2016 IRS Free e-File Audit & Honor Roll

Analysis of the adoption of best practices in:

- Consumer Protection
- Site, Service & Infrastructure Security
- Responsible Privacy Practices & Transparency

OTA
Online Trust Alliance

Released February 24, 2016

THE ONLINE TRUST ALLIANCE (OTA)

The Online Trust Alliance (OTA) is a 501c3 charitable non-profit with the mission to enhance online trust and user empowerment while promoting innovation and the vitality of the Internet. Its goal is to help educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity.

OTA supports collaborative public-private partnerships, benchmark reporting, and meaningful self-regulation and data stewardship. Its sponsors and supporters include leaders spanning public policy, consumer protection, technology, e-commerce, social networking, mobile, email and interactive marketing, financial services, government, NGOs and industry organization.

OTA is supported by grants, donations and annual corporate pledges and support across multiple industries, representing the private and public sectors. To learn how you can support OTA visit https://otalliance.org.

UNDERWRITTEN IN PART BY GRANTS AND DONATIONS FROM:

AGARI	Agari builds disruptive, data-driven security solutions that eliminate email as a channel for cyberattacks and enable businesses and consumers to interact safely, leading a growing coalition of security partners to help fix email for good. The Agari solution analyzes over 10 billion messages per day, helping global brands protect their enterprise, partners and customers from advanced phishing attacks. https://agari.com
digicert®	DigiCert is a premier provider of enterprise security solutions with an emphasis on authentication and encryption via managed PKI and high-assurance digital certificates for the web and the Internet of Things. DigiCert helps its customers enable scalable, trustworthy and reliable identity management and encryption for web servers, smart devices, industrial systems, manufacturing and healthcare. https://digicert.com
Symantec.™	Symantec Corporation is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives. https://symantec.com

This Audit has been powered in part by tools, resources and data provided by leading organizations and OTA member companies including: Agari, AVG Technologies, DigiCert, Disconnect, Distil Networks, Ensighten, High-Tech Bridge SA, IID, Microsoft, Return Path, SiteLock, Symantec, SSL Labs and Verisign.

TABLE OF CONTENTS

INTRODUCTION

According to the IRS, more than 120 million returns are expected to be filed electronically in 2016.[1] As taxpayers engage in the annual filing of tax returns, cybercriminals are already prepared and ready to help. The income filing tax season is like Christmas for cyber thieves, ripe for reaping millions of dollars from unsuspecting victims. Tax scams are on the rise in both sheer numbers and in sophistication. Recognizing the financial opportunity, criminals are increasingly penetrating IRS systems, targeting e-file service providers and harming consumers through bank account take-overs, identity theft, ransomware and compromising completed returns to redirect tax refunds.

Criminals are increasingly successful in compromising users' identities and bank accounts while violating the privacy of the American people. In the first 11 months of 2015, the IRS reports it blocked $8 billion in individual fraudulent tax returns. What we do not know is how much was not blocked. Rising numbers of bogus or fraudulent tax filing sites are being set up using off-shore accounts with the explicit goal of capturing personal data and redirecting tax refunds. In some cases, these sites pass an individual's actual 1040 return to the IRS, but simply change the bank routing information to intercept refunds. While the consumer receives what appears to be a confirmation that their return was filed and is being processed, they are unaware of the damage being initiated.

Other common exploits include IRS impersonation telephone calls and emails that tell taxpayers to update their records in order for their returns to be processed.[2] Most recently, malicious and bogus ads purporting to be from legitimate e-file companies are being served on reputable websites, driving malicious downloads and key loggers resulting in additional identity theft. While the user visits trusted websites the malware can be automatically downloaded to their device. According to research, over 400 fraudulent tax related domains were registered between January 15 and February 14, 2016. Of these, 260 were "IRS branded" and the balance targeted e-file tax preparation services.[3]

Compounding the threat landscape is the growing sophistication of tax related scams that target tax and legal professionals, including Business Email Compromise Emails (BEC), which is also known as "CEO Fraud." Moving from crimes of opportunity to micro-targeting, these attacks use socially engineered emails to capture log on credentials, allowing criminals to breach systems and associated client data.[4]

The IRS also continues to be a target. In early 2016, the IRS reported it identified unauthorized attempts to obtain e-file PINs for 464,000 Social Security numbers, of which 101,000 were successful.[5] This breach follows a 2015 incident where criminals successfully obtained personal information and previous year tax returns from more than 300,000 taxpayers by exploiting the IRS "Get Transcript" database.[6] [7]

[1] https://www.irs.gov/uac/Newsroom/2016-Tax-Season-Opens-Jan-19-for-Nations-Taxpayers

[2] IRS Tax Scams / Consumer Alerts https://www.irs.gov/uac/Tax-Scams-Consumer-Alerts

[3] Gary Warner, Cyber Researcher, University of Alabama http://garwarner.blogspot.com/

[4] FBI BEC http://www.ic3.gov/media/2015/150122.aspx

[5] WSJ Hackers Breach IRS February 9 http://www.wsj.com/articles/identity-thieves-breached-irs-computer-systems-agency-says-1455066304?mod=trending_now_7

[6] IRS "Get Transcript" database http://www.wsj.com/articles/irs-says-cyberattacks-more-extensive-than-previously-reported-1439834639

[7] IRS Get Transcript database May 26, 2015, press release https://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application

To help lower-income taxpayers obtain free tax preparation and e-filing services, the U.S. Internal Revenue Service (IRS) has entered into a contractual agreement with 13 software developers that requires them to offer free tax preparation and e-filing for filers with an adjusted gross income of $62,000 or less.[8] These for-profit companies are part of the Free File Alliance, a nonprofit coalition of industry-leading tax software companies who have partnered with the IRS to help millions of Americans prepare and e-file their federal tax returns for free. [9] [10]

Addressing the rising tide of fraudulent tax preparation sites, many of which have targeted the approved e-file sites, in 2009 the IRS established a set of minimal security requirements and standards for these service providers.[11] These measures were designed with industry input to help delineate legitimate sites from fraudulent ones while addressing security and privacy fundamentals.[12]

ASSESSING RISK & COMPLIANCE

In response to threat intelligence, inquiries and reports of possible e-file site insecurity, in early February 2016, OTA commissioned an audit of the 13 listed free file e-file tax sites for compliance against auditing methodology developed by the Online Trust Alliance. While there are hundreds of other e-file tax sites and service providers, for the purpose of this research and Audit the term "e-file" or "e-file sites" refers only to the 13 free e-file sites listed on the IRS site. The core audit criteria map to other recently audited segments including the 2016 Presidential Candidates[13], Top 100 FDIC insured banks, Top 500 ecommerce sites and other segments included in OTA's annual Online Trust Audit and Honor Roll.[14] In addition this study also tested for compliance to several of the IRS e-file security standards.

