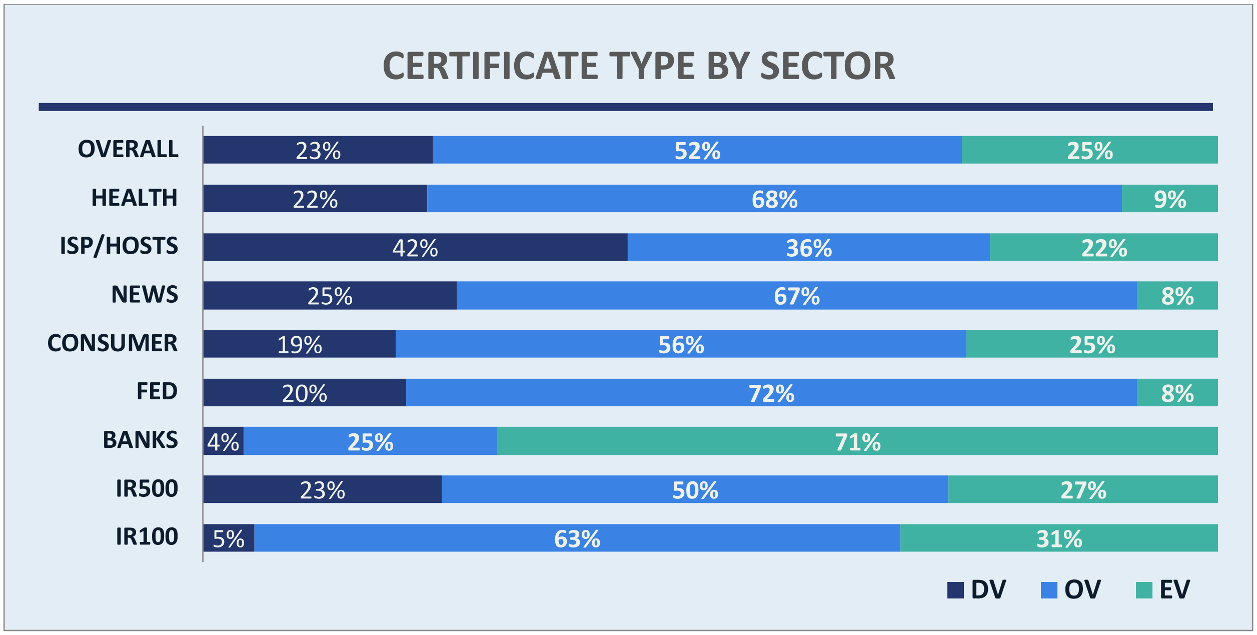


Figure 14 – SSL/TLS Certificate Type by Sector, 2018

Figure 14 shows adoption rates for each type of certificate by sector. Rates vary significantly by sector, with Banks tilted heavily toward EV certificates (71%), Federal, Healthcare and News sites tilted toward

OV certificates (67%-72%), and ISP/Host sites leaning toward DV certificates (42%). Figure 15 charts the overall shift over time, which shows a modest decrease in EV certificates in favor of DV certificates with OV certificates remaining flat.[41] When choosing certificate authorities and the type of certificate to use, domain owners should view the situation comprehensively and consider support and service in addition to the basic issuance of certificates.

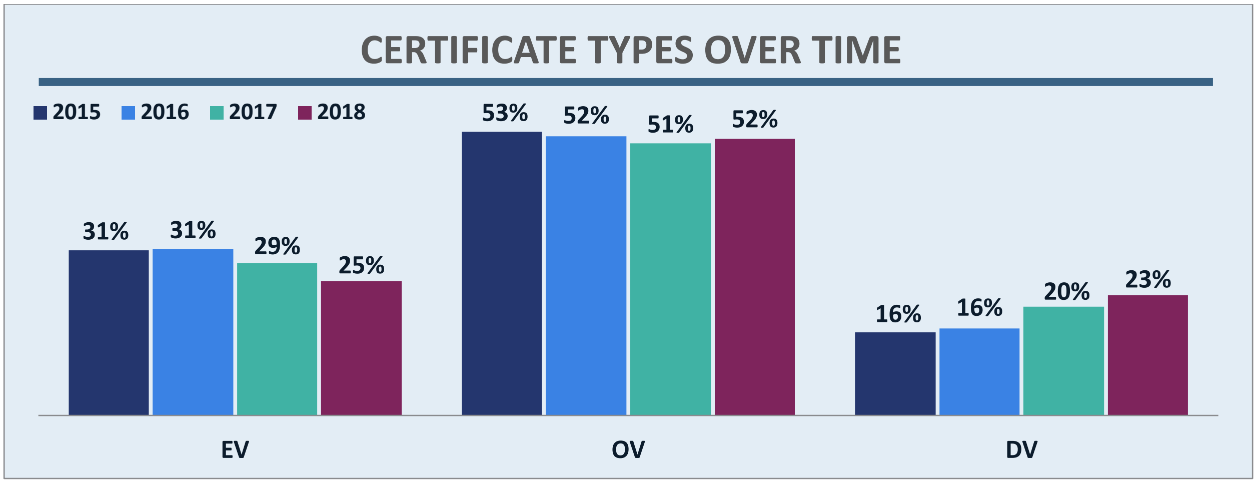


Figure 15 – SSL/TLS Certificate Type, 2015-2018

DDoS Mitigation

While outside the scope of this year's Audit methodology, organizations need to implement measures to help detect and mitigate the impact of a DDoS attack. According to Kaspersky Labs, there was 13% less DDoS activity in 2018 than in 2017, though the average duration of attacks grew from 95 minutes in Q1 of 2018 to 218 minutes in Q4.[42] Globally these attacks remain unpredictable and persistent, and vary widely in terms of volume, speed, and complexity. To combat these incidents, it is becoming increasingly important to constantly monitor threats to optimize the mitigation strategy. OTA recommends on-premise firewalls and dedicated DDoS appliances (or equivalent cloud services) to help stop malicious traffic. When configured properly, the associated malicious traffic can be effectively blocked and dropped before it reaches the intended servers.

Vulnerability Reporting Mechanisms

This was added to the methodology in 2017. Bonus points were awarded to organizations that have a mechanism to submit vulnerability reports either directly on their site or via third-party "bug bounty" programs. It was added in part because it is recognized as a best practice by NTIA, NIST and the FTC. Use of this practice nearly doubled, from 6% to 11%, since first assessed in 2017, but still remains fairly low. The Consumer sector led with 43% adoption, followed by ISP/Hosts at 25%, News at 9% and Banks at 6%. Having such a mechanism is recognized as critical to effectively respond to reports from third-party researchers and is relatively simple to implement. OTA advocates for sites to have a vulnerability reporting mechanism either hosted on their site (such as the online form designed by OTA) or by one of the leading third-party "bug bounty" programs.[43]

Malvertising

Cybercriminals have recognized the inherent vulnerability of the advertising ecosystem and use its complexity to distribute misleading messages and/or ads with malicious code in an effort to compromise users' devices and business systems. Known as malicious advertising, or "malvertising," it poses a growing threat to everyone who accesses ad-supported content online, as well as ad-supported services. In the last year, new techniques have been used to obscure malicious ads, and one firm estimates that malvertising is costing the online ad industry more than $1 billion a year.[44] Late in 2018, Amazon filed suit against operators of a site using malvertising to redirect users to their fraudulent site.[45] Though malvertising incidents were not tracked in the Audit, organizations should understand the ecosystem delivering ads for their sites and the protections that are in place to block malicious ads.

Privacy, Transparency & Disclosures

Note: In prior Audits, the term "privacy policy" was used to refer to a site's representation of their privacy practices. To align with global nomenclature, the term has been changed to "privacy statement". It should also be noted that the Audit assesses the assertions made in the privacy statement but not the organization's actual practices, which can vary dramatically from the stated policies, since the Audit only takes an external view.

The 2018 Audit showed modest increases in the transparency and readability of published privacy statements, with clear room for improvement. More statements are presented in a layered manner, disclosures are more complete and language is shifting toward more consumer-friendly wording instead of a contract written for a legal audience. Some of this may be the result of increased awareness of, and compliance with, the EU's General Data Protection Regulation (GDPR).

With the advent of GDPR it is more important than ever for organizations to embrace data stewardship. In addition, organizations need to be aware of other regional transborder rules such as the APEC Cross-Border Privacy Rules System. These are a set of voluntary yet enforceable privacy standards to allow data to flow across the Asia-Pacific region.[46] In 2020, the California Consumer Privacy Act (CCPA), which is largely modeled after the GDPR principles, will also go into effect, forcing US-based organizations to implement additional privacy protections if they wish to engage in the largest market in the U.S.[47] OTA has been advocating for increased transparency and discoverability of privacy statements since 2009, including recommending disclosure of data collection, usage, sharing and retention practices. Best practices include:

Basic notice/disclosure items

- Make sure the privacy statement has a link and is easily discoverable from the home page.
- Place the revision date of the statement at the top of the page.
- Provide access to archived versions of the statement, allowing users to see what has changed.
- Use a simple layered and/or short notice designed to help consumers understand the statement.
- Use icons to help consumers navigate privacy statements in conjunction with layered/short notices.
- Write statements for the site's target audience and demographics. Consider providing multi-lingual versions supporting non-English-speaking site visitors.

Clearly state key compliance policies

- Compliance with Children's Online Privacy Protection Act (COPPA) or related regulations.[48]

- Disclose whether the site honors Do Not Track (DNT) browser settings and preferably honor users' DNT browser settings.
- Provide a summary of the data retention policy, including a specific timeframe and for what reason data is retained.

Protect privacy and define protected sharing

- Do not share personal data with any third party except to deliver service to the user. Provide a clear statement including details regarding if, what and for what purposes data is shared.
- Require vendor compliance by contract and notify consumers that service providers are prohibited from the use or sharing of their data for any purpose other than providing services on behalf of the site.
- Provide disclosure of cross-device tracking.
- Utilize tag management systems or privacy solutions to manage third-party trackers.
- Disclose whether data will be shared to meet legal obligations and make best efforts to notify consumers if their data is requested by third parties due to legal requirements.

In 2017, the 100 baseline points were reallocated from 50% for privacy statement elements and 50% for use of tracking to 55% for the privacy statement and 45% for use of tracking. Privacy scores this year averaged 70, down from 73 in 2017, primarily due to more stringent scoring. Scores ranged from Internet Retailers at 67 to Consumer at 76. While most sector scores were down, Banks rose from 65 to 69 and News rose from 70 to 71.

