
2016 Online Trust Audit Email Authentication Practices Deep Dive & Reality Check

July 20, 2016

Craig Spiezle
Executive Director
Online Trust Alliance

<https://otalliance.org/DMARC>



LEARN • INNOVATE • COLLABORATE

Industry Panel



Mike Jones

Director, Product Management, Agari



Rob Holmes

General Manager, Fraud Protection, Return Path



Alexander García-Tobar

CEO, ValiMail



Jeff Wilbur

VP Marketing, Iconix
VP Research, Online Trust Alliance

© 2016 All rights reserved. Online Trust Alliance (OTA)



Slide 2

LEARN • INNOVATE • COLLABORATE

Why Care?

SC Magazine > News > APWG report: Phishing surges by 250 percent in Q1 2016

Bradley Barth, Senior Reporter
May 25, 2016

APWG report: Phishing surges by 250 percent in Q1 2016

eSecurityPlanet > Network Security > Grand Ole Opry, Sprouts, Seagate Breached by Phishing Attacks

Share this content:



Grand Ole Opry, Sprouts, Seagate Breached by Phishing Attacks

The Anti-Phishing Working Group observed more phishing of 2016 than in any other. It began tracking data in its anti-cybercrime coalition's Trends Report. In keeping APWG reported that the websites it detected jumped percent between October

While a brief spike in phishing expected in December 21 holiday-themed phishing attacks surge of attacks came as 123,555 of which were identified in November 2016

Thousands of employees' W-2 tax forms were accessed by attackers.

By Jeff Goldman | Posted 10/12/16



Adrian Bridgewater
July 12, 2016

Business email compromise (BEC) netting billions for scammers

Share this content:



information was disclosed ex

"We believe that any person provided a Form 1099, the c

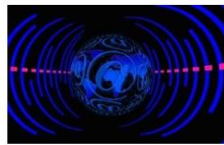
In a similar breach, Sprouts F

come from a senior executive employee provided the data

Just when you thought it was safe to go back into the ransomware littered expanses of cyberspace, a new acronym (and attack vector) surfaces.

So-called Business Email Compromise (BEC) is also sometimes called CEO fraud and it is gauged to be on the rise in 2016.

A family cousin to ransomware in a sense, BEC attacks take the form of spoofed emails targeted at medium to large businesses.



Don't get sucked into the scam

- Rise in phishing attacks, precision, variety of methods
- Entry point for >90% of breaches

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 3



LEARN • INNOVATE • COLLABORATE

Honor Roll Overview

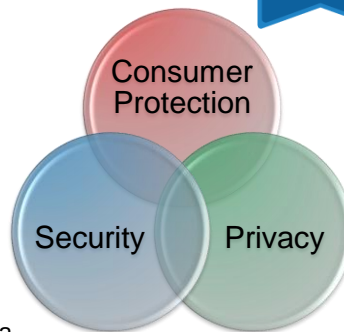


• Audit of 1,000 web sites

- Internet Retailer Top 500
- FDIC Banking 100
- Top 100 Consumer Services
- Top 100 News/Media
- Top 50 Federal Gov't
- OTA Members

• Scoring

- 100 baseline points for each category
- Weighted composite analysis, ~50 criteria
- Bonus points for emerging practices
- Penalty points for
 - Vulnerabilities, privacy practices, data loss incident & fines/settlement
- Honor Roll = 80% of total points, 55% or better in each category



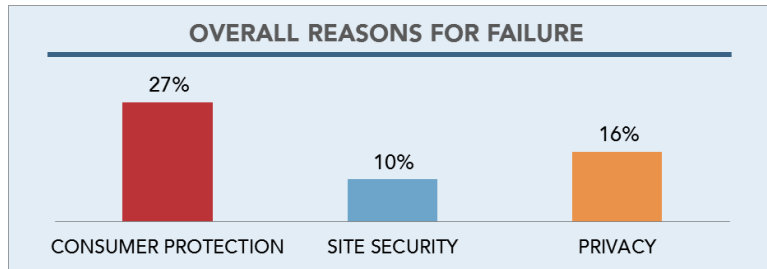
© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 4



LEARN • INNOVATE • COLLABORATE

Summary of Failures



- Primary cause(s) of failure –
 - Consumer protection – lack of DKIM at top-level domain
 - Site security – use of old ciphers, lack of latest protocol
 - Privacy – broad data sharing, many trackers that share data
- Sites can fail in more than one area