OTA has deep expertise in such audits, leveraging test tools and industry resources developed over the past seven years. Since 2009, the Online Trust Audit has conducted audits of leading consumer-facing web sites and applications, providing a benchmark review of businesses' and government's commitment to security, privacy and consumer protection best practices. As the cyber threat increases and privacy concerns heighten, the relevance and timeliness of this report is significant, underscoring the imperative that data security, protection and privacy need to be integrated into every service, business process, website and mobile application. Criteria are updated annually through a multi-stakeholder process and public call for comments, reflecting the threat landscape, security standards and privacy practices.[15]

[8] Free File Software Offers, https://apps.irs.gov/app/freeFile/jsp/index.jsp?ck

[9] About the Free File Alliance https://www.irs.gov/uac/About-the-Free-File-Alliance

[10] In addition the IRS also provides a list of authorized e-file providers for individuals who provide services on a fee basis. https://www.irs.gov/uac/Authorized-IRS-e-file-Providers-for-Individuals

[11] IRS e-file Security & Privacy Standards https://www.irs.gov/uac/IRS-e-file-Security-Privacy-and-Business-Standards-Mandated-as-of-January-1-2010 1) Use of EV-SSL (Extended Validation Secure Sockets Layer), certificates, providing validation of the site owner through a visual trust indicator in the browser, 2) File all user tax management URLs with the IRS, 3) Contract with a PCI-certified vulnerability scanning service to scan the service periodically, 4) Create and publish a privacy policy and information safeguard policies, 5) Obtain a privacy seal from an IRS-approved service, 6) Implement a challenge-response like a CAPTCHA for filing, 7) No use of private domain name registration and 8) Report all security incidents.

[12] New IRS e-File Security & Privacy Standards FAQs https://www.irs.gov/uac/New--IRS-e-file-Security-and-Privacy-Standards-FAQs (*updated April 2015*).

[13] OTA Audit of Top Presidential Candidates http://otalliance.org/2016candidates

[14] OTA Online Trust Audit https://otalliance.org/HonorRoll

[15] OTA Audit Methodology https://otalliance.org/initiatives/2015-honor-roll-methodology

Testing was initiated February 2 and ran through February 18, 2016. As compliance concerns and site vulnerabilities were observed, OTA shared a draft of the report with the IRS. OTA staff offered assistance and detailed briefings, raising the importance of oversight and compliance testing of the free e-file firms they reference as well as all authorized e-file providers. As of February 21, the IRS has not responded to OTA's offer of assistance or to discuss these findings.

Consistent with past annual methodology updates, the 2016 SSL scoring tools have been revised to reflect compliance with current standards and protocols, while placing increased weight on exposure to known vulnerabilities and risks. In addition, the methodology has been updated in two other areas reflecting current SSL standards and global privacy landscape.

First, sites with security scores of C or lower are automatically considered failing the security category, thereby failing the overall audit. Second, as the Do Not Track (DNT) standard has evolved through the W3C standards process, disclosure of honoring or not honoring browser-based DNT settings has now been integrated into the core privacy score. Sites which fail to disclose whether they honor such user settings lose points as part of the core privacy policy assessment.[16]

This research did not evaluate the marketing practices of the sites nor the definition of "free", though OTA researchers observed a wide range of fee services tied to free filing. According to data reported by the IRS and analyzed by the OTA approximately 70% of taxpayers qualify for Free File and less than 3% haven taken advantage of it. This low usage indicates there may be significant barriers to usage, low awareness and/or discoverability of the program. Consumers are encouraged to evaluate the free e-file offerings as many have added fees for features such as error checking, which the typical consumer should consider in order to submit a tax return with confidence.

The OTA e-file Honor Roll Audit and report serves the following objectives:

- Promote best practices and provide tools and resources to assist the public and private sectors to help enhance their security, data protection and privacy practices.
- Recognize leadership among e-file firms and their respective commitment to best practices which aid in the protection of online trust and confidence in online services.
- Assist consumers in making informed decisions about the security and privacy practices of sites they frequent.
- Aid consumers in fighting identity theft and IRS related fraud.
- Provide assistance to the IRS and other organizations on how to develop continuous monitoring of third-party services.
- Evaluate e-file firms' compliance to the IRS security standard mandate.

[16] It is the opinion of OTA that pointing to the existing self-regulatory solutions such as those serving industry trade groups does not address the core consumer issues of data collection and usage and intent of the DNT standard.

EXECUTIVE SUMMARY

The privacy and data security landscape is rapidly evolving with new threat vectors emerging daily. In the tax filing arena, attacks are happening at the IRS, via bogus sites and via fraudulent returns. Consumers and businesses need to safeguard themselves as much as possible to navigate these services safely.

On the whole, e-file sites scored well with 54% achieving Honor Roll status, but there are concerning undercurrents – six failed in either Consumer Protection (lack of email authentication, opening consumers up to fake emails purporting to be from their sites) or Site Security (exposing data via weak ciphers or protocols). The overall Privacy scores were strong but sites had more third-party sharing than expected.

All of these issues can easily be addressed and underscore that e-file firms (and all organizations) should adopt an operational security and privacy discipline. As reported in the OTA's 2016 Data Protection and Breach Readiness Guide, 92% of publically reported breaches in 2015 could have been prevented – these findings highlight the risk to e-file services and the urgency of addressing shortcomings immediately.

OTA encourages all e-file sites to examine their practices against the list of criteria audited and address the gaps to raise their scores across all categories. Of critical importance is implementing comprehensive email authentication (SPF and DKIM) for all domains and subdomains along with publishing DMARC "reject" policies to help prevent spoofed messages from reaching consumers and business users. Because the volume of fraudulent email traffic is on the rise, along with the use of look-a-like domains infringing on IRS and e-file services providers, failure to protect these domains from abuse places consumers at unnecessary risk.

Implementing the latest protocols and ciphers on websites along with "Always On SSL" will ensure the best possible security environment for site visitors. It is alarming that three of the sites tested are failing security basics, leaving their sites and users exposed to risks which have been documented for as much as two years. Fortunately these issues can be addressed quickly, but highlight the need for continuous monitoring of systems and infrastructure.

Privacy, user control of their online behavior tracking, as well as control on the use and sharing of users' data is a global issue. While it is understood that many sites rely on affiliate marketing and re-targeting, considering the sensitivity of the data, the typical consumer would likely be surprised by the sites' data collection and sharing activities. Restricting data sharing and honoring Do Not Track are key issues to be addressed. Overall, implementation of these practices will further protect consumers' data and privacy and reduce the likelihood of fraudulent returns and identity theft.

As an aid to consumers and businesses, this report includes practical tips for businesses and consumers to help protect themselves from being victims in the area of cyber tax fraud. The remaining sections detail the methodology and examine each major audit category in detail, including adoption rates of key criteria, comparison to other sectors, and insights, observations and recommendations for the e-file sites. While outside the scope of this research, consumers should closely evaluate free offers of any service provider. In addition, based on limited sampling of authorized e-file providers that are not part of the free file program, additional oversight is also recommended for their respective security and privacy practices.

Updates may be found at https://otalliance.org/TaxFraud.