Overall, slightly fewer organizations received failing privacy scores (declining from 16% to 15%), though results varied widely by sector (privacy failures grew from 16% to 23% for Internet Retailers and dropped from 34% to 14% for Banks and 19% to 10% for News). As represented in Figure 16, scores for the privacy statement component (worth 55 points) were in a fairly narrow range – from 25 to 33. Disappointingly, the overall average of 27 means that most organizations are only earning half of the privacy statement points available. Tracking scores were much more encouraging since all sectors earned more than 87% of the available 45 points.

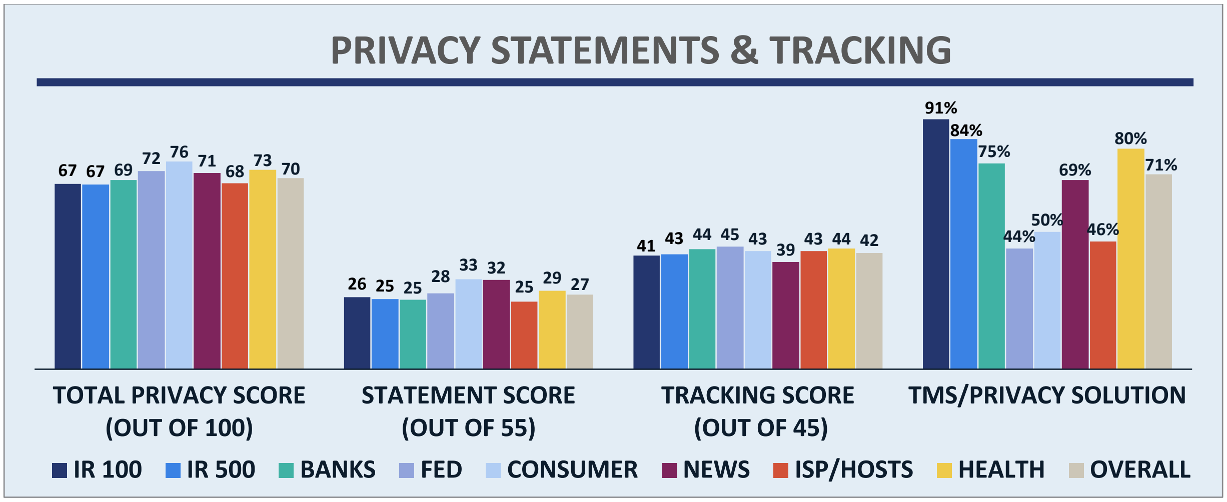


Figure 16 – Privacy Statement Scores and Tracking by Sector

Sites that rely on advertising and third-party analytics are faced with the challenge of managing third-party tracking. A growing challenge for site owners is knowing the respective data sharing practices of partners and the "domino data effect" which may occur with personal data being disclosed. Tag management systems and privacy solutions help monitor third-party data collection and sharing in real time. Bonus points were awarded if they were present.[49] Overall adoption grew to 71% from 69% in 2017, and this element is being considered for baseline scoring in future audits. Internet Retailers led adoption (84%). The Federal sector had the lowest adoption (44%), which is attributed to the low number of tags employed and the fact that they do not rely on advertising or data sharing.

Transparency

Providing both a clear notice of privacy statement revisions with a date stamp at the top of the page and a link to archived versions of previous privacy statements helps maximize transparency. Both elements are part of baseline scoring in the 2018 Audit. Overall, 47% of organizations had a date stamp at the top of the page (up slightly from 46% in 2017), but adoption varied widely – from only 2% in the Federal sector to 74% in the News sector. For the first time, privacy statement dates were captured – 31% of statements had no date stamp, while 11% had a date prior to 2017, 11% had a date in 2017, and 47% had a date after January 1, 2018. The Consumer sector privacy statements are the most "current" (71% have dates in 2018 or later), while the Healthcare sector has the least current statements (only 19% in 2018 or later). Use of version tracking for historical comparison of privacy statements dropped from 6% in 2017 to 3% in this year, primarily due to shifts in the list of audited organizations. Leading sectors are Consumer (12%) and ISP/Hosts (10%).

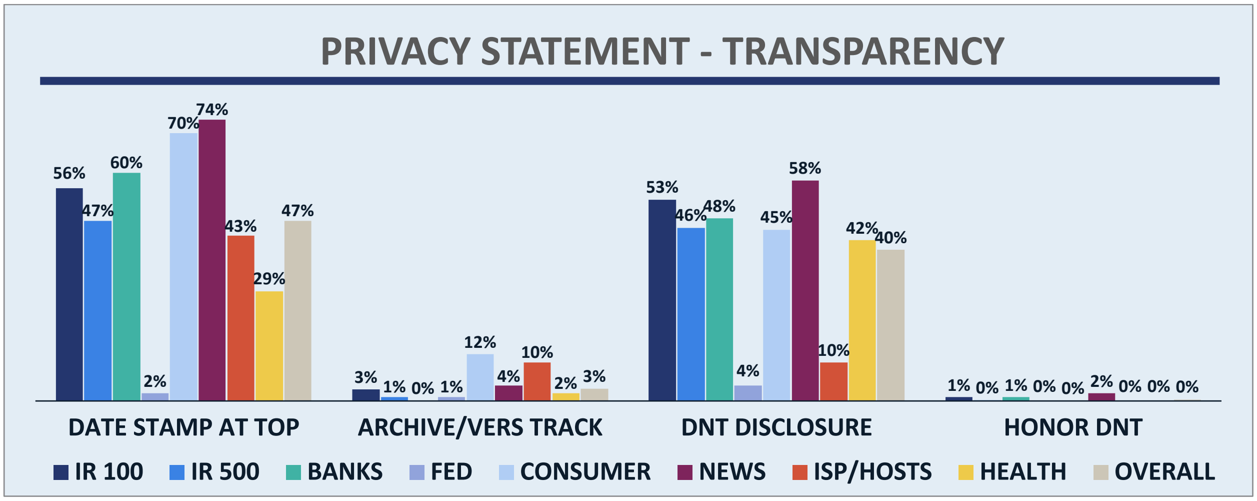


Figure 17 – Privacy Statement Transparency by Sector

Because disclosure of a site's Do Not Track (DNT) policy is currently a legal requirement in many jurisdictions, it is important for sites to state their DNT policy and ideally honor the browser's DNT setting as users visit the site. As shown in Figure 17, overall disclosure of DNT policy continues to rise, now at 40% versus 37% in 2017 and 13% four years ago. However, honoring of DNT settings has fallen even further, from 2% in 2017 to less than 0.5% this year. Overall, DNT seems to be coming to an end. Most browsers now incorporate other mechanisms to either automatically block online trackers (e.g., via native features, extensions or plug-ins) or give users direct control over block lists. Recently, support for DNT has been removed in version 12.1 of Apple's Safari browser, the project has been declared final by the W3C, and the new California Consumer Privacy Act (CCPA), which goes into effect on January 1, 2020 no longer requires it.[50] [51] Given this trend, it is likely that DNT will be removed as a scoring element in future Audits, though a significant portion of the privacy score is still tied to trackers on sites.

Readability & Disclosures

Designing a site's privacy statement for the intended readers instead of a legal audience has been long recognized by privacy professionals as a necessary shift. Not only does the language need to be written at the appropriate reading level, but the layout should maximize readability. Figure 18 outlines results for three scoring elements – layered short notices (baseline), user friendly icons (bonus) and making the privacy statement available in multiple languages (bonus). Use of layered notices jumped significantly to 47% from 29% in 2017, led by the News sector at 71%. Use of icons doubled from 1% to 2%, led by the Consumer sector at 7%. Support of multi-lingual privacy statements actually dropped, from 7% to 4%, which can be mostly attributed to changes in the list of audited organizations. OTA believes having the privacy statement in multiple languages helps enhance transparency and readability. It was observed that in some cases the language used for the privacy statement was triggered by browser settings or IP address location, so not every multi-lingual offering may have been captured in the Audit.

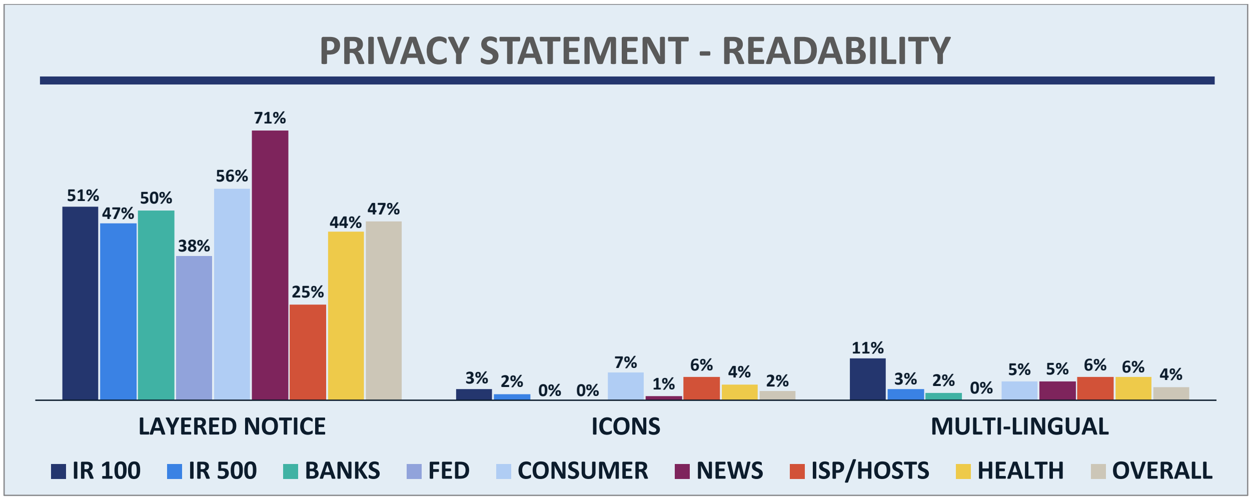


Figure 18 – Privacy Statement Readability by Sector

Data Handling

Maintaining and disclosing data sharing and retention practices is a core component of the privacy statement. In the 2018 Audit the data sharing element was broken into two parts – one for the core concept that data is not shared except potentially with third parties who help deliver the service, and one for language about sharing data with affiliates or other external third parties. Figure 19 outlines the results.

