Secure the Institutional Email Brand

Email authentication
DMARC case study: UW-Madison

Jesse Thompson
Technical Architect, Email Team Technical Lead
UW-Madison, Division of Information Technology

~30%

...of email sent to the world
from @wisc.edu is not authenticated

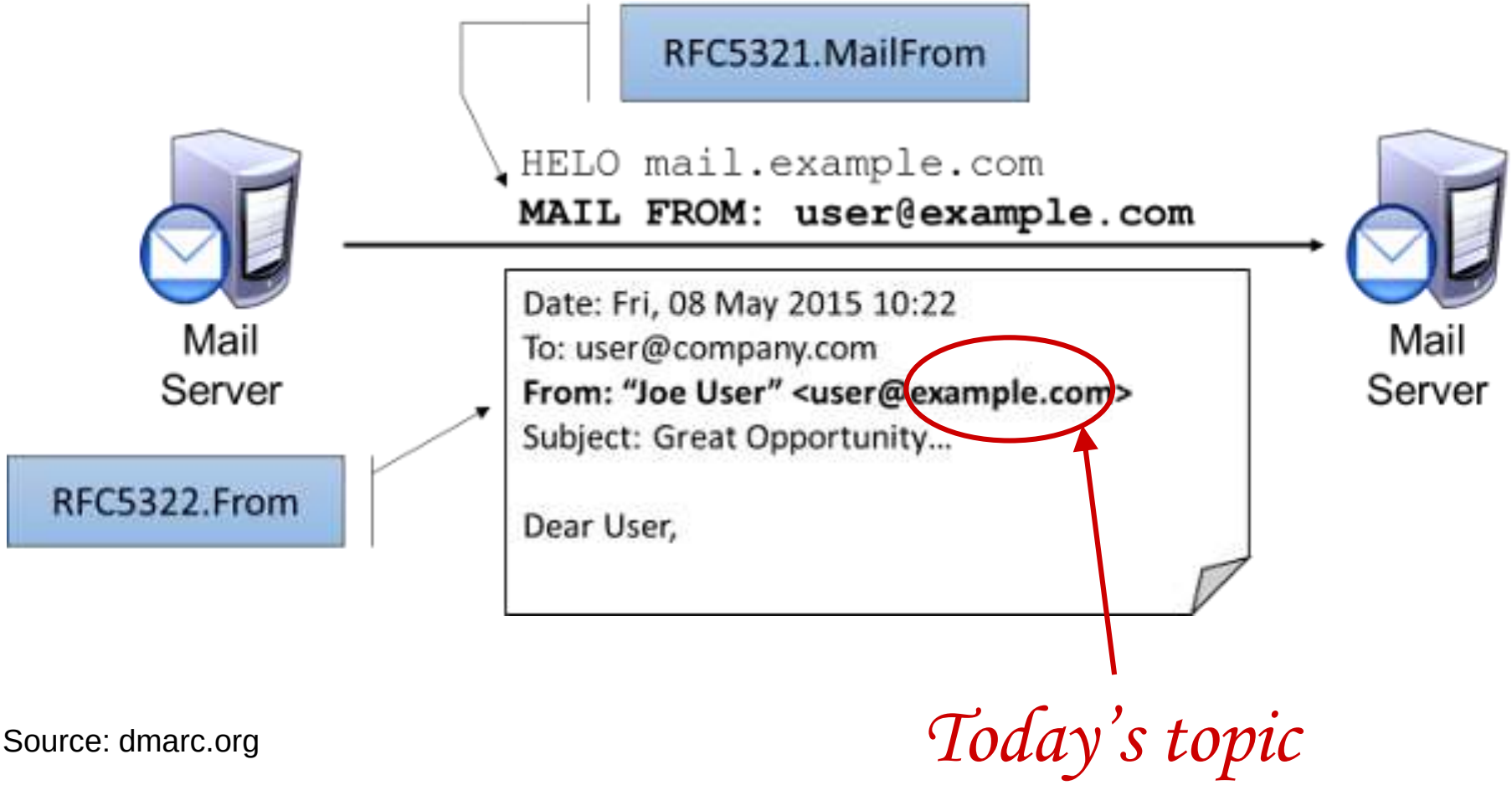
~10%

…of external email to internal users
from @wisc.edu is not authenticated

“91%

of phishing attacks are display name spoofs”

https://www.helpnetsecurity.com/2017/02/01/phishing-display-name-spoofs/



Source: dmarc.org

Today’s Takeaways

1) **Understand email authentication & DMARC**
2) Learn to measure how your email domains are being used and abused
3) How to progress towards compliance and a better future state

What is email authentication?

“Email authentication verifies that an email is actually from you or your business. Think of it like a digital signature: it protects your brand, identity and reputation. It's one of the most important steps you can take to improve your deliverability.”