E-FILE SITES AUDIT HIGHLIGHTS

OTA believes a strong commitment to data stewardship and meaningful self-regulation mutually benefits consumers and organizations in all sectors. We have been impressed with the increased engagement over the years of many types of organizations, along with public support from hundreds of entities, ranging from consumer-facing sites to technology providers. This Audit examines three main categories:

- Consumer Protection – protection of email via authentication and encryption between servers, and protection of domains from hijacking
- Site Security – server security, use of encryption for web sessions, protections such as firewalls and potential site vulnerabilities
- Privacy – data sharing, retention, notice and third-party restriction policies in the privacy policy, as well as analysis of third-party tracking on the site

Each of the three categories is worth 100 baseline points. In addition, bonus points can be earned for emerging best practices in each of the categories. To qualify for the Honor Roll, sites must achieve a combined score of 80% or higher, yet not fail (score less than 55) in any single category.

The results of the 2016 e-file Sites Audit are shown in Figure 1 below – 54% (seven) of the 13 sites made the Honor Roll (overall achievement of 80% or higher) while 46% failed. There was no middle ground, all sites either made the Honor Roll or received a failing grade in one or more categories.

E-FILE FREE TAX FILING SERVICES
ONLINE AUDIT RESULTS

Honor Roll	Failed
eSmart Tax	1040.com
ezTaxReturn.com	1040Now.net
FreeTaxUSA	FileYourTaxes.com
H&R Block Free File	Free1040TaxReturn.com
TaxAct	Jackson Hewitt Online
TaxSlayer	Online Taxes at OLT.com
TurboTax Free File	

Figure 1 – 2016 e-file Sites Audit Results. For the links to the free tax file sites audited, visit http://irs.gov/freefile

COMPARISON OF E-FILE SITES TO OTHER SECTORS

Given the prevalence of fraud, IRS security and privacy mandates and the sensitivity of data handled in this sector, OTA expected to find strong adoption of the best practices advocated in the Audit. As seen in Figure 2, the 54% Honor Roll achievement for e-file sites is higher than all but the social sector evaluated in 2015 (the average achievement across other sectors was 44%). The failure rate of 46%, shown in Figure 3, is equal to the overall average across all sectors but is disappointing given the nature of e-file sites' business and should be concerning for potential customers of these services. In addition it suggests added oversight, such as quarterly reviews and assessments, should be required for companies that participate in the Free File Alliance or qualify to be an authorized e-file provider.

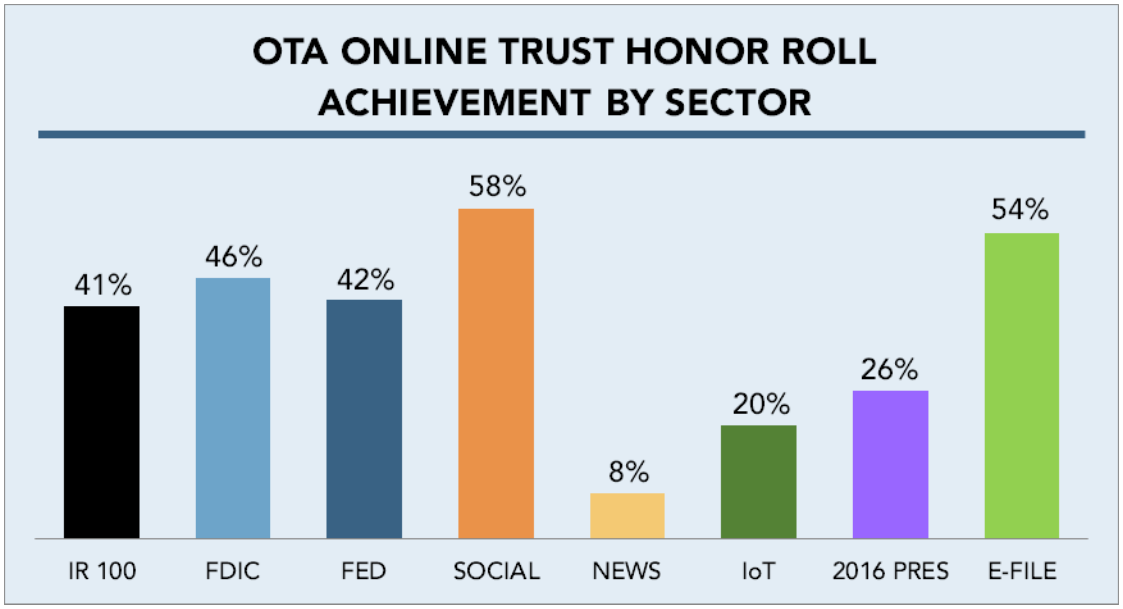


Figure 2 – Honor Roll Achievement by Sector

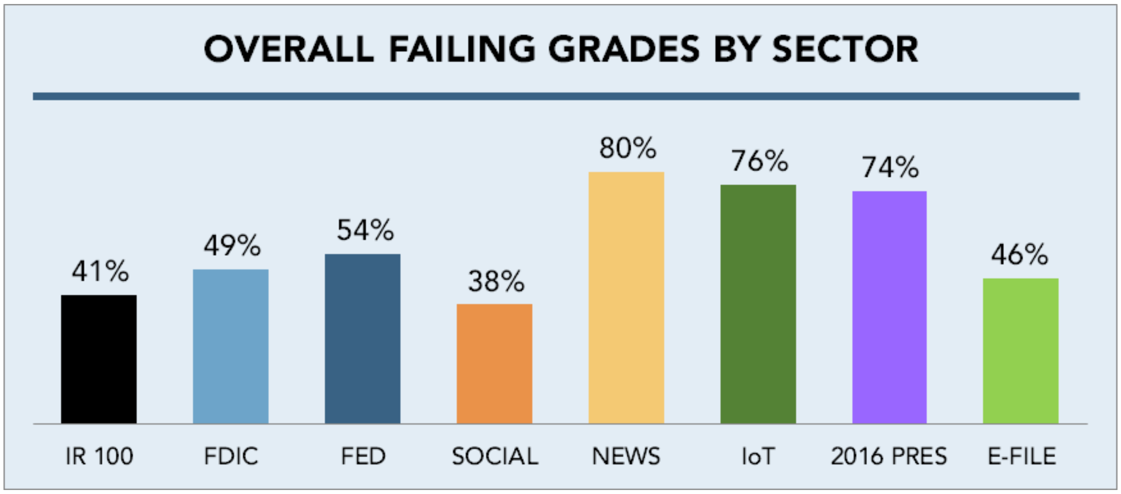


Figure 3 – Percent of Organizations with Failing Grade by Sector

While not all e-file sites may be able to achieve Honor Roll status, the fact that there is no middle ground is surprising, especially for services dealing with the most sensitive consumer data – so why the higher than expected failure rate?

FAILURE RATES

To answer this question, it is useful to look further inside the data. Figure 4 shows failure rates within each of the three main categories audited. While these 13 e-file sites performed well in Privacy (the only sector with no failures), they had a higher than average failure rate in Consumer Protection and the highest failure rate in Site Security by nearly 2:1. It is important to note that sites can fail in more than one category – in this case five sites failed in Consumer Protection and three sites failed in Site Security. The steps required to address these failures are straightforward and are discussed in later sections.