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 5



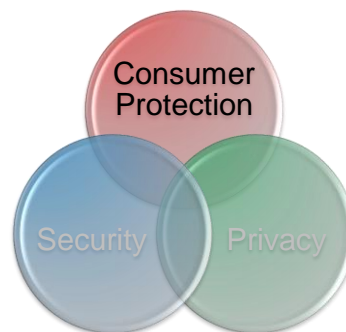
LEARN • INNOVATE • COLLABORATE

Consumer Protection

- Base points *Italics = new for 2016*
 - Email authentication
 - SPF and DKIM at top-level and subdomains (*increased weight for TLD*)
 - DMARC record and policy
 - DMARC reject/quarantine
 - *Increased weight for reject*

- Bonus points
 - TLS for email
 - DNSSEC
 - IPv6

- Penalty points
 - Domain locking (not locked)
 - *Malvertising incident in last year*



- Can the app or website be spoofed, fooling a person to open/download an update, open an attachment or simply open an email with a drive-by exploit?
- Does the site or app exercise best practice to help prevent brand-jacking and domain abuse?

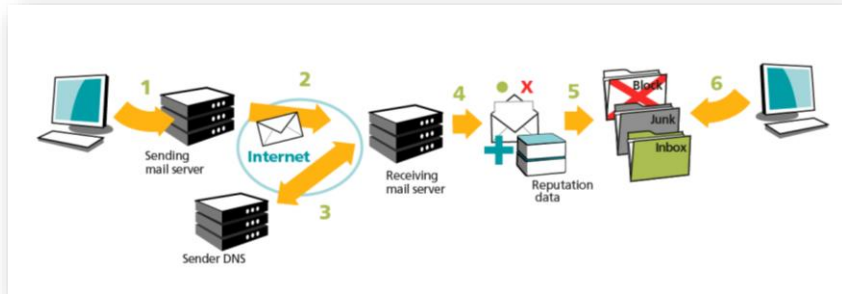
© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 6



LEARN • INNOVATE • COLLABORATE

Email Authentication Overview



- **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

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 7



LEARN • INNOVATE • COLLABORATE

Leveraging SPF and DKIM

SPF

- **Authenticates Message Path**
- Authorized senders in DNS

DKIM

- **Authenticates Message Content**
- Public encryption keys in DNS

DMARC



Consistency
A method to leverage the best of **SPF** and **DKIM**



Policy
Senders can declare how to process unauthenticated email



Visibility
Reports on how receivers process received email



Aggregated Insights
Telemetry into mail streams (RUA)



Failure & Spoofed email reports (RUF)

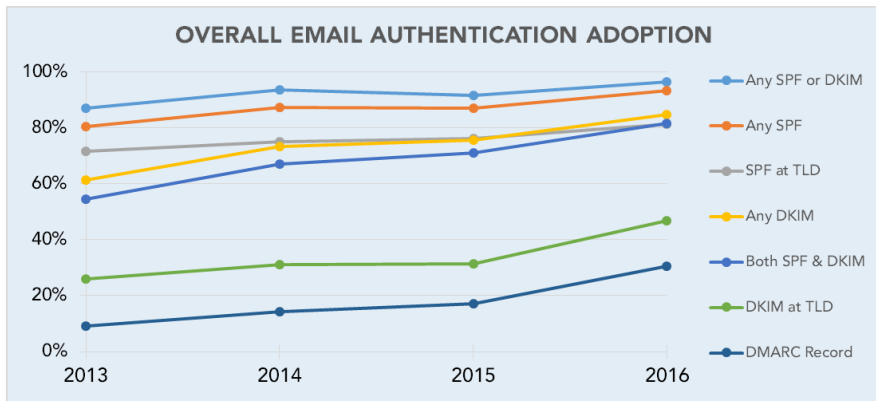
© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 8



