2014
EMAIL INTEGRITY AUDIT

Best Practices to Enhance Trust &
Fight Malicious & Deceptive Email

OTA
Online Trust Alliance

Released August 6, 2014

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Since 2004, OTA has been working on the development of best practices and standards to enhance the integrity of the email channel. While email continues to flourish as a vibrant medium to engage and connect consumers worldwide, fraudulent actors and cybercriminals continually utilize email for malicious purposes. With the advent of interest-based advertising, markets have the ability to increase the precision and relevance to reach consumers. Unfortunately cybercriminals are doing the same and leveraging email's open structure for illicit purposes.

Targeted email-based spear phishing campaigns are an ongoing threat to consumers worldwide. Phishing compromises unsuspecting consumers and business users, driving identity theft, ransomware, account takeovers and data breach incidents. Left unabated, these threats run a significant risk of undermining the trust and confidence in email.

The Email Integrity Audit is a companion to the 2014 Online Trust Audit and Honor Roll report released in June 2014. This Audit provides an in depth review of email security best practices, focusing on the best practices necessary to help detect and to block spoofed and forged email.

This Audit tracks the adoption of three critical email authentication standards; Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting & Conformance (DMARC). The Audit also includes Transport Layer Security (TLS) a recommended best practice to enhance the privacy of email communications while in transit from one user to another.

By implementing email authentication, organizations can help protect their brands and consumers from receiving spoofed and forged email. Building on the SPF and DKIM protocols, DMARC adds a policy assertion providing receiving parties (e.g., ISPs and corporate network email administrators) with indications on how to handle messages which fail authentication. Equally as important, DMARC provides a reporting mechanism back to the brand / domain owner about both their authentication practices and about email sent by unauthorized third parties.

It is widely accepted that when organizations implement SPF, DKIM and DMARC across all of their outbound email streams they achieve three major benefits:

1. Increased protection from consumers receiving malicious and fraudulent email
2. Improved brand reputation protection
3. Enhanced deliverability of legitimate email into users' inboxes

There has been growth in the deployment of email authentication in all industry sectors, yet major and systemic issues remain. The failure to apply authentication standards comprehensively risks placing consumers and employees in harm's way. This is often the result of companies authenticating only selected sub-domains and failing to authenticate their top level domain which is the domain most often abused. The inconsistent use of authentication is like reinforcing and locking the front door to your house, while leaving your side door or garage doors wide open.

In addition to the implementation of these standards, brand owners should monitor both existing and new domain registrations for look-a-like domains and brand-jacking. Proactive defensive domain registrations are a critical step in protecting a brand by reducing the availability of look-a-like domains. Such domains can be used for socially engineered exploits including spear phishing and other nefarious purposes and can be easily mistaken by the user resulting in their device and online credentials being compromised.

EMAIL TRUST SCORECARD

New to this report, OTA has introduced the Email Trust Scorecard, an assessment which measures the adoption of these recommended best practices. Qualifying for the email honor roll is achieved by implementing both SPF and DKIM consistently for the top level domain and for observed sub-domains, along with publishing a DMARC record.[1]

Figure 1 below highlights that the vast majority of organizations across all segments have yet to adopt email authentication practices comprehensively, putting consumers businesses and their brands at risk. As outlined across all segments only 8.3% qualified.

"Combined SPF, DKIM and DMARC has helped to block hundreds of thousands of messages, helping to protect our customers from potential email threats. DMARC is invaluable and promises to be one of the most noteworthy developments in the email industry in the last decade."

Sal Tripi, Assistant Vice President, Digital Operations & Compliance, Publishers Clearing House

The data in this report confirms that organizations recognize the benefits of email authentication. Today the majority of consumer mailbox providers and ISPs utilize email authentication to fight spam and malicious email. However a lack of comprehensive adoption across brands' top level corporate domains and delegated sub-domains raises significant concerns, indicating a disconnect between the email marketing, operations, IT and security teams within many organizations.