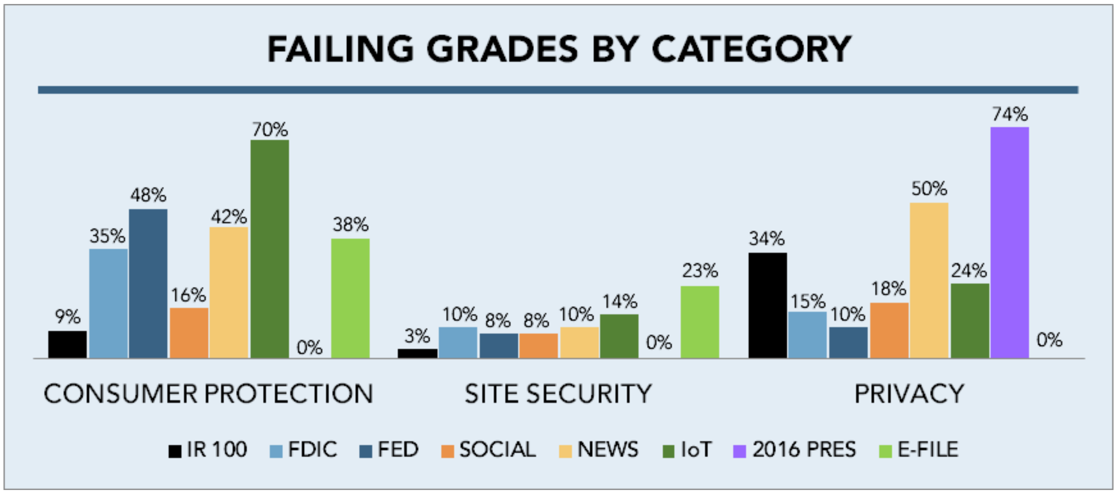


Figure 4 – Percent of Companies with Failing Grade by Sector and Category

AVERAGE BASELINE SCORES

Figure 5 below shows the average baseline score (out of 100) in each main category by sector. Again, e-file sites have a strong overall Privacy score (81), the second highest of all sectors audited. The Consumer Protection score of 54 was tied for second lowest (only IoT was lower), showing that support for email authentication needs to be improved significantly. In the Site Security area, e-file sites were second lowest with an average score of 82, but this average obscures the underlying fact that three sites had failing scores (less than 55), which is concerning.

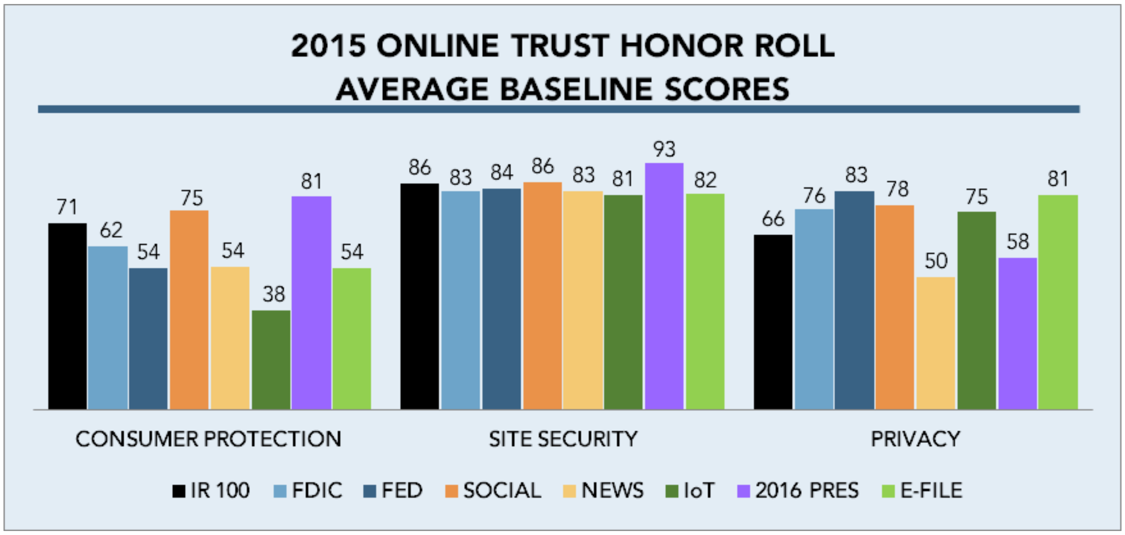


Figure 5 – Major Category Scores by Sector

CONSUMER PROTECTION FINDINGS

This category scores the adoption of email authentication and associated technologies to help protect consumers from receiving fraudulent email purporting to come from e-file sites. As outlined in the Introduction, the increase in the volume and sophistication of email purporting to come from e-file services underscores the importance of authenticating all email streams and associated domains.

The key email authentication protocols broadly accepted by the public and private sectors include Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), which allow recipients to verify the sender. In addition, Domain-Based Authentication, Reporting and Conformance (DMARC) allows senders to receive feedback on their authentication status and instruct ISPs and mail systems to reject or quarantine forged email. Finally, opportunistic Transport Layer Security (TLS) encrypts sessions between mail servers to prevent fraud and eavesdropping.

Testing was initiated by creating accounts and signing up for newsletters from each e-file provider. Email headers, server connections and DNS from each provider were analyzed. Adoption of email authentication was bimodal – four sites had no email authentication at all, leaving them wide open to be spoofed, while the remaining eight supported both SPF and DKIM, though not always at the "top-level" (primary) domain, which kept scores for some sites from being even higher. In fact, one site, though supporting both SPF and DKIM, still failed since the top-level domain is left completely unprotected, playing into the hand of cybercriminals who typically forge the most recognizable domains.

Support for DMARC is 39%, the highest of all but social sites, though only one site has asserted a policy instructing receiving networks, ISPs and email providers to quarantine or reject messages that fail authentication. Improvement needs to be made in the use of opportunistic TLS to protect messages in transit since at only 31%, e-file sites are in the bottom half of sectors audited. Finally, one site did not lock its domain, a simple step that protects it from being hijacked, allowing criminals to redirect unsuspecting consumers to phishing and fraudulent web sites.

SITE SECURITY FINDINGS

This category scores the implementation of server security, data encryption for website sessions as well as other site protections and discovery of known site vulnerabilities. Overall scores for e-file sites were near the bottom of all sectors, driven by failures of three sites (the highest failure rate of all sectors).

Failures were caused by simple server misconfigurations, either supporting old, vulnerable standards (e.g., RC4, SHA1) or by not supporting current, more secure protocols (e.g., TLS 1.2). These configurations are simple and straightforward to change in a manner of minutes and stress the need for sites to regularly monitor and update their configurations.

