2014 Email Integrity Audit

Fighting Malicious & Deceptive Email

August 13, 2014

Craig Spiezle
Executive Director & President, OTA

Mike Jones
Director of Product Management, Agari

OTA Online Trust Alliance

LEARN · INNOVATE · COLLABORATE

About Us

OTA Online Trust Alliance

- The Online Trust Alliance (OTA) is a 501c3 charitable non-profit with the mission to enhance online trust and empower users, while promoting innovation.
- 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, meaningful self-regulation and data stewardship.

© 2014 All rights reserved. Online Trust Alliance (OTA)

LEARN · INNOVATE · COLLABORATE

Overview

- Background – 2014 Online Trust Honor Roll
- Top Level Findings – Email Trust Scorecard
- Highlights
- Either DKIM or SPF
- Both DKIM or SPF
- Subdomains
  - SPF & DKIM
- DMARC
- TLS
- Summary – Best Practices

© 2014 All rights reserved. Online Trust Alliance (OTA)

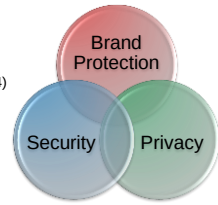
OTA Online Trust Alliance

LEARN · INNOVATE · COLLABORATE

© 2014. All rights reserved. Online Trust Alliance (OTA)

Honor Roll Overview

- **Analysis of ~800 web sites**
  - FDIC Banking 100
  - Internet Retailer 500
  - Top 50 Social
  - Top 50 News/Media (introduced in 2014)
  - Top 50 Federal Gov't
  - OTA Members
- **Scoring**
  - Up to 100 points in each category
  - Bonus points for emerging practices
  - Penalty points for
    - Data loss incident
    - Fines/settlement
    - Failure to follow established practices
  - Honor Roll = 80% of total points, 55% or better in each category



© 2014 All rights reserved. Online Trust Alliance (OTA)
Slide 4
LEARN • INNOVATE • COLLABORATE

Why Care

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

© 2014 All rights reserved. Online Trust Alliance (OTA)
Slide 5
LEARN • INNOVATE • COLLABORATE

Brand Protection - Eauth

Email Authentication

- **SPF**: *Path-based.* Sender publishes list of authorized servers. Email receiver checks if server is authorized to send for domain.
- **DKIM**: *Signature-based.* Sender inserts signature into email. Email receiver checks signature regardless of source.
- **DKIM+SPF =** Resilient email authentication infrastructure

© 2014. All rights reserved. Online Trust Alliance (OTA)
Slide 14
LEARN • INNOVATE • COLLABORATE

© 2014. All rights reserved. Online Trust Alliance (OTA)

Complementary Standards

SPF

- *Path-based (*RFC 7208)
- Authorized servers published via simple DNS record
- Very low deployment cost
- Forwarding breaks SPF

Is the messenger (server) permitted?

DKIM

- *Signature-based* (RFC 6376)
- Requires cryptographic operation by email gateways
- Public keys published via DNS
- Can survive forwarding

Is the signature authentic?

© 2014. All rights reserved. Online Trust Alliance (OTA)

Complementary Standards

DMARC

- **Overlay** – Leverages SPF and DKIM as authentication mechanisms
  - Describes how to deploy SPF and DKIM… consistency
- **Visibility** – Describes new feedback mechanism
  - Gives senders visibility into how receiver's process their email
- **Policy** – Senders can declare how to process auth-failing email
  - Specifies a DNS-based policy model that incorporating SPF + DKIM results

SPF

- *Path-based (*RFC 7208)
- Authorized servers published via simple DNS record
- Very low deployment cost
- Forwarding breaks SPF

Is the messenger (server) permitted?

DKIM

- *Signature-based* (RFC 6376)
- Requires cryptographic operation by email gateways
- Public keys published via DNS
- Can survive forwarding

Is the signature authentic?