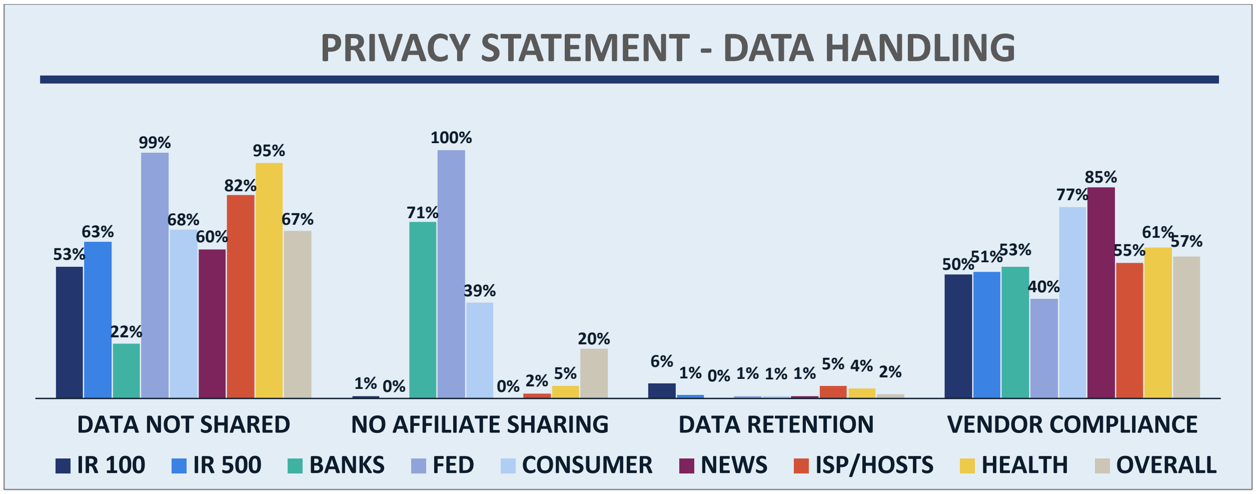


Figure 19 – Privacy Statement Data Handling by Sector

Language addressing data sharing (e.g., "we do not sell, rent or share data except to third parties who help deliver the service") is used by 67% of organizations (up from 63% in 2017), but varies widely. Affiliate sharing language varies even more, with the Internet Retailer and News sectors at 0% (meaning they all have language indicating that they share data with affiliates) and the Federal sector at 100%. Data retention language was scored much more strictly this year to align with GDPR principles. In 2017, adoption was 49% and credit was given for nearly any reference to data retention. This year, language had to be more specific, with a specific timeframe called out where possible. Use of vendor compliance language (third parties must comply with the organization's own privacy statement) grew from 48% in 2017 to 57% this year, led by the News sector at 85%. Two sectors had a notable, sharp rise in adoption of this element – Banks grew from 18% to 53% and News grew from 51% to 85%.

GDPR Compliance

For the first time this year the Audit included six variables intended to capture key aspects of GDPR compliance. It is important to note that most organizations in the Audit are based in the U.S. and may not need to directly comply with the GDPR. However, OTA felt that given the scope of GDPR and its impact on global privacy laws it was important to begin measuring how organizations were complying with key tenets of GDPR.

First, 32% of privacy statements were deemed easy to read. The goal of this GDPR requirement is that privacy statements should be easy for most users to understand, especially regarding what user data is being collected and shared. Banks had the highest percentage of easy to read statements (47%), while the News sector had the lowest level at just 8%. Clearly more work is needed here since more than two-thirds of privacy statements do not meet this goal.

GDPR does not prescribe exactly how an organization should convey what data is being collected and why, simply that the company does have to convey that information to users in some way. In that spirit, most organizations (95%) sufficiently articulated what data is being collected and for what reason. Banks led the way at 99%, while the Federal and ISP/Hosts sectors were the lowest at 90%.

Other aspects of GDPR have more specific requirements. For example, 70% of organizations in the Audit identify a means to contact the Data Protection Officer, led by the Consumer sector at 81%. The Federal sector lagged in this category at 38%. Another GDPR requirement is that organizations should lay out the process by which users can request their data, or what data they can request. Only 50% of organizations overall met this requirement, led by Internet Retailers at 71%.

Finally, there were two GDPR requirements with very low adoption rates. The first lays out the need to for organizations to disclose whether they have received specific types of "sensitive" data from third parties (e.g., biometric data, racial or ethnic origin, political opinions, religious or philosophical beliefs, and many others). Since this requirement applies only in limited cases, low adoption is not necessarily an issue. Only 1% of organizations specifically addressed this in their privacy statement, led by the Healthcare sector (4%). The second requires organizations to identify the categories of third parties data is shared with, and therefore should apply to any organization that shares data – less than 1% of organizations met this requirement.

Cross-Device Tracking

Starting with the 2017 Audit, in response to the FTC's 2017 cross-device tracking report, disclosure of tracking across various devices (e.g. desktop, phone, tablet, etc.) has been captured and receives bonus points. This year, 48% of sites had such a disclosure, up from 44% in 2017. It should be noted that cross-device tracking can have benefits, including an enhanced user experience when moving between devices, and security benefits for users logging in from other devices or IP addresses, but it also raises privacy concerns. The News sector had the highest adoption (91%), followed by the Consumer sector (80%), while the Federal sector had the lowest (12%).

WHOIS Registrations

When a company registers a domain name, the Internet Corporation for Assigned Names and Numbers (ICANN) requires businesses to submit contact information. This information is posted in the WHOIS database which is available to anyone, providing the registration is not private. The advent of GDPR has complicated WHOIS listings because personal contact information has been removed from many records for privacy reasons. Many organizations have gone one step further and redacted all of their information (even at the organizational level) making it difficult to determine who actually owns the domain.

As a result, private registrations (as defined by the ability to determine what entity owns the domain) rose this year. Overall, 78% of registrations were public (vs 87% in 2017). Further analysis reveals that 7% of the "private" records were tied directly to GDPR-related redactions, yielding a true public registration rate of 85%. Sectors with the highest use of private WHOIS registrations were ISP/Hosts (32%), Banks (29%) and Healthcare (28%). Private registrations limit consumers' ability to discover who the owner of a site is, impede transparency and may reduce consumer trust, not to mention a third party's ability to contact the site owner regarding an observed vulnerability. Conversely, private registrations are a valid and legitimate practice when registering a domain for a future company, product or marketing effort when in "stealth mode," though they should be made public once launched.

Data Loss Incidents & Regulatory Settlements

Data breaches and regulatory settlements can be indicative of poor data security, privacy and business practices. As such, they can have a major impact on an organizations' reputation and resulting level of consumer trust, while simultaneously placing the privacy and identity of users at risk. At the same time, it is important to recognize there is no perfect security and that a determined adversary with enough time and resources can compromise most any organization. As reported in OTA's 2018 Cyber Incident & Breach Trends Report, there were more than 159,700 data loss incidents tracked worldwide in 2017.[52]

This year's Audit included additional data from a variety of sources, providing a more comprehensive view of such incidents. OTA's analysis revealed that 15% of the audited organizations experienced one or more incidents, up from 13% in 2017 and 5% in 2016. The number of records lost ranged from a single record to more than 150 million. Recognizing that all incidents are not equal, organizations that experienced a cumulative loss of 1,000 records or less during the Audit period were not penalized, while the penalty assigned to breaches of more than 1,000 records was scaled proportionally with the size of the breach. Factoring in this adjustment, only 12% of organizations were penalized for a data breach. The Consumer sector had the highest level of breaches (34%), followed by Healthcare (30%).

On the regulatory front, 2% of audited organizations received a penalty for consumer protection related suits or settlements this year (flat to 2017), led by the Consumer sector (12%). Assessment included settlements from the FTC, FCC, CFPB, states and international agencies. The focus was on settlements related to consumer protection actions involving security and privacy and did not include settlements pertaining to mergers and acquisitions and/or labor issues.

Conclusion

As in prior years, the Online Trust Audit & Honor Roll serves three primary objectives:

- Promote best practices to enhance sites' security, data protection and privacy practices
- Recognize excellence in consumer protection, security and responsible privacy practices
- Provide consumers with added transparency regarding the security and privacy practices of sites they visit

The 2018 Audit saw record levels in many areas – the largest single year-to-year jump in overall Honor Roll achievement (52% to 70%), the highest levels of email authentication adoption (76% support SPF and DKIM at the top-level domain), and the highest levels of Internet encryption (73% use opportunistic TLS for email and 93% encrypt all sessions to their website). This was despite more stringent methodology criteria, tighter scoring and more weight placed on key best practices in consumer protection, site security and privacy.

Certain sectors shone this year – Federal government agencies recovered from a poor showing in the 2017 Audit to lead all sectors with 91% Honor Roll achievement, and News/Media organizations continued their near geometric growth in Honor Roll achievement, rising into the top tier at 78%. The newly added Healthcare sector came in last at 57% (which in prior years would have been a solid showing), primarily due their lack of email authentication.

In many areas adoption of best practices is nearing full saturation, at 90% or higher, and while this should be celebrated it is still incumbent on organizations that have not yet adopted these widely accepted baseline practices to place a priority on implementation.

In other areas there are concerning trends. Despite heightened awareness and sensitivity to privacy issues driven by GDPR, the California Consumer Privacy Act, and highly publicized privacy failures by large companies, privacy statements have improved little, and most organizations are scoring less than 50% on the privacy statement portion of the Audit. Of particular concern is the largely undefined sharing of data with third-party affiliates. Initial baselining of GDPR-related requirements revealed a wide range of adoption – from 1% to 95%, depending on the requirement – and this will need to be addressed as the regulatory environment, whether at the state or global level, continues to evolve.

Looking forward, there are many opportunities for organizations to limit the impact of massive data breaches and stop questionable data collection and tracking practices. Many site owners now prevent users from using known breached username/password pairs and are implementing multi-factor authentication to limit the impact of breached passwords. Similar capabilities are also being incorporated into browsers. In addition, because many website owners are not stepping up to limit data collection and tracking, others have stepped into the void. Most browsers now incorporate some level of ad and tracker blocking.

Improving security and privacy is a collective responsibility for all stakeholders, and we each need to fulfill our part to maintain trust in the Internet. OTA collaborates with all stakeholders in the public and private sector to work toward improving and enhancing the health of the Internet, providing a trusted platform for innovation. For updates visit https://otalliance.org/TrustAudit.

2018 Online Trust Audit & Honor Roll Results

The Internet Society's Online Trust Alliance conducts an annual Online Trust Audit & Honor Roll - the de facto standard for recognizing excellence in online consumer protection, data security and responsible privacy practices.