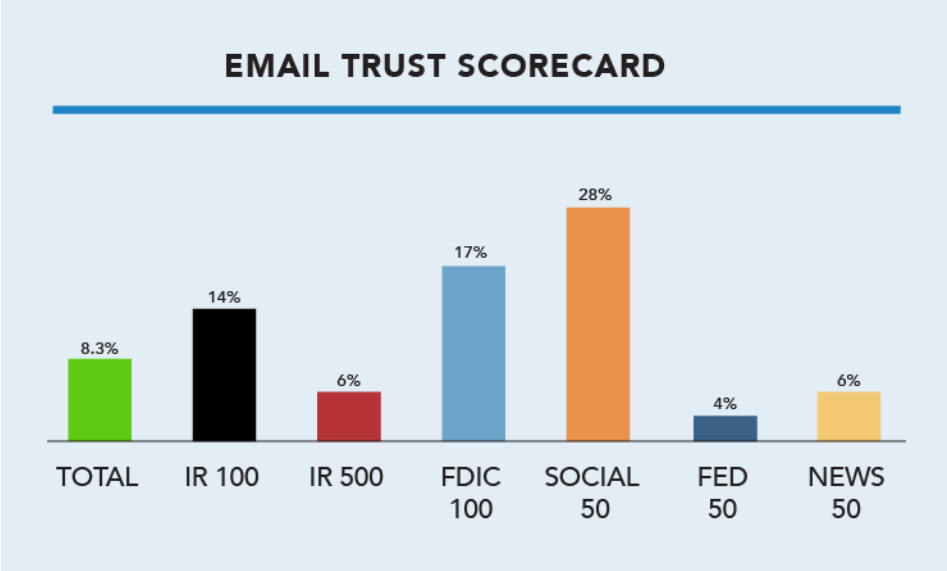

Figure 1 - Email Trust Scorecard

[1] See methodology in Appendix B, outlining audit segments. OTA includes evaluation of all industry member companies.

Email authentication is not consistently deployed for several reasons. This is often due to email marketing being delegated to third parties and groups outside of an organization's security team. Email marketers and operations teams typically lack the perspective of total brand security and may not have the incentive to engage with the security or brand management teams within their respective organizations.

Businesses that fail to implement email authentication to its fullest potential not only place their brand reputation at risk, but also unnecessarily open themselves to potential liabilities and class action suits relating to the lack of consumer protection safeguards.

Inadequate email authentication continues to be the leading cause of sites failing to qualify for the 2014 Online Trust Honor Roll (see Figure 2).[2]

"Over 400 million Microsoft users worldwide are realizing the benefits of SPF, DKIM and DMARC. As email threats and spear phishing grow, every business should make email authentication a priority to help protect their consumers, their employees and their brands."

John Scarrow, GM Safety Services, Microsoft Corporation

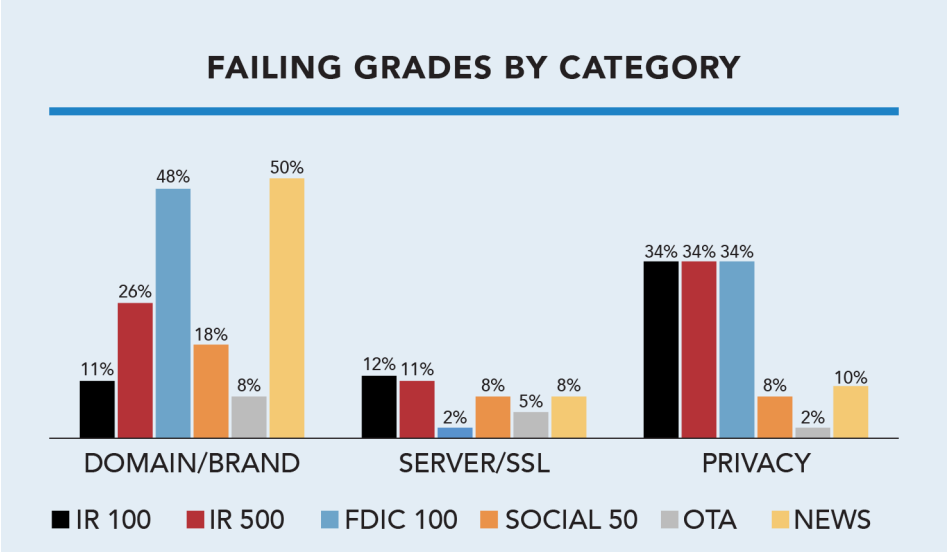

Figure 2 - Failing Grades

[2] OTA Honor Roll https://otalliance.org/HonorRoll

AUDIT HIGHLIGHTS

The following is a summary of email authentication trends and observations, for each sector. While adoption continues to climb across all sectors, the lack of comprehensive adoption at the top level domain and implementation of both SPF and DKIM, remains a significant concern to consumer and brand protection.