~ Source: Campaign Monitor

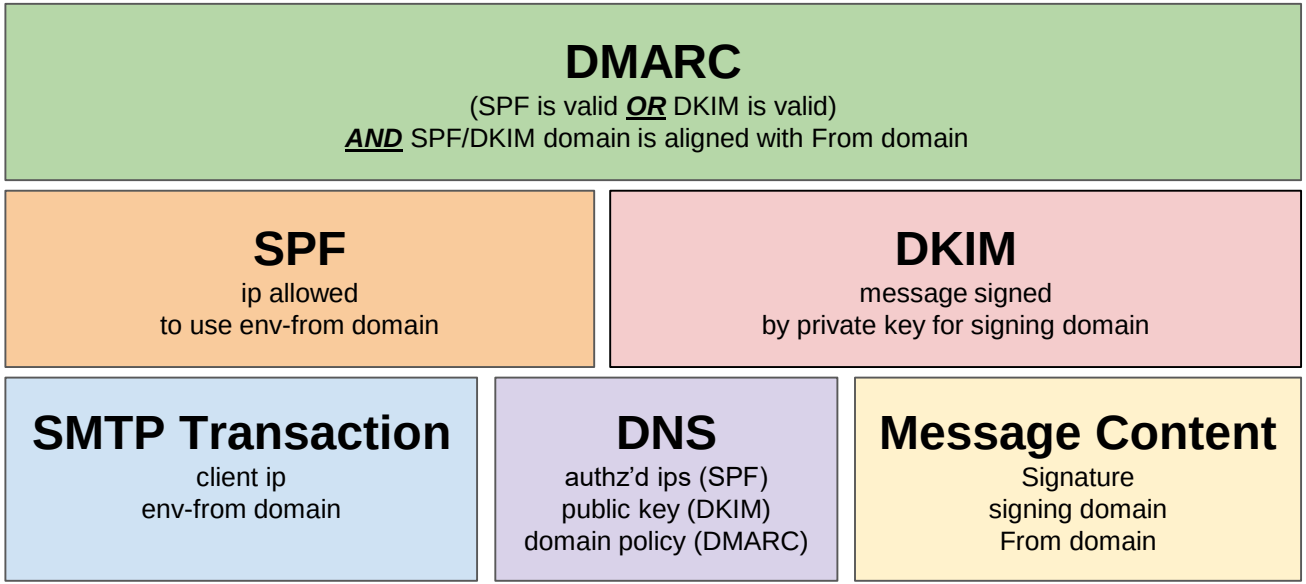
Why? ***Three perspectives***

1. Security - anti-fraud efforts
2. Marketing - simplified email delivery
3. Management - visibility and compliance

What is DMARC?

Domain-based **M**essage **A**uthentication **R**eporting and **C**onformance

1. **A**uthenticate **D**omain to **M**essage
2. **R**eporting:
   - Visibility
   - Feedback
3. **C**onformance:
   - Protection
   - Governance



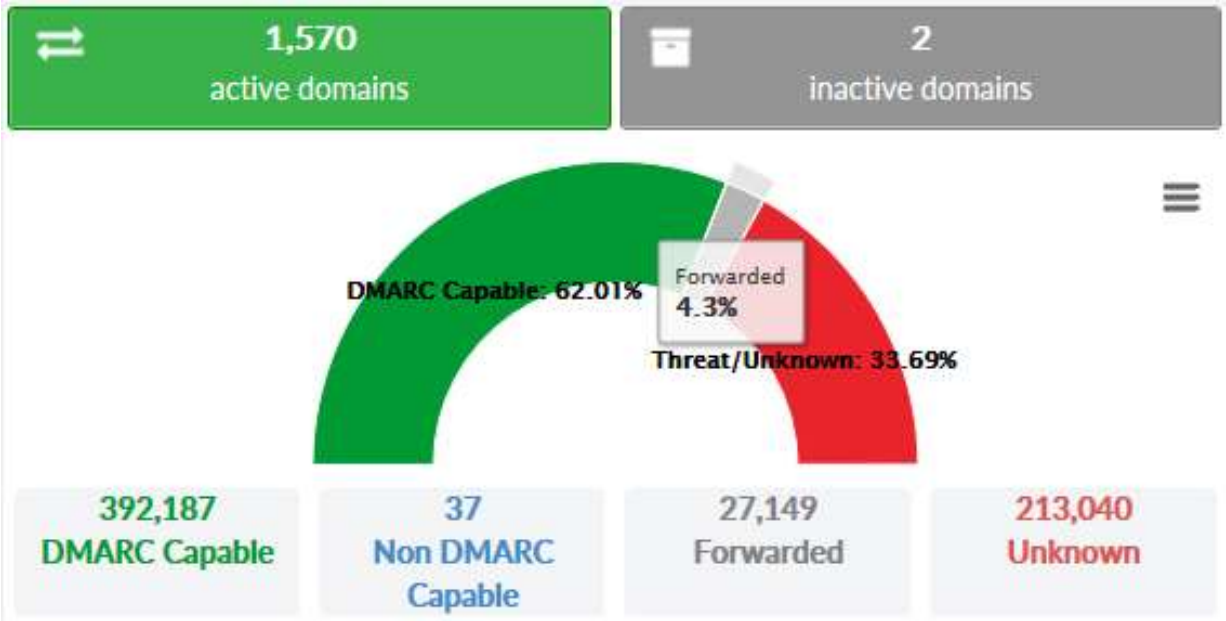
Qualities of email authentication

	Create a link between the domain and a message	Give anti-spam a trust-based model to prevent more types of phishing	Give the business a way to measure and govern the use of its domains
SMTP	No	No	No
S/MIME	Partial	No	No
SPF	No	Partial	No
DKIM	Partial	No	No
DMARC	**Yes**	**Yes**	**Yes**

Today’s Takeaways

1) Understand email authentication & DMARC
2) **Learn to measure how your email domains are being used and abused**
3) How to progress towards compliance and a better future state

Dmarcian.com (first glance at DMARC data)



30 Day Volume	2,014,865
Sending Domains	1
Potentially Fake Subdomains	582
Legit Sending Subs	1,569

Sources

(Last updated: June 30, 2017, 3:29 p.m.