70%
OVERALL ACHIEVEMENT

Highest ever, driven largely by improvements in email authentication and encryption

HONOR ROLL BY SECTOR

U.S. FEDERAL GOVERNMENT	91%	(most improved, up from 39% in 2017)
CONSUMER SERVICES	85%	
NEWS AND MEDIA	78%	(continued rapid rise year-over-year – 4%, 8%, 23%, 48%, 78%)
BANKS	73%	(nearly tripled from 27% in 2017)
INTERNET RETAILERS	65%	
ISPS, CARRIERS, HOSTERS AND EMAIL PROVIDERS	63%	
HEALTHCARE	57%	(new this year)

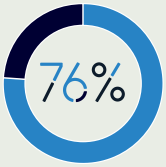
OTA
Online Trust Alliance
an **Internet Society** initiative

https://otalliance.org/2018HonorRoll

2018 Category Highlights

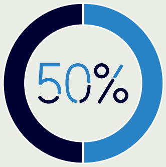
DOMAIN (TLD), BRAND, AND CONSUMER PROTECTION

Record levels of email authentication



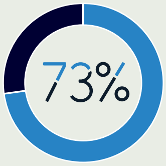
76% use both SPF & DKIM at the top level domain

SPF and DKIM prevent forged/spoofed emails.



50% have a DMARC record

DMARC provides instruction on how to handle messages that fail authentication.



73% use opportunistic TLS

TLS encrypts messages between mail servers.

SITE, SERVER, AND INFRASTRUCTURE SECURITY

Encrypted Web Sessions

52% → 93%

Huge jump from 52% in 2017
93% use HSTS/Always-On SSL/
HTTPS Everywhere

6% Only 6% use Certificate Authority Authorization (CAA)

CAA limits certificate abuse.

11% Only 11% use vulnerability disclosure mechanisms

Allows reporting of bugs and security problems.

PRIVACY, TRANSPARENCY, AND DISCLOSURES

70

Combined score dropped to 70 (73 last year) due to more stringent scoring in light of GDPR, CCPA, and other legislative efforts.

77%

use web trackers that share information with 3rd parties.

15%

15% had 1 or more data loss or breach incident.

https://otalliance.org/2018HonorRoll

2018 Sector Highlights

CONSUMER SERVICES

Added payment services and video streaming services this year.

96%

Top adoption of email authentication (96%).

76

top overall privacy score (76).

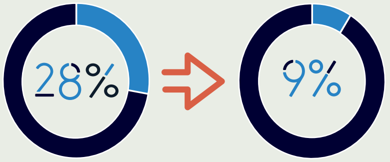
43%

highest use of vulnerability reporting (43%, next closest is 25%).

34%

Highest breach rate (34%).

INTERNET RETAILERS



Significant improvement in email authentication (failures dropped from 28% to 9%) though lowest DMARC adoption (34%).

50%

Privacy failures rose nearly 50% (to 23%) due to third-party sharing.

NEWS AND MEDIA

Added sports sites this year.

78%

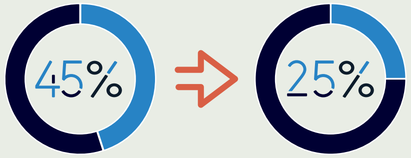
HONOR ROLL

Continued significant improvement in all areas, resulting in another jump in Honor Roll achievement (to 78%).

x4

Nearly quadrupled use of always encrypted sessions (26% to 93%).

ISPS, CARRIERS, HOSTERS AND EMAIL PROVIDERS



Significant improvement in email authentication (failures dropped from 45% to 25%).

1ST 11%

Highest adoption of TLS 1.3

2ND 20%

2nd highest support of IPv6

FEDERAL GOVERNMENT

91%

HONOR ROLL

Top overall Honor Roll achievement (91%) – big turnaround from last report when they had dropped from 46% to 39%.

94

Top site security score (94).

1ST 93%

Highest DMARC adoption (93%) and DMARC policy enforcement (83%).

46%

Highest IPv6 adoption (46%).

BANKS

45%→13%

Significant improvement in email authentication (failures dropped from 45% to 13%).

2ND 84%

Second highest use of both SPF and DKIM at top-level domain (84%, up from only 30% in last Audit).

1ST 71%

Highest use of extended validation certificates for websites (71% - more than double the next closest sector).

HEALTHCARE

NEW

New this year, represent blend of top pharmacies, testing labs, health insurance companies and hospital chains.

57%

Lowest overall Honor Roll achievement (57%), mainly due to lack of email authentication (35% failed in this area).

2ND 73

Second highest privacy scores (73). Lowest adoption of always encrypted sessions (82%).

https://otalliance.org/2018HonorRoll

Appendix B – Methodology & Scoring

The Audit criteria and methodology evolve every year, reflecting developments in security standards, privacy norms and real-world deployment. Annually, OTA actively solicits input from the Internet at-large through a 60-day call for public comments typically issued in early September.[53] In addition, several U.S. government agencies and industry standards organizations are consulted. After review, the OTA Trust Audit Planning Committee incorporates some of the core security and privacy directives, including Fair Information Practice Principles (FIPPs), NIST standards, and those supported by the Internet Society's Deploy360 Programme.[54] Reflecting this combined input, weighting and scores are re-examined annually and re-allocated to address the evolving threat landscape, regulatory environment and ease of deployment. The end result focuses on accepted best practices reflecting real-world deployment, bridging the gap between the standards and business communities. The final methodology for this year's Audit was published in August 2018 and promoted broadly to provide organizations the ability to re-evaluate their practices and optimize their scores.[55]

The Online Trust Audit includes a composite analysis focusing on three major categories:

- Consumer Protection (DNS, Domain & Brand Protection)
- Site, Server, Application & Infrastructure Security
- Privacy, Transparency & Disclosures

Sites were eligible to receive 300 base points (up to 100 points in each category), and up to 60 bonus points (20% of the base score) for implementing emerging best practices. Additionally, organizations could lose points for having regulatory settlements, data breaches, observed vulnerabilities and other key deficiencies.

To qualify for the Honor Roll, sites had to receive a composite score of at least 80% of the baseline points *and* **a score of at least 60** in each of the three main categories. The failure bar was raised to 60 in 2017, recognizing that "security is only as strong as the weakest link" and sites are built on a "chain of trust".

The 2018 Audit has been powered by technical analysis and data provided from more than a dozen organizations. Without their assistance and support, this Audit and telemetry would not be possible. Data sampling was completed between December 10, 2018 and January 31, 2019. Organizations providing data included Agari, Disconnect, dmarcian, ImmuniWeb, Infoblox, Internet.nl, Microsoft, Mozilla, SSL Labs, Sucuri, Symantec, Valimail and Verisign. Additional data was obtained from public data sources including BugCrowd, Google, HackerOne, Open Bug Bounty, Twitter and others. It is important to note that a site's configuration or practices may have changed since the sampling and the data only reflects findings during this snapshot in time.

Consumer Protection (DNS, Domain & Brand Protection)

Email continues to be the top attack vector of choice, driving business email compromise (BEC), credential and identity theft, bank account takeovers and distribution of malware.[56] The FBI reports that BEC fraud has generated $12.5 billion in financial losses since 2013, most of which could have been prevented.[57] For the past decade OTA has advocated for end-to-end email authentication to help detect and block malicious and spoofed email for all domains and subdomains managed by an organization. Adoption helps protect consumers and email recipients from distribution of malware, key loggers and related threats including ransomware, cryptomining and account takeovers, while additionally protecting the reputation of the targeted brand.

- Email authentication (Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM)) at top-level ("corporate") domains, and email subdomains. The 2018 Audit increases weight on authenticating top level domains (most recognizable to the user and most frequently spoofed), with reduced points for separate delegated sub-domains. In addition, sites with invalid SPF records received only partial or no credit – *part of base score* [58]
- Domain-based Message Authentication, Reporting & Conformance (DMARC). DMARC records where p=none and have no reporting (RUA or RUF) do not receive any credit. Referred to as "naked DMARC records", they do not provide any consumer or brand protection value since receiving networks do not respond to the policy and the brands do not get authentication and abuse reports. Weight was increased on use of the "reject" policy – *part of base score* [59]
- Implementation of "opportunistic" Transport Layer Security (TLS) for email. Weight was increased in 2018 – *bonus points* [60]
- Domain locking – *penalty if domain not locked*
- Domain Name System Security Extensions (DNSSEC) – *bonus points* [61]
- Implementation of Internet Protocol version 6 (IPv6) for web server access – *bonus points* [62]
- Multi-factor authentication – Though multi-factor authentication was awarded bonus points in the 2017 Audit, it was not repeated in this Audit due to insufficient data sources across all sectors.

Site, Server & Infrastructure Security

Best practices to secure data in transit and collected by websites, and prevent malicious exploits running against clients' devices. Sites were eligible to score up to 100 base points, provided any single core SSL/TLS criteria (ciphers, key exchange or protocol support) did not score below 60. Sites were tested with several tools to look for known vulnerabilities, HSTS configuration and mismatched certificates. [63, 64] In 2017 server security was expanded to include application security, patching cadence and IP reputation. It was extended further in 2018 to include robust assessments of content security policy and preventions related to third-party content on sites. Support of Always On SSL was incorporated into baseline scoring in 2018.[65]

Bonus / Penalty Points

- Extended Validation SSL Certificates (EV SSL) – *bonus points* [66]
- Certificate Authority Authorization (CAA) – new in 2018 – *bonus points*
- Web Application Firewall – *bonus points*
- Testing for XSS, iFrame exploits, malware, malicious links – *penalty if these threats exist*
- Vulnerability & Bug Reporting Mechanism – Instituted in 2017, sites earn bonus points for reporting mechanisms including online forms and/or using third-party bug bounty reporting. Data was analyzed by online searches using keywords, as well as searching third-party bug bounty programs including HackerOne and Bugcrowd [67, 68] – *bonus points*

Privacy, Transparency & Disclosures

Best practices for all organizations include providing users with clear notice, transparency and control of the data being collected, tracked and shared with third parties. The privacy score is comprised of up to 100 points covering: inclusion of appropriate disclosures; structure of the privacy statement itself (including adoption of generally accepted Fair Information Practice Principles (FIPPS)); and tracking and third-party data collection.[69] Privacy statements were read and scored by OTA/Internet Society analysts.