© 2014. All rights reserved. Online Trust Alliance (OTA)

DMARC Value

OTA Online Trust Alliance

Domain Owners & Email Senders Receive:

- Enhanced brand protection
- Ability to communicate what to do with illegitimate email
- Feedback loop to improve and monitor their authentication infrastructure
- Visibility on both the abuse of their domain and to optimize authentication across all domains and subdomains

Receiving Networks & ISPs receive:

- Clarity for handling of un-authenticated & failing email
- Uniform and scalable method to determine email legitimacy
- Freedom to act on email with confidence – no more guessing
- Scalable methods to provide feedback to Domain Owners

End Users

- Greater confidence of the email channel and significant reduction in risk of phishing from DMARC domains.

© 2014. All rights reserved. Online Trust Alliance (OTA)

© 2014. All rights reserved. Online Trust Alliance (OTA)

DMARC Policy

- Policy options:
  - "none" – simply monitor and supply feedback
  - "quarantine" – process email with high degree of suspicion
  - "reject" – do not accept email that fails DMARC check
- Policy discovery:
  - Receivers extract the RFC5822.From domain, query DNS for TXT record:
    - _dmarc.mail.sub.example.com
  - If none found, extract and attempt "Organizational Domain":
    - _dmarc.example.com
  - Method caps # of DNS lookups in DMARC policy discovery to 2

© 2014. All rights reserved. Online Trust Alliance (OTA)

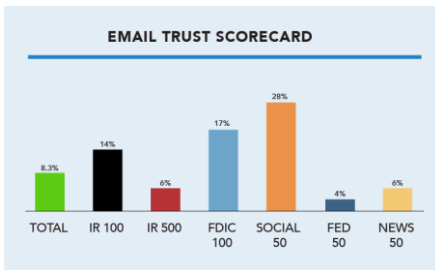
Why Care

"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

© 2014 All rights reserved. Online Trust Alliance (OTA)

Summary



- Passing Scores = SPF & DKIM @ TLD and DMARC

© 2014 All rights reserved. Online Trust Alliance (OTA)

© 2014. All rights reserved. Online Trust Alliance (OTA)

Highlights

- Only 8.3% have fully implemented SPF, DKIM and DMARC. on consumer facing brands.
- Email Authentication - Adoption of both SPF and DKIM rose across all sectors. Led by the IR100 with 88% adoption, the IR 500 showed the largest growth climbing from 56%.
- 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.
- DMARC – Adoption continues to rise in all sectors, but the growth must accelerate to help maximize consumer protection.
- 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.

© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN • INNOVATE • COLLABORATE

Highlights

- FDIC 100 - Highest failure rate caused by lack of email authentication support (especially DKIM at their TLD).
- Social 50 - Top social sites including social networking, dating, gaming and document sharing sites received the highest score for DMARC adoption (36%).
- Social led all segments in DKIM adoption at their TLD outpacing the FDIC and IR 500 by over 2:1
- Federal Government 50 - Consistently scored at the bottom of every email authentication adoption metric. Only 4% passed, due in part to only 20% adopting DKIM at their TLD and only 6% publishing a DMARC record.

© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN • INNOVATE • COLLABORATE

Why Care

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

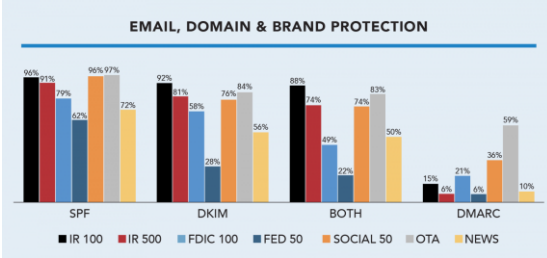
Josh Aberant, Twitter's Postmaster

© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN • INNOVATE • COLLABORATE

© 2014. All rights reserved. Online Trust Alliance (OTA)

Overview



© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN · INNOVATE · COLLABORATE

Trends – 5 Years of Growth

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%

© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN · INNOVATE · COLLABORATE

Trends Both - A Best Practice!