As expected (because it is mandated by the IRS for free e-file sites), adoption of Extended Validation (EV) SSL certificates is the highest of all sectors at 92%. EV SSL certificates help website visitors know they're on the right site via a trust indicator, helping to distinguish them from fraudulent web sites. One site was not supporting an EV SSL certificate at the time of the audit, therefore was out of compliance with the IRS security mandate. Of additional concern is the fact that this site is using a Domain Validated (DV) SSL certificate, which is prone to abuse. It is generally accepted that DV certificates should not be used by any site collecting sensitive or personal information.

The missed security opportunity is adoption of "Always On SSL", which fully encrypts all traffic between the client devices and the server, thereby maximizing protection from snooping by fraudulent businesses and cybercriminals. Adoption was 54%, well above the overall average and lower than only banks and 2016 presidential candidates. Still, given the sensitivity of data handled by e-file sites, this adoption rate should be much higher. The other area of note was lack of use of web application firewalls, which at 8% adoption (one site) was the lowest of all sectors and far below the overall average of 35%.

PRIVACY FINDINGS

The 100-point baseline score for privacy is divided equally into 50 points for the content of the *privacy policy* (data sharing, data retention, notice of data sharing, Do Not Track disclosure and binding of third-party vendors' use of data) and 50 points for *third-party tracking* on the site (fewer trackers is better, and points are deducted for third-parties with loose data sharing practices). Since the IRS requires strong privacy policies and presence of a third-party privacy seal, scores were expected to be high in this area.

The average e-file site score for the privacy policy portion was 35 out of 50, tied for the highest score of all sectors audited. The average e-file site score for third-party tracking was 46 out of 50, among the top scores. The combined privacy score was 81, the second highest of all sectors (banks scored an 82). Still, there were some concerning practices, especially considering the nature of the sites and the associated information collected. While these sites do not rely on advertising, OTA was surprised to observe user data being shared with third parties for re-targeting and affiliate marketing purposes, which appeared to focus on tax services, tax software, credit reports, credit consulting and identity theft monitoring services. While the number of such third parties observed on each site was low in comparison to content-driven and ad funded sites, the "free" e-file sites may be funded in part by this data and the findings suggest a need for further oversight.

ASSESSMENT AGAINST IRS MANDATE

As mentioned in the Introduction, the IRS has specified a set of standards for e-file sites to follow. Figure 6 summarizes the adoption of these elements. As expected, use public domain registration has 100% adoption, while adoption of EV SSL certificates is 92% (one site failed to implement it) and use of an IRS-approved privacy seal is also 92% (one site uses a non-IRS approved privacy seal). The findings indicate these sites are out of compliance with IRS security mandates and their approved status should possibly be reassessed.

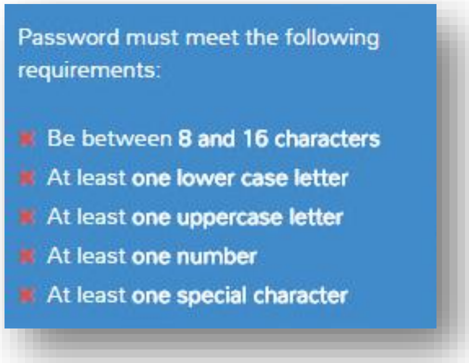
- Use of EV-SSL (Extended Validation Secure Sockets Layer) certificates, providing validation of the site owner through a visual trust indicator in the browser,
- Obtain a privacy seal from an IRS-approved service,
- Implement a challenge-response like a CAPTCHA for filing, and
- No use of private domain name registration.

ADOPTION OF IRS MANDATES	
EV SSL	92%
Challenge/Response for Filing*	38%
Privacy Seal	92%
Public Domain Registration	100%

*Tested for account setup/login, not all the way to filing

Figure 6 – Adoption Rate of IRS Mandates

The challenge/response requirement is meant to prevent automatic bot-driven submission of returns. OTA tested this element by setting up accounts at all 13 e-file sites – five supported some kind of challenge/response (e.g., CAPTCHA or code sent via text/email) as part of the account setup process, while the remaining eight had no such protection. The analysis did not go to the extent of filing returns to determine whether a challenge/response was required, but for an extra layer of safety OTA recommends the CAPTCHA be required at account setup as observed in five of the sites.


Password must meet the following requirements:

✗ Be between **8 and 16 characters**
✗ At least **one lower case letter**
✗ At least **one uppercase letter**
✗ At least **one number**
✗ At least **one special character**

Another area of note common to all e-file sites was the requirement for strong passwords as shown in the graphic to the right. All sites presented the requirement in a similar way and most tracked adherence to the requirement as a password was created, making it easy for a user to know their status during the process. Though it is nice to see this consistency, OTA recommends requiring multi-factor authentication as currently recommended by the White House.[17] This issue has less to do with the strength of a password, but more about reuse of passwords by consumers. Once a given username/password pairing is compromised, damages can quickly accelerate to that user's other accounts.

[17] https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

CONSUMER PROTECTION

By utilizing the email authentication standards Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM), organizations can help protect their brand 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, Domain-based Message Authentication, Reporting, and Conformance (DMARC) adds a policy assertion providing receivers direction on how to handle messages that fail authentication. TLS provides a means to encrypt messages between mail servers, protecting both the sender and consumer. Domain locking ensures that domain ownership cannot be transferred without the owner's permission, further helping to protect a site's brand from abuse. Domain Name System Security Extension (DNSSEC) adds security and integrity to the DNS lookup, helping to prevent "Man-in-the-Middle" (MitM) attacks, cache poisoning and DNS attacks.

RECOMMENDED BEST PRACTICES

- Implement both SPF and DKIM for top-level domains (most recognizable to the recipient / consumer), "parked" domains (not used) and any major subdomains seen on websites or used for email, including those managed by third-party email service providers.
- Implement DMARC for all appropriate domains, initially in "monitor" mode to get receiver feedback and verify accuracy of email authentication, and eventually to assert a "reject" or "quarantine" policy to receivers.
- Implement inbound email authentication and DMARC support to protect employees as well as organizational data from spear phishing exploits.
- Implement opportunistic TLS to help protect and enhance the privacy of email in transit between mail servers.
- Ensure that domains are locked to prevent unauthorized domain takeovers.
- Implement DNSSEC to further protect a site's DNS infrastructure from attack and exploits, including man-in-the middle exploits, as mandated for all government agencies by the White House in 2008.

E-FILE SITES RESULTS

As seen in Figure 5, e-file sites tied for the second lowest score among all sectors in the baseline scoring for this category. As noted in the Highlights section, the results were bimodal – four sites had no authentication at all, which means their domains can be easily abused by phishers, and one site had no protection of the top-level domain, which leaves it exposed to abuse. The eight sites with passing scores all supported both SPF and DKIM, though not always at the top-level domain. Specific results for each of the best practice recommendations were as follows. For detailed comparisons by sector, see Figure 7 below.

- **SPF and DKIM –** Adoption of the recommended best practice of using both SPF and DKIM was 62%, placing e-file sites in the middle of the pack. Use of SPF at the top-level domain (the domain of the website) was next to lowest (62%) while use of DKIM at the top-level domain was in the upper half (38%). The primary concern is four sites that have not adopted any forms of email authentication – this should be addressed immediately. Sites need to implement SPF and DKIM for all top-level domains, subdomains as well as "parked" domains.