Privacy Statement – 55 points possible. Sites can receive maximum scores by adhering to the following guidelines:

- Link / discoverability from the home page
- Date stamping of privacy statement on the top of the page
- Disclosure regarding handling of browser Do Not Track (DNT) setting
- Data retention policy statement with a specific timeframe reference (timeframe new in 2018)
- Personal data not shared, except with third parties who deliver the service
- Personal data not shared with affiliates or partners (separated from core data sharing in 2018)
- Vendor compliance – disclosure that service providers must comply with the organization's privacy statement and are prohibited from the use or sharing of data for any purposes other than providing services on behalf of the organization
- Version tracking (or access to prior versions), including posting of revision mark-ups (was bonus points prior to 2018)
- Designed as a layered and/or short notice
- Compliance with Children's Online Privacy Protection Act or similar regulation [70]

Third-Party Tracking on Site – 45 points possible for sites with no third-party trackers (with the exception of anonymous analytics). Observed trackers known to share data with third parties result in reduced points.[71]

Bonus Points

- Use of consumer-friendly icons to assist navigation
- Localized/multi-lingual statement where English may be a "second language"
- Honoring of a user's Do Not Track browser (DNT) setting
- Cross device Tracking Disclosures (added in 2017) [72]
- Implementation of tag management systems or privacy solutions to manage third-party tags

Penalty Points

- Data breaches – for breaches of more than 1000 records. For the 2018 Audit, the penalty was scaled proportionately with the size of the data breach – *penalty if qualifying incident between June 1, 2017 and December 31, 2018*
- Regulatory settlements with the Federal Trade Commission (FTC), Federal Communications Commission (FCC), Consumer Financial Protection Bureau (CFPB)[73], State or global – *penalty if settlement between June 1, 2017 and December 31, 2018.*
- Public vs. Private WHOIS registration – *penalty if private*

Appendix C – 2018 Top 50 Honor Roll

Sector	Organization	Sector	Organization
C	1040.com	C, **R**	**Google Play**
H	**23 and Me**	O	Internet Society
C	Airbnb	C	Lyft
C	Amazon Payments	G	National Oceanic and Atmospheric Administration (NOAA)
R	Apple Inc.	C	Netflix
C	Blogger	C, O	Norton LifeLock
R	Casper	G	Office of Personnel Management (OPM)
H	Costco Pharmacy	**O**	**Online Trust Alliance**
G	Dept of Agriculture (Food Safety & Inspection Service)	**C**	**PayPal**
G	Dept of Health & Human Services (Medicare)	R	Petco Animal Supplies Inc.
G	Dept of Health and Human Services (Healthcare.gov)	C, N	Reddit
G	Dept of Treasury	G	Securities and Exchange Commission (SEC)
C	DocuSign	C	Snapchat
G	Federal Communications Commission (FCC)	G	Social Security Administration (SSA)
G	**Federal Emergency Management Agency (FEMA)**	C	Square Cash
G	Federal Trade Commission (FTC)	I	Sucuri
B	**First National Bank of Omaha**	B	TD Bank, National Association
R	Fitbit Inc.	B	The Huntington National Bank
C	Flickr	C	Tinder
R, O	Gap Inc.	O	TrustSphere
G	General Services Administration (GSA)	C, O	Twitter
I	**Google Cloud**	C	UpWork
C	Google Drive	G	US Armed Forces - Coast Guard
N	**Google News** ◆	R	Walmart Inc.
C	Google Pay	C	YouTube

Sector Codes: C – Consumer Services, B – Banks, G – U.S. Federal Government, H – Healthcare, I – ISP/Hosts, N – News/Media, O – OTA / Internet Society Member, R – Internet Retailers. As noted, organizations can be in multiple segments.

Top scorers in each sector are highlighted in bold. The top overall score is marked with a ◆.

Appendix D – 2018 Honor Roll Recipients

2018 Internet Retailer 500 – Honor Roll

65% Honor Roll – 31% Failing – 14% of "Top of Class"

- ❷ 1-800 Contacts Inc.
- 1-800-Flowers.com Inc.
- 1Sale
- ❷ Abercrombie & Fitch Co.
- ❷ AC Lens
- adidas AG
- Adorama Camera Inc.
- ❷ Adore Me Inc.
- Aéropostale Inc.
- AJ Madison Inc.
- ❷ Albertsons Inc.
- Aleph Objects Inc.
- ❸ Alex and Ani LLC
- ❼ Alibris Inc.
- Allied Electronics
- ❼ Amazon.com Inc.
- ❼ American Greetings Corp.
- American Standard Brands
- AmeriMark Direct LLC
- ❹ APMEX Inc.
- ❸ **Apple Inc.**
- Aquasana Inc.
- Art.com Inc.
- Ascena Retail Group
- ❷ Ashley Stewart Inc.
- ASOS Plc Holdings
- ❷ AutoZone Inc.
- ❷ B&H Foto & Electronics Corp.
- ❷ Backcountry.com
- Balsam Brands
- Barcodes Inc.
- Bare Necessities
- ❷ Barnes & Noble Booksellers Inc.
- Barneys New York Inc.
- ❼ Bass Pro Shops
- ❷ BaubleBar Inc.
- BeachCamera.com
- bebe stores Inc.
- Belk Inc.
- ❻ Best Buy Co. Inc.
- ❷ Better World Books
- Big 5 Corp.
- Birchbox Inc.
- Bissell
- ❹ BJ's Wholesale Club
- Black & Decker Inc.
- Black Diamond Equipment Ltd.
- Blain Supply Inc.
- ❷ Blue Nile Inc.
- ❸ Bluefly Inc.
- Bob's Discount Furniture LLC
- Boohoo.com plc
- ❸ Bookbyte
- Boot Barn Inc.
- ❷ Boscov's Department Store LLC
- Boston Proper LLC
- ❸ Boxed Wholesale
- Brilliant Earth LLC
- Brooklinen
- Brooks Brothers
- ❻ BuildASign.com
- ❹ BuildDirect Technologies Inc.
- ❹ Burberry Ltd.
- CafePress Inc.
- Camping World Inc.
- ❷ Carter's Inc.
- ❷ **Casper**
- Chanel S.A.
- ❸ Chico's FAS Inc.
- ❷ Christopher & Banks Corp.
- Classic Firearms
- ❸ Code42 Software Inc.
- Columbia Sportswear Co.
- Concept2 Inc.
- Cool Stuff Inc.
- ❹ Costco Wholesale Corp.
- Crocs Inc.
- Crucial Technology
- ❹ Crutchfield Corp.
- ❷ CustomInk
- Cutlery and More LLC
- ❷ CVS Caremark Corp.
- ❸ Cymax Stores Inc.
- Databazaar.com
- dbrand
- Deckers Brands
- ❷ DeepDiscount.com
- ❷ Dell Inc.
- Destination XL Group Inc.
- Dick Blick Holdings Inc.
- ❷ Diesel
- Digi-Key Electronics
- ❹ Dollar Shave Club
- Dollar Tree Inc.
- ❷ Dolls Kill
- ❷ Dover Saddlery Inc.
- DrJays.com
- Duluth Trading Company
- Dyson Ltd.
- eCampus.com
- ❹ Eddie Bauer LLC
- ❹ Entertainment Earth Inc.
- ❻ Etsy Inc.
- Everlane Inc.
- Evine Live Inc.
- ❷ Fanatics Inc.
- Fashion Nova
- ❸ **Fitbit Inc**.
- Flight Club
- Floor & Décor Outlets of America Inc.
- Focus Camera Inc.
- ❸ Follett Higher Education
- ❷ Foot Locker Inc.
- ❹ Forever 21
- ❹ Fossil Inc.
- FragranceNet.com Inc.
- FreshDirect LLC

Bold – Top 50 Overall ◆ – Top score in sector ❷ ❸ ❹ ❺ ❻ ❼ – Consecutive years as Honor Roll recipient

2018 Internet Retailer 500 – Honor Roll, continued

Full Compass Systems Ltd.
Furniture.com Inc.
❻ GameFly Inc.
Gander Mountain
❹ **Gap Inc.**
Gardeners Supply Company
Gear Patrol LLC
GlassesUSA LLC
Global Equipment Company Inc.
Glossier Inc.
GNC Holdings Inc.
❷ Godiva Chocolatier Inc.
❸ **Google Play** ◆
❸ GoPro Inc.
GrabAGun.com
Grizzly Industrial Inc.
Groupon Goods
Guess Inc.
Hallmark Cards Inc.
HanesBrands Inc.
Hanover Company Store LLC
❸ Harry's Inc.
Helix Sleep
Herman Miller Inc.
❸ hhgregg Appliances Inc.
Hobbico
❷ Home Chef
❷ Hot Topic Inc.
HP Home & Home Office Store
❹ iHerb Inc.
❹ IKEA
❷ Indigo Books & Music Inc.
Inditex Group
J. Crew Group Inc.
J. Jill
❷ J.C. Penney Co. Inc.
❷ J.Hilburn Inc.
Jabra
❻ JackThreads Inc.
JEGS High Performance Inc.
JetPens.com
JM Bullion Inc.
❹ Joann.com

KEH Inc.
❷ Keurig Green Mountain Inc.
Klipsch Group Inc.
❷ Lakeshore Learning
❸ Lands' End
LD Products Inc.
❷ Leesa Sleep LLC
❷ Lenovo Group Ltd.
Leslies Poolmart Inc.
Levi Strauss & Co.
❹ LifeWay Christian Resources
❷ LightIntheBox Ltd.
❷ Living Spaces
❻ LivingSocial Inc.
Loot Crate Inc.
❸ Lowe's Cos. Inc.
LuckyGunner LLC
LuLuLemon Athletica Inc.
❷ LuLu's Fashion Lounge Inc.
Lumber Liquidators Inc.
LVMH
M. Gemi
❷ Macy's Inc.
Mattel
❷ Mattress Firm Inc.
Meijer Inc.
❷ Michael Kors Holdings Ltd.
Micro Electronics Inc.
❷ MidwayUSA Inc.
MLB Advanced Media
Moda Operandi Inc.
❹ Monoprice Inc.
Monrovia
❷ MotoSport LLC
Mouser Electronics Inc.
MSC Industrial Supply Co. Inc.
❷ MVMT Watches
NakedWines.com Inc.
❹ National Hockey League
❸ NatureBox Inc.
❷ Nebraska Furniture Mart
❹ New Avon LLC
❷ New Balance Athletics Inc.

New York & Co. Inc.
❺ Newegg Inc.
❺ Nike Inc.
❷ Nine West Holdings Inc.
❺ Nordstrom Inc.
❷ Office Depot Inc.
❹ OmahaSteaks.com Inc.
OMEGA Engineering Inc.
OpticsPlanet Inc.
❸ O'Reilly Auto Parts
❷ Otto Group
OvernightPrints.com
❼ Overstock.com Inc.
Painful Pleasures Inc.
Palmetto State Armory
❷ Panasonic Corp.
❷ Patagonia
❼ Payless ShoeSource Inc.
PC Connection Inc.
Performance Bicycle
❹ **Petco Animal Supplies Inc.**
❸ PetFlow
❷ PetSmart Inc.
❹ Pier 1 Imports Inc.
❸ Power Equipment Direct Inc.
Primary Arms LLC
Pro:Direct
❸ PropertyRoom.com Inc.
Provo Craft & Novelty Inc.
❷ Purple
❷ Qurate
❹ REI
❷ Reitmans (Canada) Ltd.
Rent the Runway Inc.
❷ Replacements Ltd.
❸ Restoration Hardware
RevZilla Motorsports LLC
❷ Richline Group
RobotShop Inc.
❻ RockAuto LLC
Rockler Companies Inc.
Rooms To Go Inc.
❷ rue21 Inc.