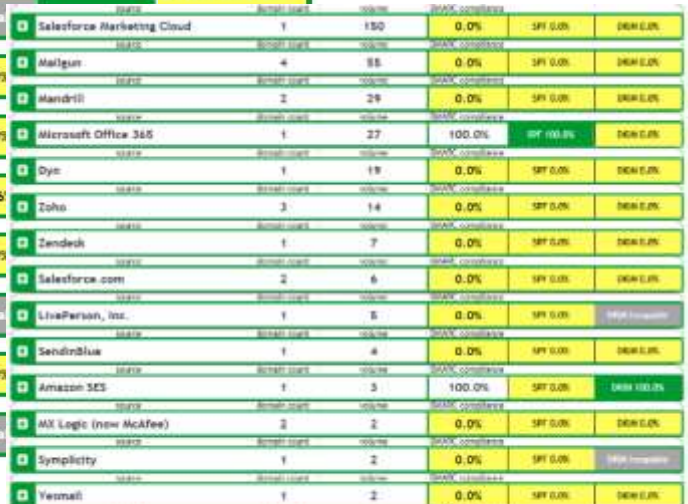
Showing DMARC Capable Sources that have delivered email for your domains in the past 7 days.

Refresh Data

Showing Data for All Domains

source	domain count	volume	DMARC compliance		
SPF-Identified Servers	768	460,362	89.85%	SPF 89.85%	DKIM 3.64%
Related Servers	128	33,834	0.0%	SPF 0.0%	DKIM 0.0%
Constant Contact, Inc.	9	18,655	0.0%	SPF Incapable	DKIM 0.0%
MailChimp					DKIM 0.0%
Emma					
MessageGears					

source	domain count	volume	DMARC compliance		
HubSpot, Inc.	1	4,275	0.0%	SPF 0.0%	DKIM 0.0%
Campaign Monitor	4	2,445	95.54%	SPF Incapa	
CASHNet (Higher One)	23	1,233	0.0%	SPF 0.0	
GetResponse	1	1,129	0.0%	SPF 0.0	
Qualtrics LLC	2	927	0.86%	SPF 0.86	
SendGrid, Inc.	4	302	0.0%	SPF 0.0	
iContact	2	300	10.0%	SPF Incapa	
Google, Inc.	3	164	0.0%	SPF 0.0	
Blackbaud, Inc.	2	157	0.0%	SPF Incapa	



source	domain count	volume	DMARC compliance		
SPF-Identified Servers	768	460,362	89.85%	SPF 89.85%	DKIM 3.64%
			413,643/460,362 messages	413,637/460,362 messages	16,752/460,362 messages

Notes on coverage and capabilities | Export domains as CSV

Show 10 entries

DMARC/From: domain	Message count	DMARC	SPF	DKIM	View in Detail Viewer
wisc.edu	246983	94%	94%	0%	
union.wisc.edu	25798	99.3%	99.3%	0%	
explore.wisc.edu	16705	99.98%	99.98%	99.98%	
cae.wisc.edu	13782	78%	78%	0%	
lists.wisc.edu	11539	94%	94%	0%	
uc.wisc.edu	8046	99.1%	99.0%	0%	
doit.wisc.edu	7472	98%	98%	0%	
admissions.wisc.edu	6813	99.90%	99.90%	0%	
waisman.wisc.edu	5597	98%	98%	0%	

From: Domain	IP	PTR	Country	Messages	Policy Applied	Override Reason	DKIM			SPF		
							DMARC	Raw	d=	DMARC	Raw	Domain
explore.wisc.edu	129.145.17.217	mail01.explore.wisc.edu		16722	None	none	aligned	pass	explore.wisc.edu	aligned	pass	explore.wisc.edu
explore.wisc.edu	129.145.17.217	mail01.explore.wisc.edu		1	None	none	aligned	pass	explore.wisc.edu	fail	temperror	explore.wisc.edu
explore.wisc.edu	144.92.197.141	wmauth1.doit.wisc.edu		1	Quarantine	forwarded	fail	fail	explore.wisc.edu	fail-unaligned	pass	wisc.edu

source	domain count	volume	DMARC compliance
Related Servers	128	33,834	0.0%

Notes on coverage and capabilities | Export domains as CSV

1/33,834 messages

Show 10 entries

DMARC/From: domain	Message count	DMARC	SPF	DKIM
icecube.wisc.edu	12040	0%	0%	0%
athletics.wisc.edu	6183	0%	0%	0%
wecan-help.education.wisc.edu	3516	0%	0%	0%
wisc.edu	2112	0%	0%	0%
nmrfam.wisc.edu	1878	0%	0%	0%
news.wisc.edu	1468	0%	0%	0%
wvdl.wisc.edu	1099	0%	0%	0%
cdr.wisc.edu	769	0%	0%	0%
uhs.wisc.edu	639	0%	0%	0%

Related Servers: Absent any email authentication results, email sources can sometimes be related to an email stream if external factors are considered such as *server reverse names and network ownership*.