- **Email Trust Scores** -4 Of the consumer facing domains and websites sampled, only 8.3% have fully implemented SPF, DKIM and DMARC. OTA's members represent early adopters with over 63% fully implemented the standards but were omitted from this calculation to focus the analysis on consumer facing brands.

- **Email Authentication** - Adoption of both SPF and DKIM rose across all sectors. Led by the Internet Retailer 100 with 88% adoption, the Internet Retailer 500 showed the largest year-to-year growth climbing from 56% to 74% adoption (see Figure 5).

- **Top Level Domains (TLDs) vs Sub-Domains** - SPF and DKIM adoption continues to grow primarily at delegated sub-domains, yet disappointingly, brands are failing to authenticate at the TLD, affording limited brand and consumer protection (see Figures 6 & 7).

- **Domain-based Message Authentication, Reporting & Conformance (DMARC)** - Adoption continues to rise in all sectors, yet remains disappointingly low. There remains significant room for improvement, especially in the Fed 50, FDIC 100, IR 100/500 and News 50 sectors (See Figure 8).

- **Top 100 Internet Retailers (IR 100)** - Continues to outpace all segments in adoption of SPF and DKIM, yet lag behind the FDIC 100 and Social 50 in adoption of DMARC indicating a missed opportunity for brand and consumer protection.

- **FDIC 100** - The top 100 FDIC insured banks (FDIC 100), had the highest failure rate compared to all sectors, caused by lack of email authentication support (especially DKIM at their TLD), as reported in the 2014 Honor Roll audit (see Figure 2). Only 17% of the FDIC 100 have passing email scores reflecting consumers are at a higher risk of receiving forged and spoofed email from a major bank.

- **Social 50** - Top social sites including social networking, dating, gaming and document sharing sites received the highest score for DMARC adoption (36%) (See Figure 8). Social led all segments in DKIM adoption at their TLD outpacing the FDIC and IR 500 by over 2:1 (see figure 7).

- **Federal Government 50** - Consistently scored at the bottom of every email authentication adoption metric. Only 4% passed the Email Trust Scorecard, due in part to only 20% adopting DKIM at their TLD and only 6% publishing a DMARC record.

EMAIL AUTHENTICATION STANDARDS

Email Authentication helps to solve an inherent design flaw of internet email - it is simple to send email using any identity one chooses, fooling the user into opening mail purporting to be sent from a legitimate brand or organization. In late 2003 the standards community, including leaders in the public and private sector, began to develop solutions and technologies to address this vulnerability. Nearly a decade later, two protocols have emerged, Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) which are widely deployed worldwide.

These protocols work to complement each other to help verify that the email is authorized by the owner of the domain used. SPF describes where a domain's email should be coming from. It works by allowing a sending domain to publish a list of IP addresses in a DNS text file which are authorized to send email on behalf of that domain when it is used in the "envelope From" address of the message. DKIM uses cryptography to sign messages originating from a server. By digitally signing those messages, the mail operator confirms that they came from him/her, taking "responsibility" for those messages. Combined they address the strengths and weaknesses of each other to provide a robust authentication mechanism.

Receiving networks (ISPs and corporate mail systems), complete the analysis of the email against the domain's DNS to make a determination on placing the email in the inbox, junk folder or blocking it. For details visit https://otalliance.org/eauth.

As outlined, the most promising and globally implemented email standards include SPF, DKIM and DMARC, each of which has seen significant adoption over the past three years. Figure 3 outlines the adoption of each standard, illustrating SPF's broader uptake across all segments – which outpaces DKIM from 4% to 34%. This delta is attributed to the fact that SPF is easier to implement than DKIM and that the SPF standard preceded the DKIM protocol by two years. Other factors include the lack of outbound mail servers capable of DKIM signing and the perceived complexity of signing.

"Email is a cybercriminal's best friend – companies don't stand a chance in winning the consumer protection war without successful implementation of DMARC, SPF and DKIM."