Bold – Top 50 Overall ◆ – Top score in sector ❷ ❸ ❹ ❺ ❻ ❼ – Consecutive years as Honor Roll recipient

2018 Internet Retailer 500 – Honor Roll, continued

Rural King
❸ Saatva Inc.
Samsonite International S.A
Scholastic Inc.
School Specialty Inc.
❷ Sears Holdings Corp.
Sears Hometown/Outlets
Sennheiser Electronic GMBH & Co.
❹ Shindigz
Shoe Carnival Inc.
Shoes of Prey Inc.
ShoppersChoice.com LLC
Shutterfly Inc.
Signet Jewelers Ltd.
Silver Star Brands
Skinit Acquisition LLC
Sonos Inc.
❻ Spiraledge
ssense.com
❷ Staples Inc.
SteelSeries ApS
Stitch Fix
❸ Summit Racing Equipment
Sun Basket
❷ Sur La Table Inc.
❺ Sweetwater

Tackle Warehouse LLC
Tapestry
❷ Target Corp.
Tarte Inc.
Teespring Inc.
❷ Tennis Warehouse
❹ The Clymb
The Container Store Inc.
The Estee Lauder Cos. Inc.
The Finish Line Inc.
❷ The Great Courses
❸ The Home Depot Inc.
❹ The Honest Company Inc.
❷ The Kroger Co.
❷ The Lakeside Collection
The Men's Wearhouse Inc.
❹ The Nature's Bounty Co.
❹ The Orvis Co. Inc.
❸ The RealReal Inc.
The Walt Disney Company Ltd.
❷ ThriftBooks Global LLC
❷ Thrive Market
❷ Tiffany & Co.
❹ Tilly's Inc.
❹ TJX Cos. Inc.
❹ TOMS Shoes LLC

Tory Burch LLC
Traeger Grills
Trans World Entertainment
TSC
❷ Tuft & Needle
Uniqlo
United States Mint
Value City Furniture
Vera Bradley Retail Stores LLC
VIPOutlet
Vitamin Shoppe Industries Inc.
Vizio Inc.
W.W. Grainger Inc.
❷ **Walmart Inc.**
❹ Warby Parker
❻ Wayfair Inc.
Weber Grills
Whirlpool
❷ Wolverine Worldwide Inc.
Xerox Corp.
YDesign Group LLC
❹ Zazzle Inc.
Zenni Optical Inc.
❹ Zumiez Inc.

Bold – Top 50 Overall ◆ – Top score in sector ❷ ❸ ❹ ❺ ❻ ❼ – Consecutive years as Honor Roll recipient

2018 Bank 100 – Honor Roll

73% Honor Roll – 27% Failing – 6% of “Top of Class”

- American Express National Bank
- ❺ Arvest Bank
- Associated Bank, National Association
- BancorpSouth Bank
- ❼ Bank of America, National Association
- ❸ Bank of Hawaii
- Bank of Hope
- ❸ Bank of the West
- Bank OZK
- Barclays Bank Delaware
- ❺ Branch Banking and Trust Company
- ❹ Capital One, National Association
- Cathay Bank
- Centennial Bank
- Charles Schwab Bank
- ❷ Chemical Bank
- CIBC Bank USA
- ❺ Citibank, National Association
- ❷ Citizens Bank, National Association
- ❺ City National Bank
- ❸ Comerica Bank
- ❸ Commerce Bank
- ❸ Compass Bank
- ❸ Deutsche Bank Trust Co, Americas
- ❹ Discover Bank
- E*TRADE Bank
- ❹ Fifth Third Bank
- First Hawaiian Bank
- First Midwest Bank
- ❷ **First Nat’l Bank of Omaha** ◆
- ❹ First Republic Bank
- ❼ Frost Bank
- Goldman Sachs Bank USA
- ❸ Hancock Whitney Bank
- HSBC Bank USA, National Association
- ❹ Iberiabank
- Investors Bank
- ❸ JPMorgan Chase Bank, National Assoc
- ❸ KeyBank National Association
- Manufacturers & Traders Trust Co.
- MB Financial Bank, National Assoc.
- MidFirst Bank
- ❻ Morgan Stanley Bank, National Assoc.
- ❹ MUFG Union Bank, National Assoc.
- New York Community Bank
- Old National Bank
- Pacific Western Bank
- Pinnacle Bank
- PNC Bank, National Association
- Prosperity Bank
- ❺ Regions Bank
- Sallie Mae Bank
- ❷ Signature Bank
- ❷ Silicon Valley Bank
- South State Bank
- Stifel Bank and Trust
- ❸ SunTrust Bank
- ❷ Synovus Bank
- ❸ TCF National Bank
- ❸ **TD Bank, National Association**
- ❷ The Bank of New York Mellon
- ❹ **The Huntington National Bank**
- The Northern Trust Company
- TIAA, FSB
- ❼ U.S. Bank National Association
- UBS Bank USA
- UMB Bank, National Association
- ❸ Umpqua Bank
- United Bank
- USAA Federal Savings Bank
- Washington Federal, National Assoc.
- Western Alliance Bank
- Zions Bancorporation, N.A.

Bold – Top 50 Overall ◆ – Top score in sector ❷ ❸ ❹ ❺ ❻ ❼ – Consecutive years as Honor Roll recipient

2018 U.S. Federal Government 100 – Honor Roll

91% Honor Roll – 8% Failing – 26% of "Top of Class"

Administrative Office of US Courts (Judiciary)
Bureau of Labor Statistics (BLS)
❹ Census Bureau
Centers for Disease Control and Prevention (CDC)
Consumer Financial Protection Bureau
❷ Dept of Agriculture
Dept of Agriculture (ChooseMyPlate.gov)
Dept of Agriculture (Food Safety & Inspection Service)
Dept of Commerce
Dept of Commerce - National Weather Service/NOAA
Dept of Commerce (Exports)
❷ Dept of Commerce (NIST)
❷ Dept of Commerce (NTIA)
Dept of Commerce (Patents & Trademarks)
Dept of Commerce (Privacy Shield)
Dept of Defense
❹ Dept of Education
❷ Dept of Education (Grants & Aid)
Dept of Education (Nat Center for Ed Statistics)
Dept of Education (Student Loans)
❹ Dept of Energy
❷ Dept of Energy (Energy Star)
Dept of Health & Human Services (Medicare)
Dept of Health & Human Services (Medicare/Medicaid)
Dept of Health & Human Services (Women's Health)
❸ **Dept of Health and Human Services (Healthcare.gov)**
❷ Dept of Health and Human Services (HHS)
Dept of Homeland Security (US Customs & Imm Svcs)
Dept of Homeland Security (Customs & Border Protection)
❷ Dept of Homeland Security (DHS)
Dept of Homeland Security (DHS)
Dept of Homeland Security (ICE)
Dept of Homeland Security (US Customs & Imm Cases)
Dept of Housing and Urban Development (HUD)
❹ Dept of Interior
Dept of Interior (US Geological Survey)
❷ Dept of Interior (US Geological Survey)
Dept of Justice (Bureau of Prisons)
❸ Dept of Justice (DOJ)

❷ Dept of Labor
Dept of Labor (OSHA)
Dept of State
Dept of State (Office of Historian)
Dept of State (Online Visa Applications)
Dept of State (Travel)
Dept of Transportation
Dept of Treasury
Dept of Treasury (TreasuryDirect)
Environmental Protection Agency
Federal Aviation Administration (FAA)
❹ Federal Bureau of Investigation (FBI)
❷ **Federal Communications Commission (FCC)**
❷ Federal Deposit Insurance Corporation (FDIC)
❷ **Federal Emergency Management Agency (FEMA)** ◆
Federal Reserve System
❷ Federal Trade Commission (Consumer Info)
❷ Federal Trade Commission (Do Not Call)
❹ **Federal Trade Commission (FTC)**
❹ First Gov (USA.gov)
Food and Drug Administration (FDA)
General Services Administration (GSA)
❷ Internal Revenue Service (IRS)
❹ National Aeronautics and Space Admin (NASA)
National Highway Traffic Safety Administration
National Institutes of Health (Cancer.gov)
National Institutes of Health (MedlinePlus)
❹ National Institutes of Health (NIH)
❷ **National Oceanic and Atmospheric Administration (NOAA)**
❹ National Park Service (NPS)
❷ National Science Foundation (NSF)
Office of Personnel Management (OPM)
Office of the Federal Register
Peace Corps
Securities and Exchange Commission (SEC)
❷ Small Business Administration
❹ Social Security Administration (SSA)
US Armed Forces - Coast Guard
US Armed Forces (Air Force)

Bold – Top 50 Overall ◆ – Top score in sector ❷ ❸ ❹ ❺ ❻ ❼ – Consecutive years as Honor Roll recipient

2018 Consumer 100 – Honor Roll

85% Honor Roll – 9% Failing – 40% of “Top of Class”

- ❸ **1040.com**
- ❸ 1040NOW
- Addicting Games
- ❸ **Airbnb**
- **Amazon Payments**
- ❸ Ancestry
- Answers.com
- AOL
- Ask.fm
- ❼ Badoo.com
- BigFishGames
- Bing
- **Blogger**
- ❸ Booking.com
- ❺ Box
- ❸ CareerBuilder
- ❷ Classmates
- Craigslist
- Dailymotion
- DeviantArt
- ❸ **DocuSign**
- ❺ Dropbox
- eBay
- eHow
- ❹ eSmart (Liberty Tax)
- ❸ Expedia
- ❹ ezTaxReturn.com
- ❸ FileYourTaxes
- ❻ Fiverr
- ❹ **Flickr**
- ❸ Free Tax Return.com
- ❹ FreeTaxUSA
- ❸ Glassdoor
- ❹ **Google Drive**
- **Google Pay**
- **Google Play**
- ❸ H&R Block
- HBO Now
- Hotels.com
- Hotwire
- Hulu
- ❺ iCloud
- ID Watchdog
- ❸ Identity Guard
- IdentityForce
- IMDb
- ❸ Imgur
- ❸ Indeed
- ❻ Instagram
- JobDiagnosis.com
- ❸ KAYAK
- ❼ LinkedIn
- ❸ **Lyft**
- ❹ Match.com
- ❸ MediaFire
- ❸ Meetup
- ❸ Miniclip
- ❸ Monster
- MSN
- MySpace
- **Netflix**
- ❹ **Norton LifeLock**
- ❸ OkCupid
- OLT Online Taxes
- OneDrive
- ❸ Orbitz
- ❸ Pandora
- **PayPal** ◆
- ❻ Pinterest
- Pogo
- ❸ Priceline
- ❼ Publishers Clearing House
- ❸ **Reddit**
- Shutterfly
- Simply Hired
- ❸ **Snapchat**
- ❸ SoundCloud
- ❸ Spotify
- **Square Cash**
- ❹ TaxACT
- ❹ TaxSlayer
- **Tinder**
- Travelocity
- TripAdvisor
- ❼ Tumblr
- ❸ TurboTax
- ❼ **Twitter**
- **UpWork**
- Venmo
- Vimeo
- VRBO
- Western Union
- Wikia
- wikiHow
- Wikipedia
- ❻ Wordpress
- Xoom
- Y8
- ❺ Yahoo!
- Yelp
- ❻ **YouTube**
- Zelle
- ❸ Zoosk
- ❼ Zynga