Qualtrics LLC

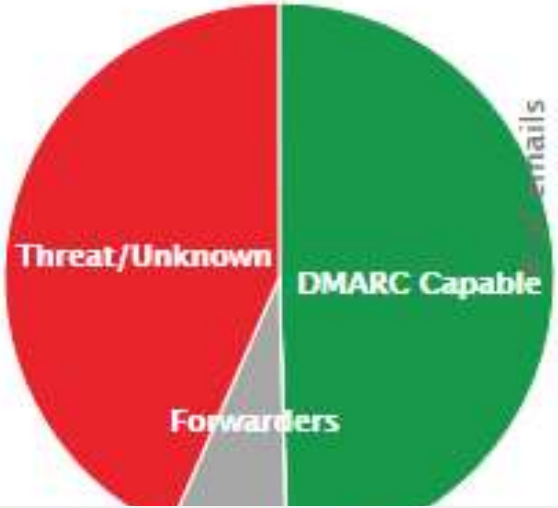
*.qemailserver.com 1

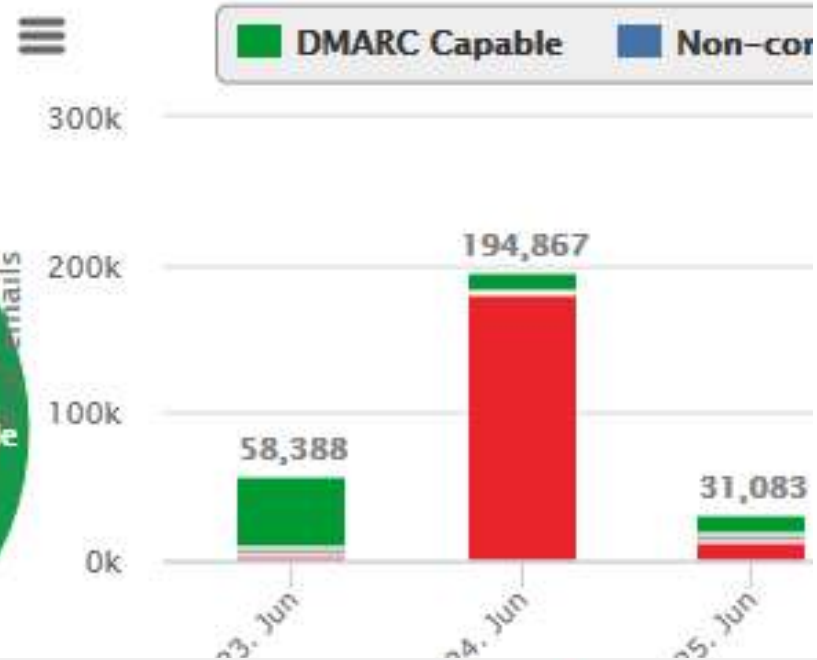
Show 10 entries

From: Domain	IP	PTR	Country	Messages
wisc.edu	162.247.217.54	smtp4.co1.qemailserver.com		387
wisc.edu	162.247.218.54	smtp4.az1.qemailserver.com		179
wisc.edu	162.247.217.52	smtp2.co1.qemailserver.com		178
wisc.edu	162.247.218.53	smtp3.az1.qemailserver.com		171

DKIM			SPF		
DMARC	Raw	d=	DMARC	Raw	Domain
fail-unaligned	pass	qemailserver.com	fail	neutral	wisc.edu
fail-unaligned	pass	qemailserver.com	fail	neutral	wisc.edu
fail-unaligned	pass	qemailserver.com	fail	neutral	wisc.edu
fail-unaligned	pass	qemailserver.com	fail	neutral	wisc.edu
fail-unaligned	pass	qemailserver.com	fail	neutral	wisc.edu

Email Volume by Category





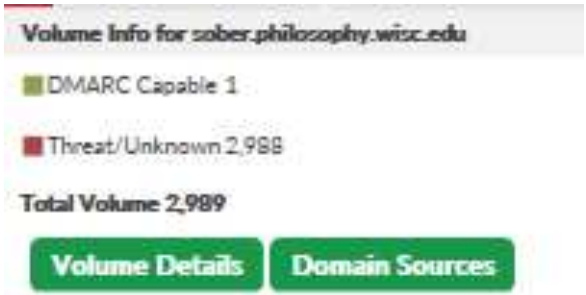
- *.xlhost.com
- *.nxdomain
- *.ediathol.com
- *.ec2-52-41-253-243.us-west-2.compute.amazonaws.com
- *.ec2-52-35-45-82.us-west-2.compute.amazonaws.com
- *.ec2-52-33-86-68.us-west-2.compute.amazonaws.com
- *.ec2-52-88-250-152.us-west-2.compute.amazonaws.com
- *.hostforweb.com
- *.portalwebhosting.com
- *.alsatary.net

Threat/Unknown sources are either fraudulent or need to be identified as legitimate.