LEARN • INNOVATE • COLLABORATE

Overall Adoption Trends



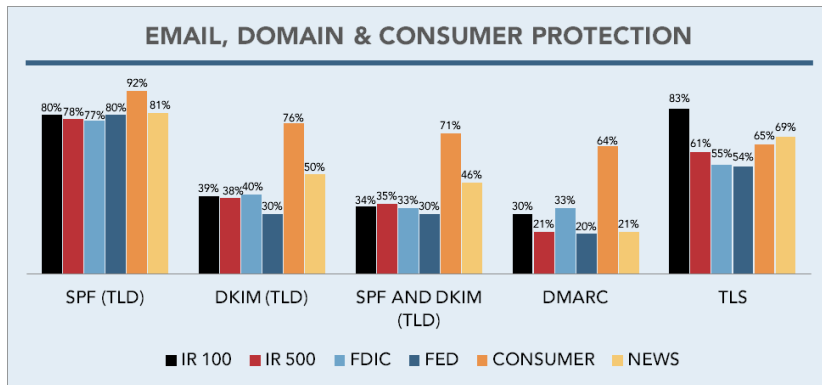
- Steady growth over time, exceeding 80% in many areas

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 9

LEARN • INNOVATE • COLLABORATE

2016 Snapshot by Sector



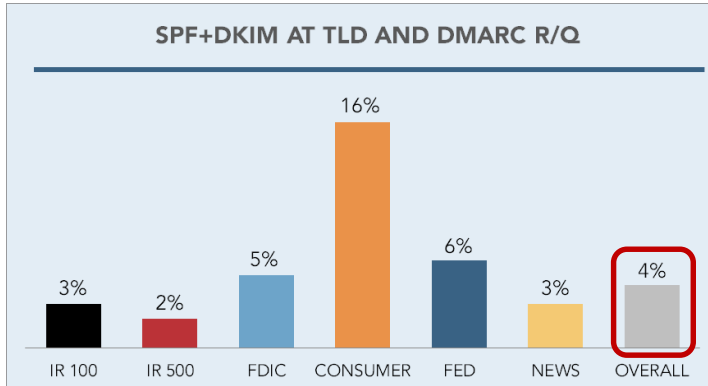
- Aids in protection from social engineering exploits including spearphishing & ransomware
- Overall adoption continues to rise, but still lacking at TLD

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 10

LEARN • INNOVATE • COLLABORATE

Reality Check



- Shows percent of organizations that support both SPF and DKIM at the TLD and have a DMARC record with a “reject” or “quarantine” policy
- Highlights need for increased focus across organizational “silos” to protect consumers, employees and brands

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 11



LEARN • INNOVATE • COLLABORATE

Top Sites Protecting Their Brand



© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 12



LEARN • INNOVATE • COLLABORATE

Stumbling Blocks



- Lack of awareness of value
- Risk tolerance
- Organizational disconnects / ownership
- Technical knowledge

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 13



LEARN • INNOVATE • COLLABORATE

Common Mistakes – SPF & DKIM



General - Incomplete authentication

SPF

- Overly broad references in the record
- Exceeding the limit of 10 DNS queries
- Typos or syntax errors (e.g., ipv4 instead of ip4)
- Use of “?all” or “+all”
- Referencing records that are missing or ambiguous
- Multiple SPF records for the same domain
- Not publishing SPF for subdomains (SPF does not propagate to subdomains)

```
agari.com. 1800 IN TXT "v=spf1
ip4:54.212.206.156 ip4:54.201.71.218
ip4:54.214.168.83 ip4:54.201.89.1
ip4:198.2.132.180 ip4:173.203.81.82
include:_spf.google.com
include:mail.zendesk.com
include:_spf.salesforce.com
include:mktomail.com -all"
```

DKIM

- Truncated DKIM records or bad characters in the key
- Key management (e.g., key rotation, key length, signing with the wrong key, etc.)
- Signing at the wrong point in the mail flow (e.g., signing at an internal hop before an outbound gateway modifies content)
- Email Service Providers adding a second DKIM signature

```
DKIM-Signature: v=1; a=rsa-
sha256; c=relaxed/relaxed;
d=valimail.com; s=google;
h=mime-version:in-reply-
to:references:from:date:
message-id:subject:to;
bh=LUZ... b=Yom...
```

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 14



LEARN • INNOVATE • COLLABORATE

Common Mistakes – DMARC

- Typos or syntax errors
 - Incorrect tag delimiters
 - Use of “_”
 - p=monitor instead of p=none
- Publishing a p=none with no RUA or RUF address
- Inappropriate use of sp=none
- Publishing unspecified or incorrect RUA /RUF domains/addresses
- Publishing multiple addresses in RUA/RUF tags
- Publishing a record without an understanding of what to do with feedback data

```
_dmarc.returnpath.com. 600 IN TXT
"v=DMARC1\; p=reject\; fo=1\;
rua=mailto:dmarc_agg@auth.returnpath.net\;
ruf=mailto:dmarc_afrr@auth.returnpath.net\;
rf=afrr\; pct=100"
```

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 15



LEARN • INNOVATE • COLLABORATE

Other Considerations

- Inbound protection
- Protecting “parked” or non-emailing domains
- Dealing with third parties
- Managing changes
- Low volume senders/departments
- Ongoing monitoring

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 16



LEARN • INNOVATE • COLLABORATE

What Now?