- **DMARC –** This area was somewhat encouraging – 38% of e-file sites have a DMARC record, placing them just behind social sites (48%) – but there is still much room for improvement. Only one of the five sites supporting DMARC uses a policy assertion ("Quarantine" in this case). Given the straightforward nature of these sites and the ease of implementing DMARC (a simple text record in the DNS), there is no reason they all should not support DMARC and be able to move quickly to a "Reject" policy, allowing receiving systems to discard spoof messages and protect consumers.

- **Opportunistic TLS –** 31% of e-file sites support this, placing them in lower half of the pack. The industry is moving quickly to broad use of TLS, driven by Google and other large mailbox providers, and there is no reason e-file sites shouldn't be able to follow suit quickly.

- **Domain Locking –** All but one (92%) have locked their domain. This is a simple issue that should be addressed immediately to help prevent unauthorized domain transfer.

- **DNSSEC –** No e-file sites have implemented DNSSEC. Though adoption in non-government sectors is low (0-4%), OMB has issued a mandate for all Federal Government sites to implement it and if viewed as an extension of IRS services, e-file sites should consider moving in this direction as well.

2015/2016 AUDIT RESULTS BY SECTOR
CONSUMER PROTECTION ADOPTION

	IR100	FDIC	FED	SOCIAL	NEWS	IoT	2016 PRES	E-FILE
SPF (any)	94%	87%	80%	92%	80%	62%	100%	69%
SPF (TLD)	85%	73%	70%	92%	62%	52%	91%	62%
DKIM (any)	93%	68%	50%	78%	64%	30%	100%	62%
DKIM (TLD)	31%	30%	28%	56%	16%	14%	78%	38%
SPF and DKIM	90%	63%	48%	76%	56%	30%	100%	62%
DMARC Record	20%	24%	14%	48%	10%	2%	4%	38%
DMARC (R or Q)*	15%	21%	14%	58%	20%	0%	0%	20%
TLS	42%	38%	38%	36%	14%	24%	57%	31%
DNSSEC	0%	1%	90%	0%	4%	4%	0%	0%
Domain Lock	100%	97%	100%	94%	92%	88%	96%	92%

* Based on organizations with a DMARC record

Figure 7 – Adoption Rate of Consumer Protection Criteria by Sector

SITE, SERVER & INFRASTRUCTURE SECURITY

A site's trustworthiness is largely defined by the security of the infrastructure. Users need assurance that the site and their data are secure. Proper implementation of best practices in this category also protects the site itself from attack.

RECOMMENDED BEST PRACTICES

Best practices in this category can be summarized as follows:

- Optimize server SSL implementation using information gleaned from tools such as Qualys SSL Labs and High-Tech Bridge SA,[18] with specific focus on vulnerabilities that earn a letter grade of "C" or below.
- Use EV SSL certificates for domains and sites.
- Implement AOSSL or HTTPS on all pages to maximize data security and online privacy.
- 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 and third-party content for malicious links, cross-site scripting, iFrame exploits, malware and malvertising.[19]
- 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.
- Establish mechanisms and processes for responding to third-party reporting of site and service vulnerabilities.

E-FILE SITES RESULTS

As illustrated in the middle set of bars in Figure 5, e-file sites had the second lowest score of all sectors in the baseline scoring for this category. This was largely due to three failing sites – the non-failing sites had an average score of 90, which would place them near the top of all sectors.

Specific results for each of the best practice recommendations were as follows. For detailed comparisons by sector, see Figure 8 below.

- **Optimized SSL/TLS –** As noted, scoring within this area was bimodal, with three failing sites and the remainder averaging a score of 90. Failures were due to support of protocols or ciphers with long-known vulnerabilities (e.g., RC4, SHA1) or lack of support for recent, more secure protocols (e.g., TLS 1.2) and could be remedied in minutes by reconfiguring the sites to support the proper standards. This points out the need to constantly monitor and assess site configurations to ensure they keep pace with the latest patches and upgrades.

[18] https://ota.ssllabs.com/
[19] https://otalliance.org/resources/type/advertising-integrity-fraud

- **EV SSL Certificates –** As noted, support of EV SSL is an IRS mandate for e-file sites and all but one have complied, yielding a 92% adoption rate. This is by far the highest rate of all sectors (the next closest is banks at 67%, then online retailers at 24%). Implementation of EV SSL is an easy way to allow users to verify they are on the right site (via a green trust indicator in the browser address bar).

- **AOSSL –** Adoption of this key best practice was in the top half (54%), outpacing all but the banks (78%) and presidential candidates (70%). Given that taxpayers are submitting their most personal information on e-file sites, this level of adoption should be higher. Additional incentives include the Federal government itself, which has mandated use of AOSSL for all government sites by December 31, 2016, and Google, whose search results and rendering in Chrome are enhanced for sites supporting AOSSL.

- **Web App Firewall –** Only one e-file site (8%) has implemented a web app firewall, placing them far below all other sectors (overall average is 35%, next lowest is social sites at 12%). Given the sensitivity of the e-file sites, adoption should be much higher.

- **Site Vulnerabilities –** Based on legal limitations, OTA's limited testing for XSS/iFrame and other vulnerabilities was inconclusive. OTA recommends that all e-file sites regularly conduct penetration testing and scans as mandated by the IRS. No sites were found to have malware or malicious links.

2015/2016 AUDIT RESULTS BY SECTOR
SITE SECURITY ADOPTION

	IR100	FDIC	FED	SOCIAL	NEWS	IoT	2016 PRES	E-FILE
EV SSL	24%	67%	11%	21%	8%	4%	4%	92%
Always On SSL	15%	78%	17%	35%	14%	20%	70%	54%
Web App Firewall	47%	32%	46%	12%	28%	36%	35%	8%

Figure 8 – Adoption Rate of Site Security Criteria by Sector

RECOMMENDED BEST PRACTICES

Best practices can be summarized as follows:

- Publish discoverable, easy to find, and comprehensible privacy policies.
- Share details of data retention policies including clarification if such data is retained after the online interaction is terminated.
- Make best efforts to provide notice to consumers if their data is requested by third parties due to legal requirements. Suggested draft copy includes the statement "*To the extent we are legally permitted to do so, we will take reasonable steps to notify you in the event that we are required to provide your personal information to third parties as part of legal process*." [20]
- Create a layered, concise summary linking to an expanded policy. Use icons to help consumers navigate the policy elements more easily. Provide a clear statement including details if, what and for what purposes personal data is being shared with third parties. See OTA short form, linking to the full policy – http://otalliance.org/privacy-policy.
- Write policies for the site's target audience and demographics. Consider providing multi-lingual versions representing the diversity of non-English speaking site visitors. See Spanish version of OTA's privacy policy – https://otalliance.org/politica-de-privacida.
- Disclose whether the site honors Do Not Track (DNT) settings in the site's privacy policy, and preferably honor users' DNT browser settings as required by the State of California. Suggested copy –

  > *XYZ site respects enhanced user privacy controls. We support the development and implementation of a standard "do not track" browser feature, which is being designed to provide customers with control over the collection and use of information by third parties regarding their web-browsing activities. At this time XYZ does not respond to DNT mechanisms. Once a standardized "do not track" feature is released, XYZ intends to adhere to the browser settings accordingly.*

- Utilize tag management systems or privacy solutions that can manage third-party trackers and ensure they are acting properly.