- *.uchicago.edu
- *.charter.net
- *.emwd.com
- *.cornell.edu

Example hijacked web domain

☐	sober.philosophy.wisc.edu	⋮	☑ p=none (org)	✖ No SPF Record	✖ No Signing



Non-compliant Sources

*.educationpartners.com 1

Show 10 entries

Education Partners

From: Domain	IP	PTR	Country	Messages
wisc.edu	167.89.50.99	o1.em.educationpartners.com		39

DKIM			SPF			As Received By
DMARC	Raw	d=	DMARC	Raw	Domain	
fail-unaligned	pass	educationpartners.com	fail-unaligned	pass	em1.educationpartners.com	google.com

*.jumpforwardemail.com 1

Show 10 entries

JumpForward

From: Domain	IP	PTR	Country	Messages
wisc.edu	198.37.154.206	o2.email.jumpforwardemail.com		2

DKIM			SPF			As Received By
DMARC	Raw	d=	DMARC	Raw	Domain	
fail-unaligned	pass	sendgrid.net	fail-unaligned	pass	sendgrid.net	google.com (50%), Yahoo! Inc. (50%)

Forwarders

	volume
Gmail / Apps Forwarding	28,797
DigitalOcean Inc.	2,183
1&1 Mail & Media Inc.	2,105
OVH	1,114
Rackspace	537
GoDaddy	423
Yahoo	349
Proofpoint	264

SPF Domain	As Received By
lists.ucla.edu	google.com

source
Endurance International Group
Cisco IronPort Hosted MX
Fasthosts Internet Ltd
Servers that break DKIM signatures (or create spoofed signatu...
UPC (now Ziggo)
Comcast
Listbox
Liquid Web Inc

Today’s Takeaways

1) Understand email authentication & DMARC
2) Learn to measure how your email domains are being used and abused
3) **How to progress towards compliance and a better future state**

Justify with ROI

Convince management that DMARC compliance is worth investing in the necessary organizational change

Take a 3-pronged approach to ROI justification to ensure all stakeholders are at the table

1) Security - anti-fraud efforts
2) Marketing - simplified email deliverability
3) Management - visibility and compliance

Metrics

Use the DMARC reports to measure things related to the ROI for stakeholders in Security, Marketing & Management

- Exact domain phishing (Threats/Unknown category)
    - Also try to measure the tangents: compromised accounts and lookalike domain phishing
- Reputation of the brand (Percentage of DMARC alignment)
    - Also try to measure the cost of procuring 3rd party email deliverability assistance
- Compliance with governance policies (Subdomain proliferation and use)
    - Also try to measure the friction this imposes on the organization in terms of domain management inefficiencies and increased support costs

Change Management - Incentivize

Improve the ability for email senders within your organization to send compliant email

Clearly document best practices and governance policies

Provide guidance and example language for procurement and product evaluation

Offer tools and services that enable good practice by domain owners and email senders within our organization

Break down the problem

2500 domains / 365 days = 6.8 years

Plan of attack for large domain categories

- Primary domain
- Domains we host email (~400)
- New domains
- Domains used for marketing
- Servers sending email with their hostname
- Domains from DNS being coopted by spammers

Rough Plan

1) Enable DMARC reporting (p=none) and measure key metrics
2) Create DMARC compliant sub-domain(s) and document “best practices”
3) Build tools for departments and marketers to manage subdomains
4) Identify non-compliant senders using existing domains
    a) Backfill their IPs into SPF
    b) Switch them to use SMTP relay / submission service and/or DKIM-sign messages
    c) Ask them to switch the domain used in the “From”
5) Adjust Hostmaster “new domain” procedures to use restrictive SPF/DMARC

Today’s Takeaways

1) Understand email authentication & DMARC
2) Learn to measure how your email domains are being used and abused
3) How to progress towards compliance and a better future state

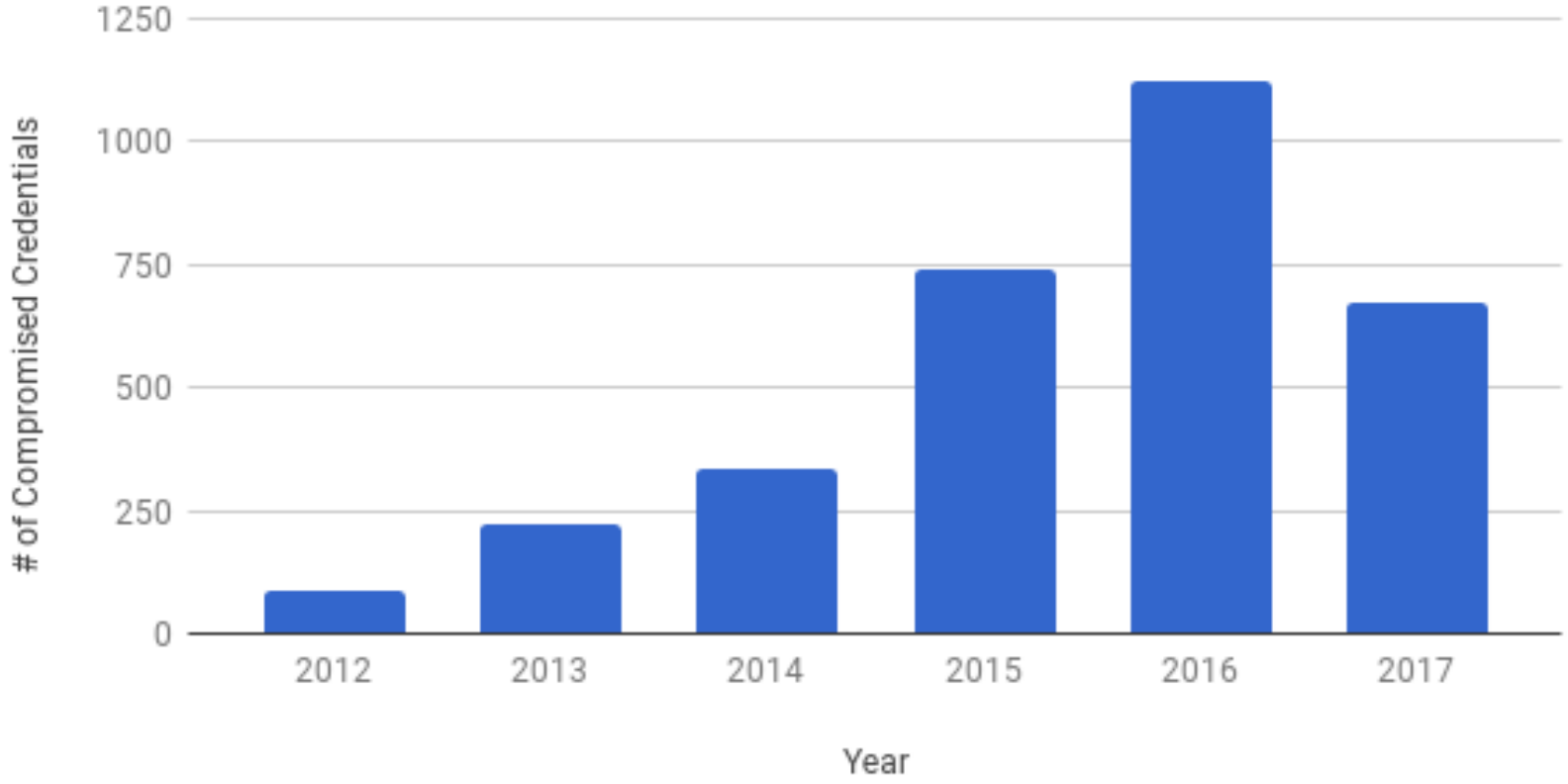
Thank you!