2014 DOMAIN & BRAND PROTECTION

BOTH DKIM AND SPF

	2010	2011	2012	2013	2014
IR 100	24.0%	42.0%	56.0%	76.0%	88.0%
IR 500	14.0%	23.0%	43.0%	56.0%	74.0%
FDIC 100	22.0%	23.0%	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%	44.0%	59.0%	69.0%	83.0%
News 50					50.0%

© 2014. All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN · INNOVATE · COLLABORATE

© 2014. All rights reserved. Online Trust Alliance (OTA)

TLD vs Subdomains - SPF

SPF ADOPTION

	2010 Top Level Domains	2011 Top Level Domains	2012 Top Level Domains	2013 Top Level Domains	2013 Any SPF	2014 Top Level Domains	2014 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%

© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN • INNOVATE • COLLABORATE

DKIM – 5 Year Growth

DOMAINKEYS IDENTIFIED MAIL - ADOPTION ANALYSIS

	2010 Any DKIM	2011 Any DKIM	2012 Any DKIM	2013 Any DKIM	2014 Any DKIM
IR 100	37.0%	55.0%	82.8%	87%	92%
IR 500	22.8%	33.4%	69.5%	65%	81%
FDIC 100	29.0%	34.4%	44.0%	50%	58%
Fed 50	4.0%	6.0%	18.0%	24%	28%
Social 50	-	52.0%	63.0%	74%	76%
OTA Members	22.0%	34.5%	57.1%	69%	84%
News 50	-	-	-	-	56.0%

© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN • INNOVATE • COLLABORATE

TLDs vs Subdomains - DKIM

DKIM ADOPTION

	2010 Any DKIM	2011 Any DKIM	2012 Any DKIM	2013 Top Level Domains	2013 Sub Domains	2013 Any DKIM	2014 Top Level Domains	2014 Sub Domains	2014 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%

© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN • INNOVATE • COLLABORATE

© 2014. All rights reserved. Online Trust Alliance (OTA)

DMARC

DMARC ADOPTION

	2012	2013	2014
IR 100	2.0%	5.0%	15.0%
IR 500	1.5%	3.0%	6.2%
FDIC 100	1.0%	13.0%	21.0%
Fed 50	0.0%	4.0%	6.0%
Social 50	18.5%	22.0%	36.0%
OTA Members	34.3%	43.8%	59.4%
News 50			10.0%

© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN · INNOVATE · COLLABORATE

DMARC - R/Q

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%

© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN · INNOVATE · COLLABORATE

Why Care

"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.

© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN · INNOVATE · COLLABORATE

© 2014. All rights reserved. Online Trust Alliance (OTA)

Transport Layer Security (TLS)

- Email is effectively plain text open for anyone to eavesdrop.
- TLS offer encryption of your message while it is “in transit”
- 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.
- Key features :
  - Encrypted Messages: 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: Uses of digital certs to authenticate the receiving servers.
- Opportunistic TLS is accomplished when used by both sending and receiving parties to negotiate a secured SSL/TLS session and encrypt the message.

© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN • INNOVATE • COLLABORATE

Lessons Learned

- Your mailing environment is dynamic.
- Requires operational discipline.
- Needs operations, marketing, IT and security to work together.
- You need to test and monitor.

© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN • INNOVATE • COLLABORATE

Recommendations

1. Adopt a holistic strategy 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 feedback and verify accuracy, and eventually to assert a “reject” or “quarantine” policy to receivers.

© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN • INNOVATE • COLLABORATE

© 2014. All rights reserved. Online Trust Alliance (OTA)

Recommendations

4. Implement inbound email authentication and DMARC to help 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. Continually monitor mail flows and keep records up to date. This includes DKIM key rotation and SPF record maintenance. Don't forget to monitor delegated domains
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.

© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN • INNOVATE • COLLABORATE

Tools & Resources

- Email Integrity Audit https://otalliance.org/emailaudit
- Online Trust Honor Roll https://otalliance.org/HonorRoll
- Charts https://otalliance.org/2014-email-integrity-audit-charts-and-tables#Email_Trust_Scorecard
- Testimonials https://otalliance.org/news-events/press-releases/industry-support-email-integrity-best-practices
- Email Security https://otalliance.org/resources/email-security
- 2014 Data Protection & Breach Readiness Guide https://otalliance.org/Breach.html

Craig Spiezle craigs@otalliance.org +1 425-455-7400

© 2014 All rights reserved. Online Trust Alliance (OTA)

OTA Online Trust Alliance
LEARN • INNOVATE • COLLABORATE

© 2014. All rights reserved. Online Trust Alliance (OTA)