Bold – Top 50 Overall ◆ – Top score in sector ❷ ❸ ❹ ❺ ❻ ❼ – Consecutive years as Honor Roll recipient

2018 News/Media 100 – Honor Roll

78% Honor Roll – 19% Failing – 2% of "Top of Class"

- ❸ American City Business Journals
- ❷ AOL News
- AP
- Axios
- Bankrate
- BBC.com
- Bleacher Report
- Bloomberg News
- ❷ Boston.com
- Breitbart
- ❸ Business Insider
- ❸ BuzzFeed
- Cars.com
- CBS News
- CBS Sports
- Chicago Tribune
- Chron
- CNBC
- ❷ CNET
- CNN
- Consumer Reports
- Daily Caller
- Deadspin
- Digital Trends
- ❸ Engadget
- ESPN
- ❷ Everyday Health
- ❷ Fox News
- Fox Sports
- ❸ Gizmodo
- ❺ **Google News** ◆
- ❷ Huffington Post
- ❷ Independent
- ❷ Kotaku
- Lifewire
- Live Science
- Los Angeles Times
- ❷ Mashable
- ❸ MSN News
- ❷ National Geographic
- NBC Sports
- New York Magazine
- ❺ New York Times
- Newsweek
- NJ.com
- ❷ NPR
- NY Daily News
- Patch
- PBS
- ❷ Politico
- Polygon
- ❸ **Reddit**
- Reuters
- SB Nation
- SFGate
- ❷ Slate
- ❷ TechCrunch
- ❸ The Atlantic
- ❷ The Daily Beast
- ❸ The Guardian
- The Motley Fool
- The National Weather Service
- The New York Post
- The Sun
- The Telegraph
- ❷ TMZ
- US News
- USA Today
- ❸ Vice
- ❷ Vox
- Wall Street Journal
- Washington Post
- Washington Times
- Weather Channel
- Weather Underground
- ❸ WebMD
- ❷ Wired
- ❸ Yahoo News

Bold – Top 50 Overall ◆ – Top score in sector ❷ ❸ ❹ ❺ ❻ ❼ – Consecutive years as Honor Roll recipient

2018 ISPs, Carriers & Hosters 100 – Honor Roll

63% Honor Roll – 35% Failing – 4% of “Top of Class”

❷ 1&1
A2 Hosting
Akamai Technologies
Amazon Web Services (AWS)
❷ AOL Mail
AT&T
AT&T Wireless
❷ Automattic
❷ BlueHost
❷ C Spire Wireless
Cable ONE
Comcast
Consolidated Communications
❷ Cox Communications
Cricket Wireless
CyrusOne
❷ Digital Ocean
e-vergent
Etheric Networks
Everywhere Wireless
❷ Frontier Communications
GoDaddy
❷ **Google Cloud** ◆
❷ Google Gmail
❷ HostGator
HostMonster
❷ iCloud Mail
❷ Incapsula Inc
iPage
KnownHost
❷ Linode
❷ LiquidWeb
❷ Mail.com
❷ MetroPCS
❷ Microsoft Azure
❷ Microsoft Outlook.com
❷ New Dream Network, LLC
Optimum by Altice
Peer 1 Network (USA) Inc
❷ ProtonMail
Psychz Networks
Rackspace
RCN
Rise Broadband
Shopify
❷ SingleHop
❷ SoftLayer
❷ Squarespace
Sucuri
Suddenlink Communications
TDS Telecom
TierPoint
Tutanota
❷ Verizon
❷ Verizon Wireless
WATCH Communications
❷ Weebly
Winters Broadband
WOW!
❷ Yahoo Mail
Yandex Mail
❷ Zoho Mail

Bold – Top 50 Overall   ◆ – Top score in sector   ❷ ❸ ❹ ❺ ❻ ❼ – Consecutive years as Honor Roll recipient

2018 Healthcare 100 – Honor Roll

57% Honor Roll – 43% Failing – 4% of "Top of Class"

23andMe ◆
Adventist Health System
Aetna Group
Ahoid Delhaize (Food Lion Pharmacy)
Albertsons Pharmacy
Alere, Inc.
Anthem
Any Lab Test Now
Ascension Health
Baylor Scott & White Health
BCBS of MN
BCBS of NJ GRP
CA Physician's Service (d/b/a BS of CA)
Cambria Health Solutions
Carefirst Inc. Group
Caresource Group
Cigna Health Group
Cigna Pharmacy
Costco Pharmacy
Counsyl
CVS Pharmacy
DaVita Healthcare Partners, Inc.
Dignity Health
Diplomat Pharmacy
Express Scripts
Florida Blue
Gene by Gene
HCSC Group
Health Net of California, Inc.
Highmark Group
Hospital Corporation of America (HCA)
Independence Health Group Inc. Group
Kroger Pharmacy
Laboratory Corporation of America
Mercy Health
Myriad Genetics, Inc.
Northwell Health
Pathway Genomics
PharMerica
Prime Healthcare Services
Providence Health and Services
Publix Pharmacy
Quest Diagnostics, Inc.
Rite Aid Pharmacy
SSM Health Care
Tenet Healthcare
United Health
UnitedHealth (Optum Rx)
Univera Healthcare Advantage
Universal Health Services
Unum Group
UPMC (Hospitals)
UPMC Health System Group (Insurance)
Walgreens Boots Pharmacy
Walmart Pharmacy

2018 Internet Society OTA* Members – Honor Roll

98% Honor Roll – 2% Failing – 12% of "Top of Class"

❻ ACT | The App Association
❹ ADT
❼ Agari
❷ Classmates
❼ Constant Contact
❼ DigiCert
❺ Distil Networks
❸ Dmarcian Inc.
❼ Ensighten
❹ **Gap Inc.**
❼ GetResponse
❷ Global Cyber Alliance
❷ Guardian Life
❼ High-Tech Bridge (now ImmuniWeb)
❼ Iconix
❼ Identity Guard
❸ Infoblox
❷ Intelius
❷ **Internet Society**
❼ Intersections
❹ Kromtech Alliance Corp.
❺ LashBack
❹ MacKeeper
❹ Malwarebytes
❼ Marketo
❼ Microsoft
❸ National Association of REALTORS
❹ **Norton LifeLock**
❼ **Online Trust Alliance** ◆
❺ OPTIZMO
❷ PeopleConnect
❹ PhishLabs (formerly Brand Protect)
❷ Security Scorecard
❹ Simpli.Fi
❼ Symantec
❺ The Media Trust
❼ **TrustSphere**
❼ **Twitter**
❹ UnsubCentral
❸ Valimail
❻ Verisign
❸ Yes Marketing
❸ Zeta Interactive

* Internet Society Organization Members who were previously OTA Members

Bold – Top 50 Overall ◆ – Top score in sector ❷ ❸ ❹ ❺ ❻ ❼ – Consecutive years as Honor Roll recipient

Appendix E – Best Practice Checklist

DNS, Domain, Brand & Consumer Protection		
❑	Valid SPF records & DKIM at the corporate and sub domains	Base Score
❑	DMARC records with reject/quarantine policy	Base Score
❑	Naked DMARC records (p=none and no RUA or RUF)	Invalid
❑	Opportunistic TLS for email	Bonus Points
❑	Implement DNSSEC	Bonus Points
❑	IPv6 Adoption	Bonus Points
❑	Multi-Factor Authentication	Bonus Points
❑	Domain locked	Penalty for not locking
❑	Inbound email authentication and DMARC checking	Not scored; recommended
Site, Server & Infrastructure Security		
❑	Server Security & Configuration	Base Score – aggregate, multiple tests
❑	SSL/TLS Certificate, Protocol, Key Exchange, Ciphers	Base Score – aggregate, multiple tests
❑	Always on SSL (https by default)	Base Score
❑	Server Patching Cadence	Base Score
❑	Certification Authority Authorization (CAA)	Bonus Points
❑	Certificate Type (EV SSL)	Bonus Points
❑	Web Application Firewall	Bonus Points
❑	Malware, malicious links	Penalty
❑	XSS / iFrame Vulnerability	Penalty
❑	Vulnerability / Bug Reporting Mechanism	Bonus Points
❑	Anti-Bot Protection	Not scored, recommended
❑	DDoS Mitigation Mechanisms	Not scored, recommended
Privacy Statement, Tracking, Transparency & Disclosures		
❑	Link to privacy statement on home page	Base Score
❑	Privacy statement date stamp at top of page	Base Score
❑	Layered short notice design (links/expand sections)	Base Score
❑	Children’s Online Privacy Protection Act (COPPA) or related reg’s	Base Score
❑	“Do Not Track” (DNT) disclosure	Base Score
❑	Data retention statement	Base Score
❑	Personal data not shared, except to third parties for service	Base Score
❑	Personal data not shared with affiliates/partners	Base Score
❑	Vendors contractually held to privacy statement	Base Score
❑	Archived/prior version of privacy statement available	Base Score
❑	Icons used to clearly identify sections	Bonus Points
❑	Multi-lingual statement option clearly linked	Bonus Points
❑	Honor DNT browser setting	Bonus Points
❑	Disclosure of cross-device tracking	Bonus Points
❑	Disclosure whether data shared for legal purposes	Bonus Points
❑	Notify user if personal data is requested by 3rd party	Bonus Points
❑	Tag Management System (TMS) in place	Bonus Points
❑	Presence of 3rd Party trackers that share data	Penalty, number of trackers
❑	Data breach reported	Penalty, number of incidents, size of breach
❑	FTC/FCC/CFPB/State/International enforcement action	Penalty, number of settlements
❑	Is your WHOIS record Private?	Penalty
❑	Comply with regulations in appropriate jurisdictions (e.g, GDPR)	Recommended