Patrick Peterson,
Founder & CEO, Agari

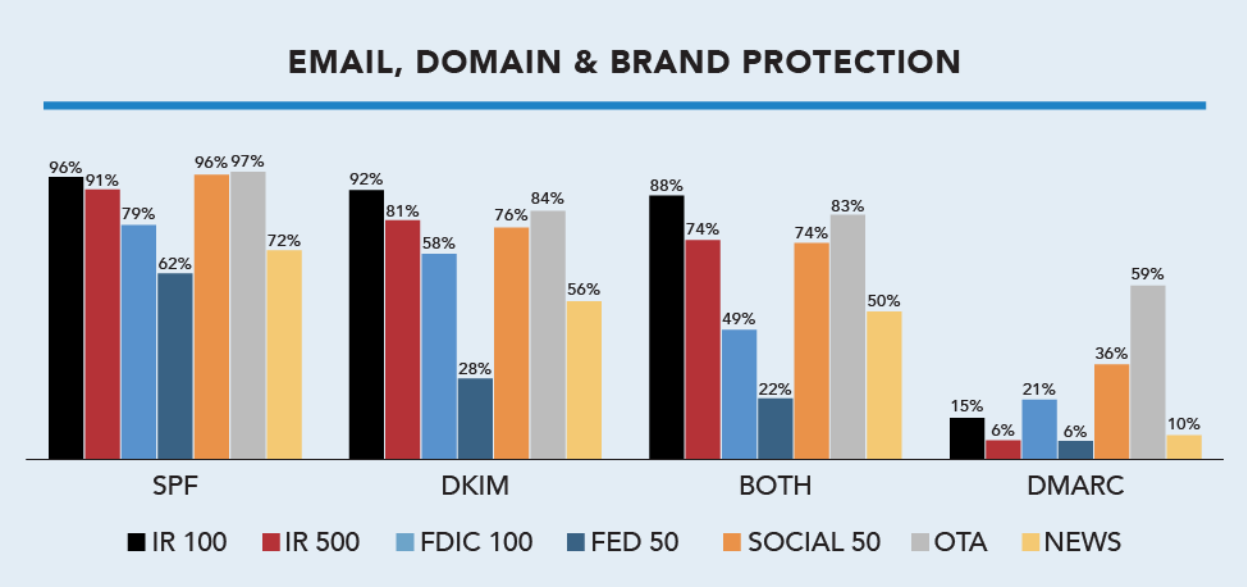

Figure 3 - Email Authentication

Combined adoption of either SPF or DKIM is reaching 100%. This high level of adoption across all segments demonstrates that groups within all organizations have recognized the benefits of at least one type of email authentication. As illustrated in Figure 4, the exceptions are the News 50 and Fed 50, where adoption continues to lag, while the Internet Retailer 500 showed the largest year-to-year growth. Considering the increased targeting of consumers via forged email purporting to be sent from U.S. Government agencies, a combined adoption rate of only 68% by this segment is concerning.

Organizations worldwide have found that simultaneous use of both SPF and DKIM best enables receivers to detect and block forged and malicious email, while reducing the risk of false positives from email being forwarded or sent from mailing lists. Combined, SPF and DKIM address the most common use cases of email, including mailing lists and mail forwarding.

Figure 5 shows the disparity in adoption of both SPF and DKIM, which is led by the Internet Retailer 100 at 88%, while the Fed 50 lags significantly at only 22%. This low adoption rate impedes receiving networks and ISPs from accurately detecting and blocking malicious and fraudulent email purporting to come from government agencies and suggests the need of a possible directive from the White House Office of Management and Budget, (OMB) or U.S. Department of Homeland Security mandating email authentication.

"SPF and DKIM are vitally important for email senders to implement today, but they are merely table stakes in an escalating battle against email fraud. DMARC is a powerful solution empowering senders who are prone to brand infringement and malicious attacks."

Robert Holmes, General Manager, Fraud & Brand Protection Services, Return Path

EITHER DKIM OR SPF

	2010	2011	2012	2013	2014
IR 100	76.0%	84.0%	97.0%	96.0%	100.0%
IR 500	54.3%	64.9%	90.6%	88.0%	98.0%
FDIC 100	55.0%	58.9%	69.0%	77.0%	88.0%
Fed 50	32.0%	38.0%	58.0%	72.0%	68.0%
Social 50	-	92.0%	96.3%	98.0%	96.0%
OTA Members	88.0%	95.0%	99.0%	100.0%	98.4%
News 50	-	-	-	-	78.0%

Figure 4 - DKIM or SPF Adoption

BOTH DKIM & SPF

	2010	2011	2012	2013	2014
IR 100	24.0%	42.0%	55.6%	76.0%	88.0%
IR 500	14.4%	23.0%	43.0%	55.6%	74.2%
FDIC 100	22.0%	23.3%	34.0%	49.0%	49.0%
Fed 50	2.0%	4.0%	10.0%	20.0%	22.0%
Social 50	-	28.0%	63.0%	72.0%	74.0%
OTA Members	36.0%	43.8%	58.6%	68.8%	82.8%
News 50	-	-	-	-	50.0%

Figure 5 - Adoption of Both DKIM & SPF

Year-to-year adoption of both SPF and DKIM grew in nearly all sectors, most notably by the Internet Retailers. It is important to note that some of the growth observed in 2014 may be attributed to more thorough analysis by OTA of the retail sector, achieved by signing up for and reviewing newsletters received directly to OTA analysts. This data confirms that online retailers and social platforms, who are most heavily reliant on email interaction, have recognized the value of email authentication. Still, more efforts are needed at the corporate domains to maximize protection.