[20] Sites should conduct a legal review to ensure this draft copy is applicable to their site and business models.

E-FILE SITES RESULTS

As noted in the Highlights section, e-file sites had strong scores in the Privacy category, placing second among all sectors and having no failures in this category. Figure 9 below shows the breakdown of the 100 baseline points into its two 50-point components – the policy score and the tracking score. The policy score assesses the privacy policy content regarding clear notice, data sharing/retention/notice practices, Do Not Track disclosure and vendor confidentiality. The tracking score reflects the number and type of third-party trackers on the site, with maximum points possible for a low number of trackers and those that have restrictive (or no) data sharing practices. It should be noted that sites may have add-ons or apps which collect and share data that may not have been detected in this analysis.

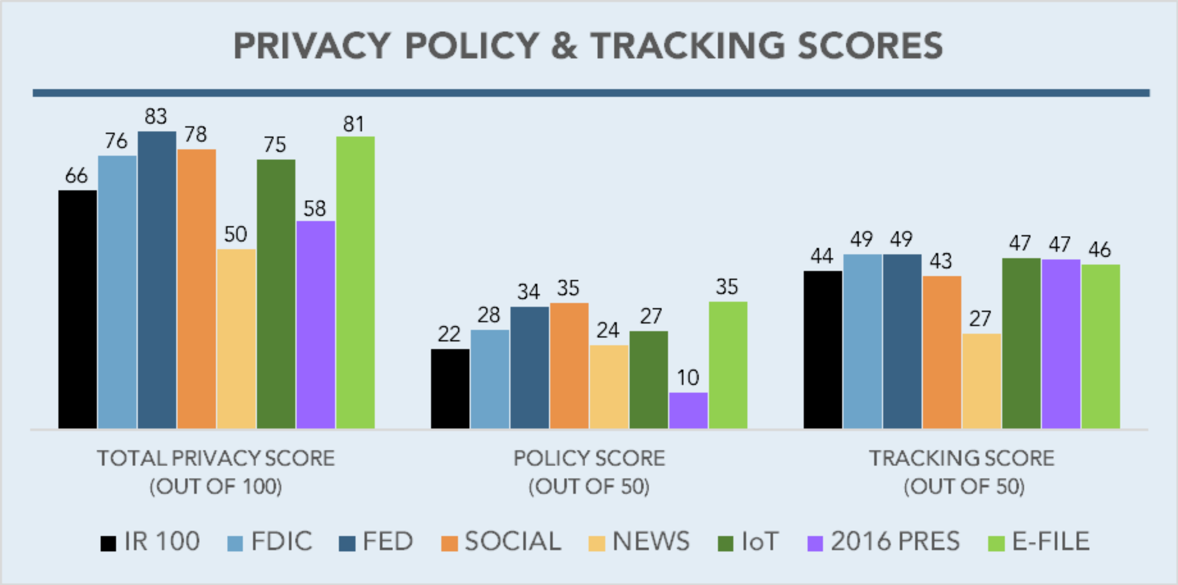


Figure 9 – Privacy Policy and Tracking Scores by Sector

The e-file sites' policy score is tied for the highest at 35, while their tracking score is near the top at 46. The number of trackers per site ranged widely (from 1 to 33) and averaged 10. However, as noted in the Highlights section, there is still a concern regarding sharing of data with third-party marketing affiliates. This underscores the need for sites to disclose their honoring of Do Not Track requests.

Consumers should be aware when visiting these sites that their data may be collected, tracked or shared for marketing purposes. Such practices, while disclosed in the privacy policy legalese of many of the sites, may come as a surprise since the sites seem to have a single purpose and the implied endorsement of the IRS.

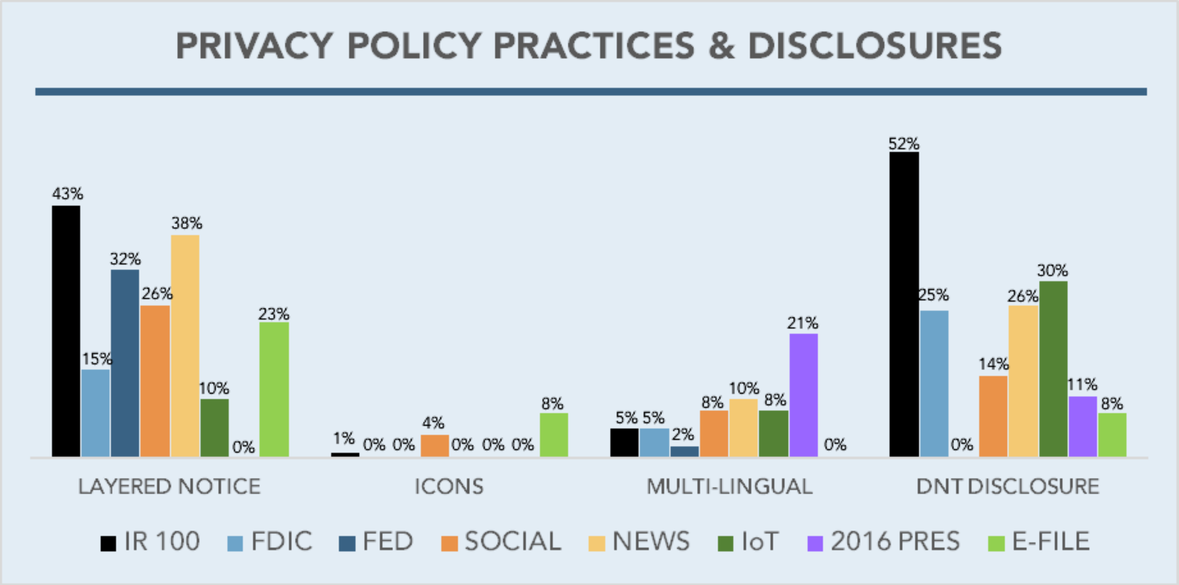


Figure 10 – Privacy Policy Implementation and Disclosure by Sector

Figure 10 above shows additional analysis of the content and implementation of e-file sites' privacy policies, most of which qualify for "bonus" points. Observations regarding these criteria are as follows:

- Layered Notice – Nearly one-fourth of e-file sites had a layered notice, which is slightly higher than the overall sector average of 21%. This is becoming an established practice that will be incorporated into baseline scoring in the 2016 Audit planned for June.
- Policy Icons – One site (8%) used icons in their privacy policy, which further aids user navigation, and no other sectors have implemented this in a meaningful way. See leading example from Publishers Clearing House.[21]
- Multi-Lingual Policies – Surprisingly, though the IRS has a wealth of Spanish-based forms and support, no e-file sites have a multi-lingual privacy policy. They are the only sector with no multi-lingual policies.
- Do Not Track – Only one e-file site addresses Do Not Track in their policy (lagging all but the Federal government sites), and none said they would honor the Do Not Track setting. This requirement is mandated by the State of California for all sites with users who reside in the State and is now a standard, so this requirement is now part of the baseline scoring for the privacy policy in the audit.