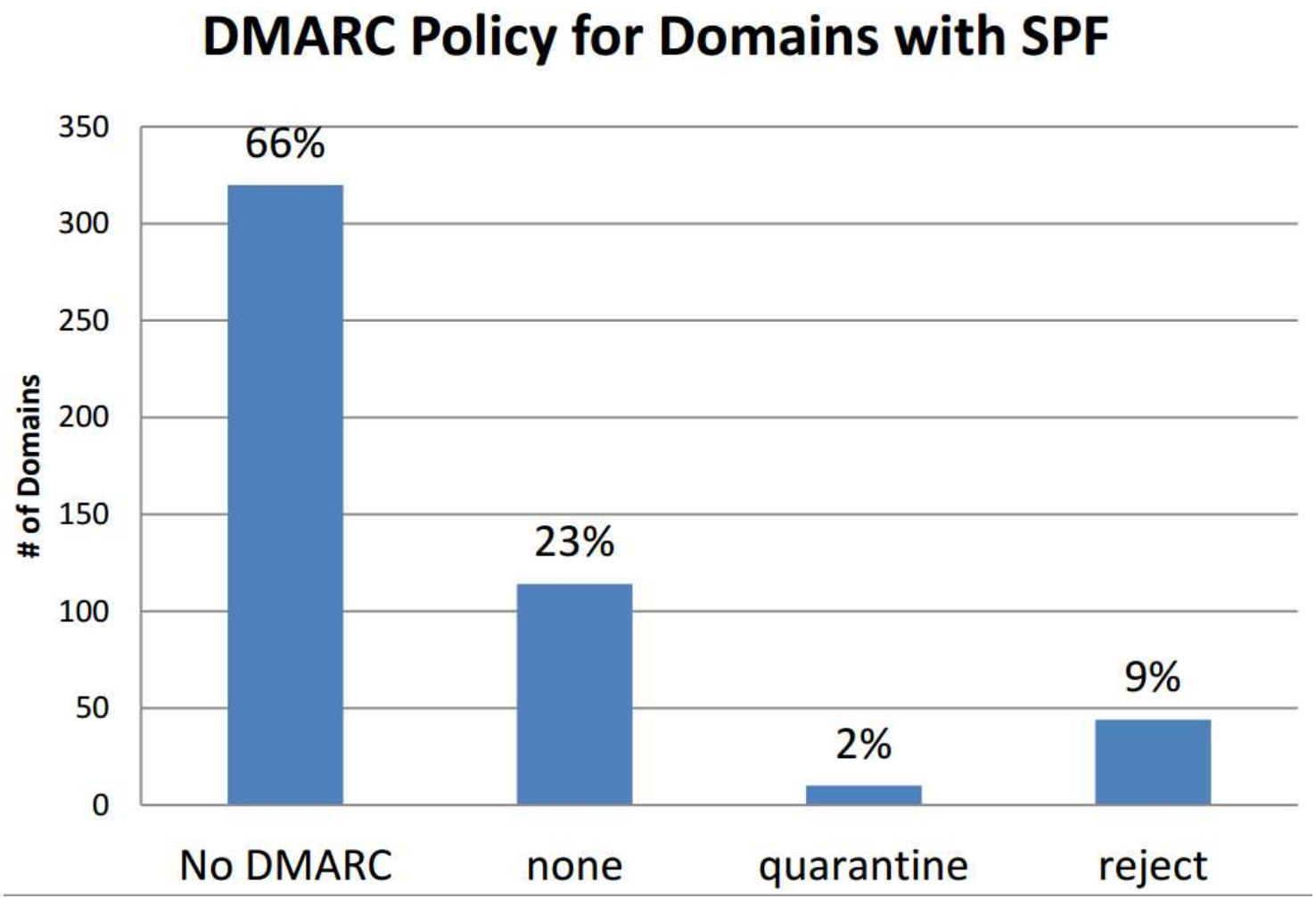
Q & A

Jesse Thompson
jesse.thompson@wisc.edu
@zjt

Bonus Slides

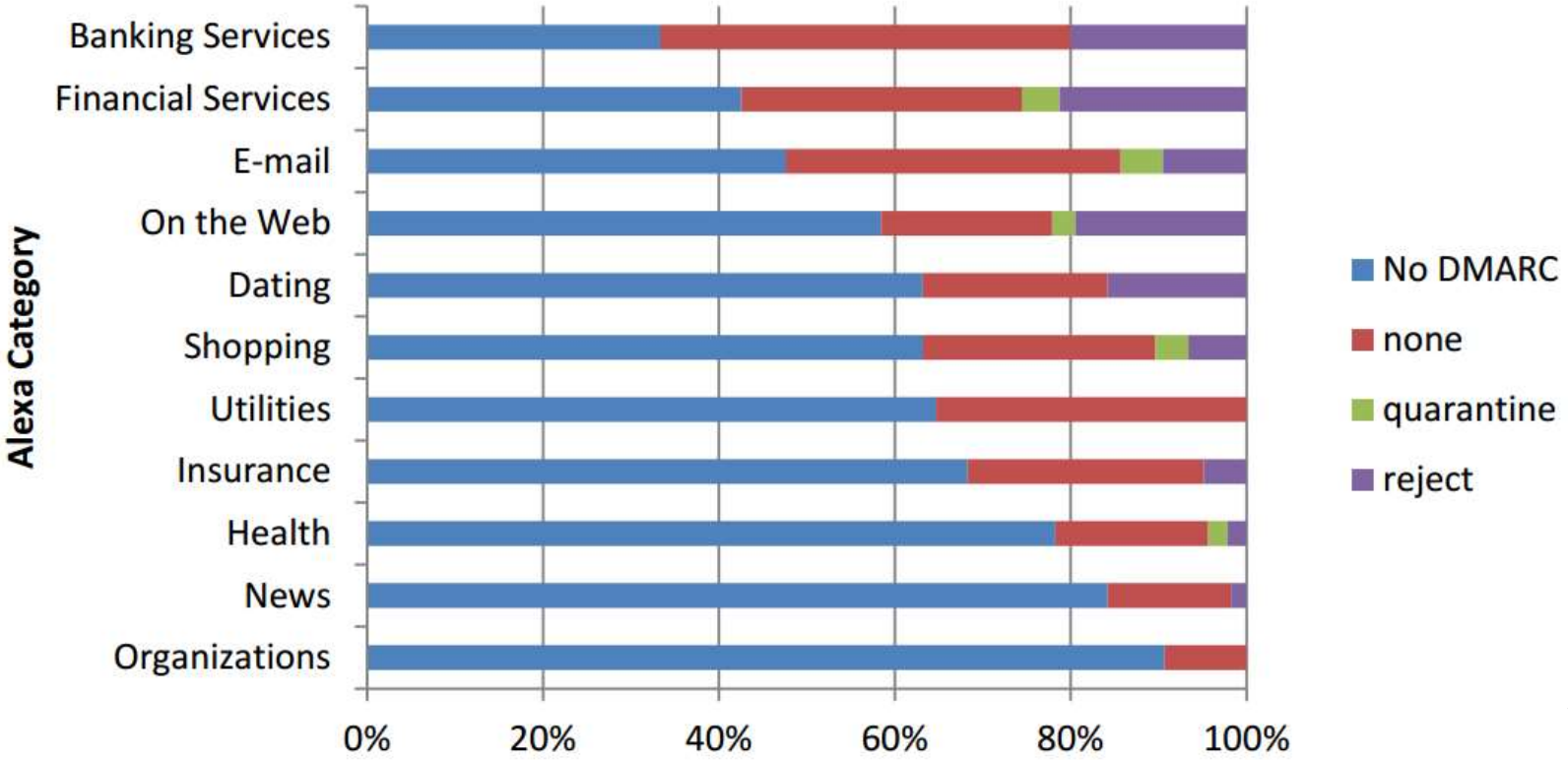
Number Of Detected Compromised Credentials Used To Breach The UW-Madison Enterprise Email Service (by Year)




DMARC Policy for Domains with SPF
# of Domains
350
300
250
200
150
100
50
0
66%
23%
2%
9%
No DMARC
none
quarantine
reject