- Self-assessment – inventory, stakeholders, etc.
- Get help – OTA, industry resources
- Build a business case
- Implement and put processes in place

© 2016 All rights reserved. Online Trust Alliance (OTA)



Slide 17

LEARN • INNOVATE • COLLABORATE

Tools & Resources

OTA

- Email Security <https://otalliance.org/eauth>
- DMARC <https://otalliance.org/dmarc>
- Resources <https://otalliance.org/eauth/resources>
- TLS <https://otalliance.org/tls>
- Online Trust Audit & Honor Roll <https://otalliance.org/HonorRoll>
- Contact admin@otalliance.org +1 425-455-7400

OTA Members

- Agari <https://www.agari.com/resources/>
- Dmarcian <https://dmarcian.com/>
- Return Path <https://www.returnpath.com/StopEmailFraud/>
- ValiMail <http://www.valimail.com/>

© 2016 All rights reserved. Online Trust Alliance (OTA)



Slide 18

LEARN • INNOVATE • COLLABORATE

SPF Adoption

CONSUMER PROTECTION SPF ADOPTION						
	2013	2014	2015		2016	
	Top Level Domains	Top Level Domains	Top Level Domains	Any SPF	Top Level Domains	Any SPF
Internet Retailer Top 100	77%	78%	85%	94%	80%	96%
Internet Retailer Top 500	69%	75%	77%	89%	78%	93%
FDIC 100	62%	68%	73%	87%	77%	91%
Federal 50	60%	62%	70%	80%	80%	94%
Consumer 100	94%	94%	92%	92%	92%	95%
News 100	-	58%	62%	80%	81%	93%
OTA Members	98%	95%	100%	100%	100%	100%

- Overall SPF grew in most sectors (especially Fed, News)
- SPF at TLD grew in nearly all sectors – big jumps in News, Fed; dip in top 100 retailers
- Retailers, banks, Fed and News sites still have room for improvement

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 24



LEARN • INNOVATE • COLLABORATE

DKIM Adoption

CONSUMER PROTECTION DKIM ADOPTION						
	2013	2014	2015		2016	
	Top Level Domains	Top Level Domains	Top Level Domains	Any DKIM	Top Level Domains	Any DKIM
Internet Retailer Top 100	26%	33%	31%	93%	39%	96%
Internet Retailer Top 500	18%	27%	27%	83%	38%	89%
FDIC 100	30%	27%	30%	68%	40%	71%
Federal 50	22%	20%	28%	50%	30%	58%
Consumer 100	62%	56%	56%	78%	76%	90%
News 100	-	14%	16%	64%	50%	77%
OTA Members	58%	73%	78%	94%	93%	99%

- “Any DKIM” grew in all sectors, with large jumps in Consumer, News
- DKIM at TLD grew significantly in nearly all sectors, but still lags “Any DKIM” by 38% overall

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 25



LEARN • INNOVATE • COLLABORATE

DMARC Adoption

DMARC ADOPTION

	2013	2014	2015	2016	
	Record	Record	Record	Record	R or Q*
Internet Retailer Top 100	5%	15%	20%	30%	17%
Internet Retailer Top 500	3%	6%	8%	21%	14%
FDIC 100	13%	21%	24%	33%	24%
Federal 50	4%	6%	14%	20%	40%
Consumer 100	22%	36%	48%	64%	29%
News 100	-	10%	10%	21%	14%
OTA Members	44%	59%	77%	75%	25%

* As % of sites with a DMARC record

- Use of DMARC records grew in all sectors, led by retailers and Consumer, but is still a fraction of overall authentication levels
- Use of DMARC policy assertions also grew, but is still in early stages

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 26



LEARN • INNOVATE • COLLABORATE