The financial services sector, which continues to be targeted by spear phishing exploits resulting in millions of dollars of financial losses, has disappointing results - failing to reach 50% adoption of both SPF and DKIM. Equally as concerning is the failure of U.S. Government sites to adequately protect 78% of their domains.

"Implementing DMARC stopped nearly 25 million attempted attacks on our customers. Not only is DMARC shutting down spoofed domain attacks, but it has also cut the overall volume of daily attacks in half since 2012."

Trent Adams, Senior Advisor on email security for PayPal and eBay Inc.

An additional concern is inconsistent DKIM signing. Such evidence was observed both within specific sub-domains and multiple sub- domains of a single company. OTA's analysis revealed that mail being sent from specific sub-domains may be authenticated one day, but not the next. Several instances were found where leading commerce and banking sites authenticating less than 10% of the total mail sampled. This may be due to the use of multiple vendors across lines of businesses or the lack of an integrated corporate email authentication strategy. The result, however, is that it preempts receiving networks from being able to confidently reject or block unauthenticated or failing domains from malicious, unauthorized sources. This is an opportunity for the email marketing community and service providers to take a proactive role enhancing their client's brand protection efforts.

TOP LEVEL DOMAIN VS SUB-DOMAIN ANALYSIS

A critical component and value of email authentication is the importance of authenticating domains at the top level or brand domain. While email service providers have championed the merits of email authentication for deliverability and inbox placement, generally they have failed to make the case of the importance for brand protection and safeguards to help curb spear phishing. Ironically, forged email purporting to be from a brand's domain will impact consumer trust in that firm's legitimate email marketing campaigns. While deliverability into the mailbox may be achieved for mail coming from a brand's sub-domain, consumer willingness to open the email may be adversely impacted due to past spoofing incidents.

There is a large disparity between the protection of a brand's main domain and their sub- domain's adoption of both SPF and DKIM. For example, coming from an organization's top level domain otalliance.org versus the sub domain email.otalliance.org. The largest variance (52%), is found in DKIM adoption in the Internet Retailer 100 where 85% of subdomains use DKIM compared to only 33% of top level domains at the same companies.

SPF ADOPTION

	2010	2011	2012	2013		2014	
	Top Level Domains	Top Level Domains	Top Level Domains	Top Level Domains	Any SPF	Top Level Domains	Any SPF
IR 100	76.0%	84.0%	67.0%	77.0%	85.0%	78.0%	96.0%
IR 500	54.3%	64.9%	62.5%	68.8%	78.6%	74.8%	91.0%
FDIC 100	55.0%	58.9%	60.0%	62.0%	76.0%	68.0%	79.0%
Fed 50	32.0%	38.0%	50.0%	60.0%	68.0%	62.0%	62.0%
Social 50	-	92.0%	96.3%	94.0%	96.0%	94.0%	94.0%
OTA Members	88.0%	95.0%	98.6%	98.4%	100.0%	95.3%	96.9%
News 50	-	-	-	-	-	58.0%	72.0%

Figure 6 - SPF Adoption Trends

DKIM ADOPTION

	2010	2011	2012	2013			2014		
	Any DKIM	Any DKIM	Any DKIM	Top Level Domains	Sub Domains	Any DKIM	Top Level Domains	Sub Domains	Any DKIM
IR 100	37.0%	55.0%	82.8%	26.0%	81.0%	87.0%	33.0%	85.0%	92.0%
IR 500	22.8%	33.4%	69.5%	17.8%	57.6%	65.0%	27.0%	69.8%	81.2%
FDIC 100	29.0%	34.4%	44.0%	30.0%	38.0%	50.0%	27.0%	47.0%	58.0%
Fed 50	4.0%	6.0%	18.0%	22.0%	6.0%	24.0%	20.0%	14.0%	28.0%
Social 50	-	52.0%	63.0%	62.0%	42.0%	74.0%	56.0%	44.0%	76.0%
OTA Members	22.0%	34.5%	57.1%	57.8%	28.1%	68.8%	73.4%	37.5%	84.4%
News 50	-	-	-	-	-	-	14.0%	42.0%	56.0%

Figure 7 - DKIM Adoption Trends

DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING & CONFORMANCE (DMARC)

DMARC is an emerging standard built on the foundation of SPF and DKIM, helping to reduce the threat of deceptive emails. Since being introduced in early 2012, leading brands including Apple, Facebook, Publishers Clearing House, PayPal, LinkedIn, JPMorgan Chase, Bank of America, American Greetings, Netflix and Twitter have recognized significant value from its use.