Appendix F – Implementation Resources

2018 Online Trust Audit https://otalliance.org/2018HonorRoll

2018 Audit Methodology https://otalliance.org/2018-online-trust-audit-methodology

Best Practices

Always on SSL https://otalliance.org/AOSSL

Certification Authority Authorization (CAA) https://cabforum.org/

DMARC https://otalliance.org/DMARC

DNSSEC https://www.internetsociety.org/deploy360/dnssec/

DNSSEC Test Tool https://dnssec-debugger.verisignlabs.com/

SSL Certificate best practices https://otalliance.org/SSL

Email Authentication https://otalliance.org/Eauth

Extended Validations SSL Certificates Brand Benefits https://otalliance.org/EVSSL

Internet Standards Scan https://internet.nl/

IPv6 https://www.internetsociety.org/deploy360/ipv6/

Malvertising https://otalliance.org/Malvertising

SPF / DMARC Record Checker https://otalliance.org/EauthTool

SSL Server Test Tool https://ota.ssllabs.com/

SSL/TLS Server Test Tools https://www.immuniweb.com/ssl/

Web Server Security Test https://www.immuniweb.com/websec/

Website Malware/Security Scanner https://sitecheck.sucuri.net/

Website Security Scan https://observatory.mozilla.org/

Transport Layer Security (TLS) for email https://otalliance.org/TLS

Vulnerability / Bug Report Form https://otalliance.org/VulnerabilityReports

Related Resources

Cyber Incident & Breach Response Readiness Guide https://otalliance.org/Incident

IoT Trust Framework https://www.internetsociety.org/iot/trust-framework

Smart Home Resources https://otalliance.org/SmartHome

Email Marketing Unsubscribe Practices https://otalliance.org/unsub

Native Advertising Transparency Audit https://otalliance.org/Native

Vision of Trust White Papers https://otalliance.org/vision-trust

Internet Society – Deploy360 Programme https://www.internetsociety.org/deploy360/

Internet Society – Global Internet Report http://www.internetsociety.org/globalinternetreport/

Acknowledgements

Data and analysis assistance has been provided in part by Agari, Disconnect, dmarcian, Google, High-Tech Bridge (now ImmuniWeb), Infoblox, Internet.nl, Microsoft, Mozilla, Open Bug Bounty, SSL Labs, Sucuri, Symantec, Twitter, Valimail and Verisign.

About the Internet Society’s Online Trust Alliance (OTA)

The Internet Society’s Online Trust Alliance (OTA) identifies and promotes security and privacy best practices that build consumer confidence in the Internet. Leading public and private organizations, vendors, researchers, and policymakers contribute to and follow OTA’s guidance to help make online transactions safer and better protect users’ data. The Internet Society is a global nonprofit dedicated to ensuring an open, globally connected, trustworthy, and secure Internet for everyone.

1604-2

Sponsored in part by

Symantec.

Norton LifeLock

Endnotes

[1] Google, Facebook fraudster pleads guilty to stealing $123 million in BEC scams https://www.scmagazine.com/home/security-news/cybercrime/google-facebook-fraudster-pleads-guilty-to-stealing-123-million-in-bec-scams/

[2] Marriott says fewer customers were affected by massive data breach https://www.usatoday.com/story/travel/news/2019/01/04/marriott-says-fewer-customers-affected-massive-data-hacking/2481601002/

[3] Facebook's privacy problems: a roundup https://www.theguardian.com/technology/2018/dec/14/facebook-privacy-problems-roundup

[4] EU General Data Protection Regulation (GDPR) https://eugdpr.org/

[5] 2018 CIGI-Ipsos Global Survey on Internet Security and Trust https://www.cigionline.org/internet-survey-2018

[6] OTA IoT Trust Framework https://www.internetsociety.org/iot/trust-framework/

[7] Online Trust Audit & Honor Roll https://otalliance.org/HonorRoll

[8] Source list from Internet Retailer® https://www.digitalcommerce360.com/product/top-500-database/. In some charts and tables, for the sake of brevity, the Internet Retailer Top 100 and Top 500 are abbreviated "IR 100" and "IR 500", respectively.

[9] Federal Deposit Insurance Corporation (FDIC) top ranked banks based on assets https://www.fdic.gov/bank/statistical/

[10] Top ranked consumer sites or edge providers based on site traffic for which the provider requires the user to subscribe or establish an account in order to use the service and are neither financial services or e-commerce focused.

[11] Internet Society organization members that were OTA members prior to the integration of OTA into the Internet Society.

[12] Data does not include results of the OTA Member sector due to their high level of achievement and would distort the chart axis.

[13] The Transport Layer Security (TLS) Protocol Version 1.3 https://tools.ietf.org/html/rfc8446

[14] Includes both electronic and physical data loss incidents

[15] Why You Need IPv6 https://www.infoblox.com/solutions/ipv6-readiness

[16] IPv6 Security https://www.internetsociety.org/deploy360/ipv6/security/

[17] DHS Binding Operational Directive 18-01 https://cyber.dhs.gov/bod/18-01/

[18] IETF RFC 4408 https://www.ietf.org/rfc/rfc4408.txt

[19] Gmail TLS for email warning https://arstechnica.com/information-technology/2016/02/gmail-to-warn-you-if-your-friends-arent-using-secure-email/

[20] ICANN DNSSEC Report http://stats.research.icann.org/dns/tld_report/

[21] M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 2008 https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2008/m08-23.pdf

[22] IPv6 adoption http://www.worldipv6launch.org/measurements/

[23] What is Credential Stuffing? https://www.wired.com/story/what-is-credential-stuffing/

[24] Hackers Are Passing Around a Megaleak of 2.2 Billion Records https://www.wired.com/story/collection-leak-usernames-passwords-billions/

[25] ImmuniWeb SSL Test https://www.immuniweb.com/ssl/

[26] Qualys SSL Labs https://www.ssllabs.com/projects/documentation/

[27] DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) https://drownattack.com/

[28] ImmuniWeb Website Security Test https://www.immuniweb.com/websec/

[29] Observatory by Mozilla https://observatory.mozilla.org/

[30] Sucuri SiteCheck https://sitecheck.sucuri.net/

[31] CAA Overview https://blog.qualys.com/ssllabs/2017/03/13/caa-mandated-by-cabrowser-forum

[32] OTA Advertising & Content Integrity https://otalliance.org/resources/advertising-integrity-fraud

[33] Qualys SSL Labs SSL Pulse Report https://www.ssllabs.com/ssl-pulse/

[34] Deprecating early TLS https://www.ssl.com/article/deprecating-early-tls/

[35] Open Bug Bounty https://www.openbugbounty.org/report/

[36] Let's Encrypt https://letsencrypt.org/

[37] CA Security Council 2019 Predictions http://vmblog.com/archive/2019/01/10/ca-security-council-2019-predictions-the-good-the-bad-and-the-ugly.aspx

[38] Half of All Phishing Sites Now Have the Padlock https://krebsonsecurity.com/2018/11/half-of-all-phishing-sites-now-have-the-padlock/

[39] IRS eFile Security & Privacy Standards Mandate published January 1, 2010 https://www.irs.gov/uac/irs-e-file-security-privacy-and-business-standards-mandated-as-of-january-1-2010

[40] Extended Validation Certificates are Dead https://www.troyhunt.com/extended-validation-certificates-are-dead/

[41] Note that approximately 30% of the sites in 2018 are new to the Audit, making precise year-to-year comparison difficult.

[42] Kaspersky Labs DDoS Attacks Q4 2018, https://securelist.com/ddos-attacks-in-q4-2018/89565/

[43] OTA Vulnerability Reporting Form https://otalliance.org/VulnerabilityReports

[44] Malicious code hidden in advert images cost ad networks $1.13bn https://www.zdnet.com/article/malicious-code-hidden-in-advert-images-cost-ad-networks-1-13bn-last-year/

[45] Amazon sues over malicious ads https://www.geekwire.com/2018/amazon-files-suit-malvertising-campaign-alleging-sophisticated-widespread-scheme-deceive-consumers/

[46] APEC Cross-Border Privacy Rules http://www.cbprs.org/

[47] California Consumer Privacy Act https://en.wikipedia.org/wiki/California_Consumer_Privacy_Act

[48] COPPA https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

[49] Note while the presence of such solutions was verified, it is possible sites may not use the solutions or data.

[50] Apple is Removing "Do Not Track" From Safari https://gizmodo.com/apple-is-removing-do-not-track-from-safari-1832400768

[51] Tracking Preference Extension (DNT) https://www.w3.org/TR/tracking-dnt/

[52] OTA 2018 Cyber Incident & Breach Trends Report https://otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf

[53] Call for comments press release https://otalliance.org/news-events/press-releases/ota-requests-public-comments-2018-online-trust-audit-methodology

[54] Internet Society Deploy360 Programme https://www.internetsociety.org/deploy360/

[55] August 23, 2018 methodology press release https://otalliance.org/news-events/press-releases/internet-society%E2%80%99s-online-trust-alliance-announces-methodology-tenth

[56] Verizon Data Breach Investigations Report, page 11 https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

[57] Business Email Compromise the $12 Billion Scam https://www.ic3.gov/media/2018/180712.aspx

[58] OTA email authentication overview, resources and tools https://otalliance.org/eauth

[59] OTA overview of DMARC and resoruceshttps://otalliance.org/DMARC

[60] SSL/TLS security and deployment best practices https://otalliance.org/resources/ssl-best-practices

[61] DNSSEC Basics https://www.internetsociety.org/deploy360/dnssec/basics/

[62] IPv6 https://www.internetsociety.org/deploy360/ipv6/

[63] Qualys SSL Labshttps://ota.ssllabs.com/

[64] ImmuniWeb https://www.immuniweb.com/ssl/

[65] AOSSL https://otalliance.org/AOSSL

[66] EV SSL https://otalliance.org/resources/extended-validation-certificates-evssl

[67] NTIA Vulnerability Reporting Guidelines and practices https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities

[68] OTA Vulnerability Reporting Form https://otalliance.org/VulnerabilityReports

[69] FIPPS https://cryptome.org/2014/11/nstic-fipps.pdf

[70] COPPA https://www.ftc.gov/tips-advice/business-center/privacy-and-security/children's-privacy

[71] Third party tracking data – Primary source includes data from https://disconnect.me/trackerprotection/blocked netting out https://disconnect.me/trackerprotection/unblocked

[72] FTC Cross Device Tracking Recommendations https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf

[73] CFPB https://www.consumerfinance.gov/