[21] http://privacy.pch.com/

Additional privacy observations:

- **Tag Management Systems/Privacy Solutions (TMS/PS) –** Though e-file sites would not be expected to have a significant number of third-party trackers, TMS/PS can help sites better manage, review and monitor data sharing in real time. As noted, the number of trackers varied from 1 to 33, averaging 10. More than two-thirds (69%) of the sites utilize a TMS/PS, the highest of all sectors and well above the overall sector average of 55%. [22]
- **Private WHOIS Registrations –** As noted in the Highlights section, the IRS mandates that e-file sites not use private domain registrations and all sites have complied, yielding a private registration rate of 0% (or conversely, a public registration rate of 100%). This is important to ensure transparency, allowing anyone to see who actually owns these sites.

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

TIPS FOR BUSINESSES & TAX FILING PROFESSIONALS

1. **Recognize Security and Privacy are not Absolutes and Must Evolve.** Regularly review how you store, manage and secure your data. Encryption is a fundamental requirement and failure to encrypt is frequently being cited as the cause for regulatory action and lawsuits. Test the SSL configuration of your servers monthly. Suggested tools include https://ota.ssllabs.com/ and https://www.htbridge.com/ssl/.

2. **Know Your Users.** Enforce effective password management policies. Attacks against user credentials, including spear phishing, brute force, sniffing, host-based access and theft of password databases, remain very strong attack vectors warranting the use of effective password management controls. Adopt multi-factor authentication (e.g. smartcard and PINs in addition to a password) for access to administratively privileged accounts.

3. **Help Consumers; Curb Fraudulent Email.** Require email authentication on mail servers to help detect malicious email, spear phishing and spoofed email. All organizations should authenticate outbound and inbound email with SPF and DKIM, and adopt a DMARC with reject or quarantine policies. https://otalliance.org/eauth

4. **Only Allow Trusted Devices.** Permit only authorized wireless devices to connect to your network, encrypt the traffic of wireless communications and devices such as routers, printers, point of sale terminals and credit card readers. Keep all "guest" network access on separate servers and employ strong encryption on access devices including personal devices and phones used by employees.

5. **Stop Cyber Eavesdropping.** Implement Always On Secure Socket Layer (AOSSL) for all servers requiring log on authentication and data collection. AOSSL helps prevent sniffing of data being transmitted between client devices, wireless access points and intermediaries. https://otalliance.org/AOSSL

6. **Know Who Your Sites Are.** Secure your WHOIS records and review server certificates for vulnerabilities to assess the risk of your domains being hijacked. Attackers have targeted "Domain Validated" (DV) SSL certificates to impersonate websites and defraud consumers. Upgrade to "Organizationally Validated" (OV) or "Extended Validation" SSL (EVSSL) certificates. EVSSL certificates offer the highest level of authentication, providing assurance that the site owner is who they purport to be by presenting the user a green trust indicator. https://otalliance.org/SSL and https://cabforum.org/about-ev-ssl/

7. **Security and Privacy Is Beyond Your Walls.** As more businesses rely on cloud services, organizations must complete risk assessment of their vendors on an ongoing basis. Assessments should review e-providers' security and data privacy practices, confirming alignment to your standards, regulatory requirements and policies.

8. **Being Prepared Is Not Just For Boy Scouts.** Test and continually refine a data breach response plan. Regularly review and improve the plan based upon changes in your organization's information technology, data collection and security posture. https://otalliance.org/Breach

TIPS FOR KEEPING SAFE DURING TAX SEASON

□	**The IRS Does Not Call.** A common scam involves a fraudster calling, claiming to be the IRS and asserting the taxpayer owes money and must pay immediately. The IRS never asks for personal or financial information by email, phone, text or social media nor does it ever call to demand payment. Cyber criminals have learned how to spoof phone caller ID to display "Internal Revenue Service." Report suspicious calls to the IRS at 1-800-366-4484.
□	**The IRS Does Not Email; *Block Spoofed & Forged Email* – Be Skeptical.** Do not respond to an unsolicited email that requests your private or sensitive information or asks you to click on a link. For information, type www.irs.gov directly into your browser. Only use email services which provide complete email authentication checks. Leading consumer services including Yahoo! Mail, Gmail and Outlook / Hotmail support these standards. All business inbound email should validate the sender. Cybercriminals can make messages and webpages look authentic. https://otalliance.org/eauth
□	**Ask Before You Share.** If you are asked for something sensitive such as a Social Security Number (SSN), ask why it is needed and what systems are in place to protect it.
□	**Less is More; Check Default Settings.** Privacy is not the default setting on social sites, which typically make most of your information widely accessible unless you specify otherwise. Change the settings to the privacy level you feel comfortable with. Also, do not share too much – just because a form has blanks, it doesn't mean you have to provide that information.
□	**Protect your Device (PC, Mac, Tablet & Phone).** Keep security software on your devices, and keep it updated. Think of it like locking your home's doors and windows to protect everything inside. Activate auto-locking on your phone, requiring passwords.
□	**When Free Wi-Fi Costs.** Criminals set-up look-a-like hotspots to eavesdrop on unprotected data, and capture user passwords. Consider using a virtual private network (VPN) or tether your computer to your mobile device. Make sure connections are encrypted (https). https://otalliance.org/aossl
□	**Look For The Green.** The IRS and leading organizations now mandate the use of Extended Validation SSL Certificates. Look for the green trust indicator in your browser to help validate that the site you are visiting is legitimate. https://cabforum.org/about-ev-ssl/
□	**Passwords.** Strong passwords are not enough. Use unique passwords and two-factor authentication where possible. Reusing passwords expands the impact of a compromise.
□	**File Tax Returns As Soon As Possible.** When it comes to filing taxes, putting it off to the last minute increases the risk of someone filing a bogus return in your name. File as early as you can.
□	**Check Your Credit History.** Free credit reports are available at annualcreditreport.com. Reports can help indicate use of your identity for nefarious purposes. We recommend ID theft monitoring services and checking your reports monthly. https://otalliance.org/breach

Material in this publication is for educational and informational purposes only. Neither the publisher, the Online Trust Alliance (OTA), its members nor the authors assume any liability for any errors or omissions nor how this publication or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this publication. OTA makes no assertions or endorsements regarding the security, privacy or business practices of companies that may choose to adopt such recommendations outlined. For legal advice or any other, please consult your personal attorney or appropriate professional. The views expressed in this publication do not necessarily reflect the views of OTA member companies, report contributors or affiliated organizations.

OTA MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. For updates visit https://otalliance.org/TaxFraud.