"DMARC dramatically reduced the number of forged emails sent to our users. DMARC was a direct benefit to our users by blocking these impersonations."

Josh Aberant, Twitter's Postmaster

DMARC record provides direction to receiving networks on how to validate email authentication using SPF and DKIM. DMARC also provides a feedback mechanism, allowing for fraudulent messages to be reported to the domain owner.

Domain owners may receive both aggregated (RUA) and failure reports (RUF), providing telemetry on their legitimate email as well as the email authentication failures. A major part of DMARC's value is the reporting of email traffic seen by receiving networks. This reporting shows legitimate email coming from all known sources for a sender, including sending delegated to third parties. More importantly, it shows unauthenticated email traffic for a sender's domains, which may be forged email from bad actors misusing the sender's domain as well as reporting inaccurate email authentication practices.

Figure 8 shows that DMARC adoption has grown significantly across all segments, but still has significant room for adoption. The chart includes an analysis of DMARC records which have set Reject ("R") or Quarantine ("Q") policies. These stated policies provide receiving networks increased confidence in blocking email that fails authentication. While these benefits are significant, implementation of such policy assertions should only be done with due diligence and only be considered after a comprehensive evaluation of all email streams and careful review of DMARC feedback reports.

It should be noted that the "R or Q" calculation shown in Figure 8 is a percentage of domains that have published a DMARC record. As the awareness of DMARC increases and more records are published, the calculated percent of R or Q reported may decline, while the absolute number of such policy assertions has not. As DMARC adoption matures, it is expected the implementation of R or Q policies will rise.

DMARC ADOPTION

	2012	2013		2014	
	Record	Record	R or Q	Record	R or Q
IR 100	2.0%	5.0%	40.0%	15.0%	40.0%
IR 500	1.5%	3.0%	26.7%	6.2%	32.3%
FDIC 100	1.0%	13.0%	15.4%	21.0%	9.5%
Fed 50	0.0%	4.0%	0.0%	6.0%	0.0%
Social 50	18.5%	22.0%	63.6%	36.0%	50.0%
OTA Members	34.3%	43.8%	10.7%	59.4%	13.2%
News 50	-	-	-	10.0%	0.0%

Figure 8 - DMARC Adoption Trends

INBOUND EMAIL AUTHENTICATION

Cybercriminals have recognized the value of confidential and proprietary business data and have developed sophisticated abilities to compromise business systems to acquire consumer data. Spear phishing and malware distribution to compromise business users' passwords and system access is growing as experienced by many email service providers and recently evidenced in the attack on one of Target Corporation's vendors.[3] This well-orchestrated threat underscores that all organizations in both the public and private sector must implement email authentication verification on inbound messages to help protect employees and internal systems from attacks.

While the focus of this report is on a company's outbound adoption of email authentication for brand and consumer protection, the full value of authentication is only realized when both the sender and receiver are participating in the process. While consumer ISPs have overwhelmingly adopted inbound authentication, this affords little protection for business-to-business communications.

A key issue limiting enterprise and government sectors from implementing (both inbound and outbound) email authentication has been the low level of support and integration in the commercial systems and software used to send and receive email. Unfortunately, in many enterprises the email infrastructure does not natively support outbound signing or inbound checking for SPF, DKIM or DMARC. Equally as concerning is the lack of support for inbound authentication from leading MTAs (Mail Transfer Agents), the hosting community and email technology providers. OTA encourages customers to reach out to their vendors and review their respective product road-maps. It is expected that within twenty-four months, inbound email authentication will become a standard offering akin to email AV, spam and malicious threat detection capabilities.[4]

Email Authentication Resources
For a summary of resources on SPF, DKIM and DMARC visit https://otalliance.org/eauth including white papers, third party tools and record validators.

[3] http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

[4] See https://otalliance.org/emailaudit for a listing of MTA support.

TRANSPORT LAYER SECURITY (TLS)

Today email is effectively a plain text communication sent from email clients to receiving email servers or from one server to another. This design limitation leaves the content of a message in transit open for anyone to eavesdrop; from a wireless hotspot at the airport or coffee shop to your ISP and internet backbone providers that carry your messages throughout the world.

Transport Layer Security (TLS) helps solve this issue by offering encryption technology for your message while it is "in transit" from one secure email server to another. That is, TLS helps prevent eavesdropping on email as it is carried between email servers that have enabled TLS protections for email. Just as TLS can be used to secure web communications (HTTPS), it can secure email transport. In both applications, TLS has similar strengths and weaknesses. To maximize the content security and privacy, TLS is required between all the servers that handle the message including hops between internal and external servers.

TLS is rapidly being adopted as the standard for secure email. Since 2007, led by the Financial Services Roundtable / BITS, leading banks including JPMorgan Chase, Bank of America and others have implemented TLS for communications between banks to provide added security and privacy for bank-to-bank emails.[5]

Key features of TLS includes:

- **Encrypted Messages:** TLS uses Public Key Infrastructure (PKI) to encrypt messages between mail servers. This encryption makes it more difficult for hackers to intercept and read messages.

- **Authentication:** TLS supports the use of digital certificates to authenticate the receiving servers. Authentication of sending servers is optional. This process verifies that the receivers (or senders) are who they say they are, which helps prevent spoofing.

Opportunistic TLS is accomplished when used by both sending and receiving parties to negotiate a secured SSL/TLS session and encrypt the message. Today, leading consumer ISPs and mailbox providers including Comcast, Google, Microsoft and Yahoo are supporting TLS. The 2015 OTA Online Trust Honor Roll and future Email Integrity Audits will incorporate TLS adoption as a key metric.

OTA recommends organizations adopt TLS and periodically test their servers to help ensure their configuration is secure and optimized. Updates to this best practice and related resources may be found at https://otalliance.org/TLS.

[5] http://www.bits.org/publications/security/BITSSecureEmailApr2007.pdf

CONCLUSION

The OTA Email Integrity Audit works to highlight best practices and identify those companies that have demonstrated a commitment to consumer safety, security and privacy.

The reports highlight positive growth and momentum, yet also point out significant vulnerabilities. The email community needs to expand their influence and engage their security and IT counterparts. All brand owners in both the public and private sectors need to adopt the following best practices:

1. Adopt a holistic strategy to implement email authentication across all email channels and domains including; 1) TLDs, 2) sub-domains, 3) parked domains and 4) domains that don't send email.

2. Implement both SPF and DKIM for domains. Combined they provide coverage for the majority of use cases including mail forwarding.

3. Implement DMARC for all actively used email domains, initially in "monitor" mode to obtain receiver feedback and verify accuracy of email authentication, and eventually to assert a "reject" or "quarantine" policy to receivers.

4. Implement inbound email authentication and DMARC support to protect employees and corporate data from spear phishing exploits.

5. Publish DMARC"reject policies" for "parked domains"and any domain not used for email.[6]

6. Continually monitor and update mailflows including third party delegated domains, update DKIM keys and SPF records with current sending IP addresses.

7. Implement opportunistic TLS to enhance users' privacy and security of their email while in transit.

8. Monitor domain registrations for look-a-like domains which can be used to fool consumers into thinking they are receiving legitimate email from your organization.

As the world economy and society at-large become increasingly reliant on the Internet, it is incumbent on the business community, government agencies and associated trade organizations to embrace these practices, moving from a compliance mindset to one of stewardship. Collectively we have an opportunity to enhance trust and integrity in email while helping to protect consumers from harm.

Updates to the report with additional data and resources are posted https://otalliance.org/emailaudit. To submit comments or suggestions, email editor @ otalliance.org.

[6] Parked domains refer to domains acquired, but not used.

ACKNOWLEDGMENTS

Data and analysis has been provided in part by: Agari, American Greetings, bounce.io, Constant Contact, Digicert, Exact Target, Facebook, ICONIX, Lashback, Microsoft, Responsys (Oracle), OPTIZMO, Return Path, Silverpop, Symantec and Twitter. Special thanks to OTA strategic advisors for their input including Shaun Brown, Mark Goldstein and Joe St. Sauver.

ABOUT ONLINE TRUST ALLIANCE (OTA)

The Online Trust Alliance (OTA) is a 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 members and supporters include leaders spanning public policy, technology, e-commerce, social networking, mobile, email and interactive marketing, financial, service provider, government agency and industry organization sectors.

OTA is a 501(c)(3) tax exempt global non-profit focused on enhancing online trust with a view of the entire ecosystem. OTA is supported by donations and support across multiple industries, representing the private and public sectors. To support OTA visit https://otalliance.org/donate.

APPENDIX A
EMAIL TRUST SCORECARD PASSING SCORES

Federal Top 50

U.S. House of Representatives

U.S. Senate

FDIC Top 100 Banks

American Express Bank, FSB American Express Centurion Bank Arvest Bank
Bank of America California
Bank of America
Capital One Bank (USA)
Capital One
Charles Schwab Bank
Chase Bank USA
FIA Card Services
SunTrust Bank
U.S. Bank National Association
USAA Federal Savings Bank
USAA Savings Bank
Wells Fargo Bank Northwest
Wells Fargo Bank South Central Wells Fargo Bank

Internet Retailer Top 500

1-800-Flowers.com Inc.
Amazon.com Inc.
American Greetings Corp.
Ancestry.com Inc.
Apple Inc.
Bidz.com Inc.
Christianbook.com LLC
Coastal Contacts Inc.
Crutchfield Corp.
eBags Inc.
Etsy Inc.
Frys.com
Groupon
JackThreads.com
Kate Spade
LivingSocial Inc.
Netflix Inc.
Newegg Inc.
Nordstrom Inc.
Overstock.com Inc.
Shutterfly Inc.
Silver Star Brands
Sweetwater
Target Corp.
Title Nine
TJX Cos. Inc.
Vistaprint N.V.
zulily Inc.

News/ Media Top 50

Google News
New York Times
PR Web

Social Top 50 [1]

AOL
Badoo.com
Box
Dropbox
Facebook
Foursquare
iCloud
Instagram
LinkedIn
MeetMe
Twitter
Yahoo!
YouTube
Zynga

OTA Members [2]

Act-On Software
American Greetings Interactive
Agari
AVG Technologies
BaseGrow
bounce.io
Constant Contact
Distil Networks
eBay Enterprise
Ensighten
eWayDirect
ExactTarget
flybuys
GlobalSign
Harland Clarke Digital
High-Tech Bridge SA
Iconix
Identity Guard
Innovyx
Intersections
LashBack
Listrak
MarkMonitor
Marketo
MeetMe
Message Systems
Microsoft
OPTIZMO
Publishers Clearing House
Return Path
Sailthru
Simpli.fi
Silverpop
SiteLock
Symantec
TRUSTe
TrustSphere
Twitter
ZEDO
Zynga

[1] Social 50 includes top social networking, dating, entertainment, document storage, photo and collaboration sites.
[2] Does not include academia, law enforcement, professional members, public sector, non-profits or members companies who joined since May 1, 2014.

APPENDIX B - METHODOLOGY

Data sampling was completed between April 15 and May 23, 2014 as part of the overall 2014 Online Trust Audit, evaluating domain and brand protection, site security and privacy enhancing best practices. In total, over 800 web sites were evaluated and over 100 million email headers. It is important to note that a site's email practices and DNS may have changed since the sampling and the data only reflects findings observed during this snapshot in time.

Details on the methodology is posted at https://otalliance.org/initiatives/2014-methodology.

Segments Evaluated:

- IR100 & IR 500 (Interent Retailer 100 & Internet Retailer 500). Ranking based on revenue as reported by Internet Retailer Magazine, produced by Vertical Web Media. Ranking as of May 1, 2014. http://www.internetretailer.com/top500/.
- FDIC top 100 banks (FDIC 100). Based on net assets as reported by the Federal Deposit Insured Corporation. Ranking as of December, 31, 2013. http://www.managingmoney.com/fdic.php.
- Top 50 Federal Government sites (Fed 50). Based on a combination of consumer traffic and recent cybercriminal targeting of Federal Government sites including forged email campaigns and phishing sites. Includes Cabinet level agencies at risk of such exploits.
- Top 50 Social Networking and sharing sites (Social 50). Includes social networking, dating entertainment, gaming, document storage, photo and colloboration sites..
- Top 50 News and Media sites (News 50). Includes top ranked news, content and media sites, (non-ecommerce or social).
- OTA Member Companies (OTA Members). Includes commercial members including consumer and business to business sites. Does not include academia, law enforcement, professional members, public sector, non-profits or members companies who joined since May 1, 2014. https://otalliance.org/about-us/members.