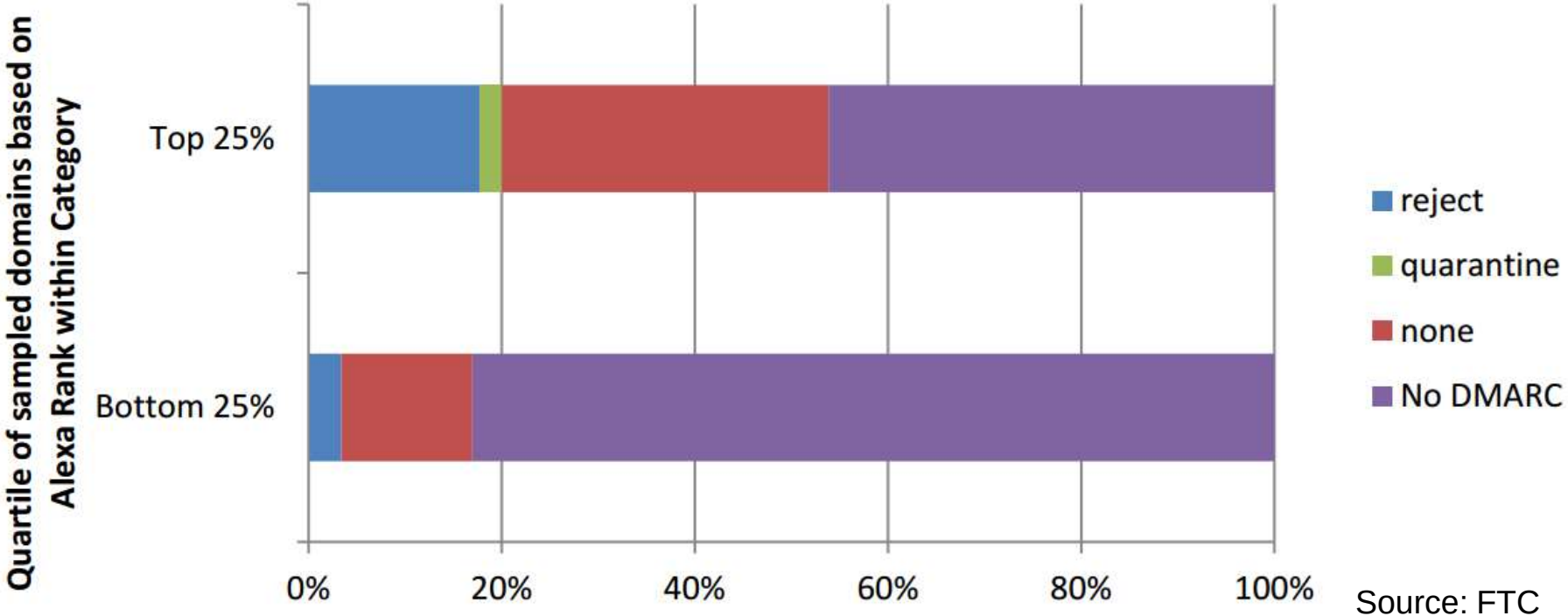
Source: FTC

DMARC Policy for Domains with SPF by Category



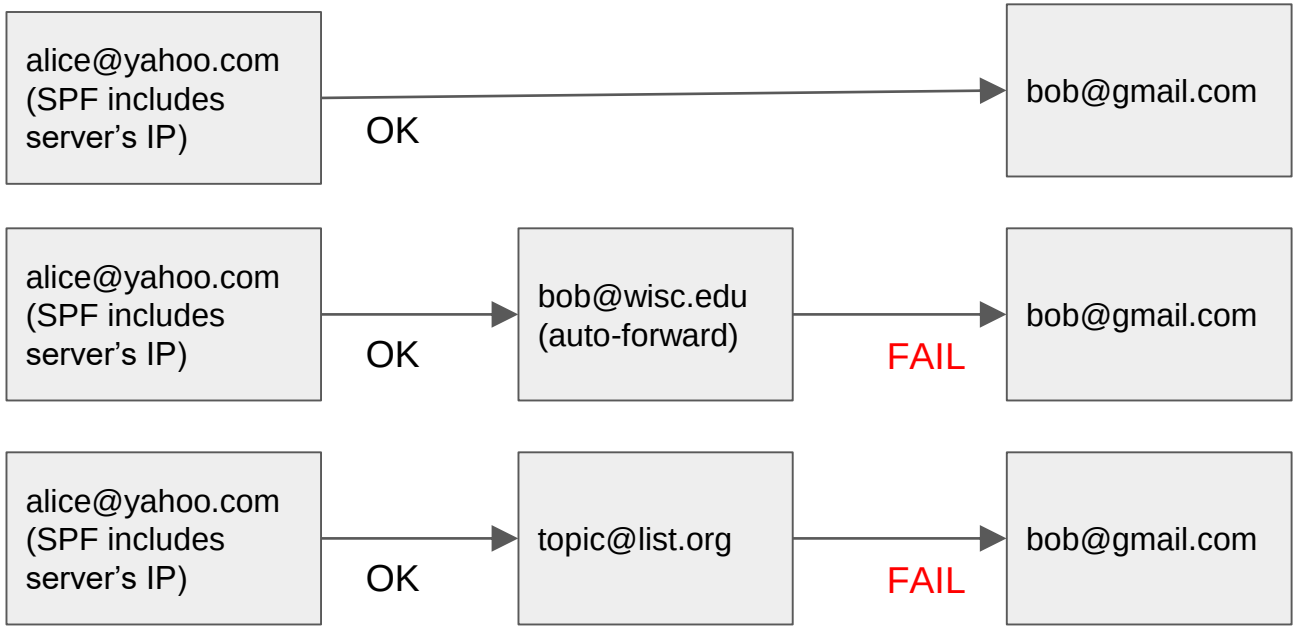
Source: FTC

DMARC Policy for Domans with SPF by Popularity



Source: FTC

Forwarding breaks SPF



Example SPF

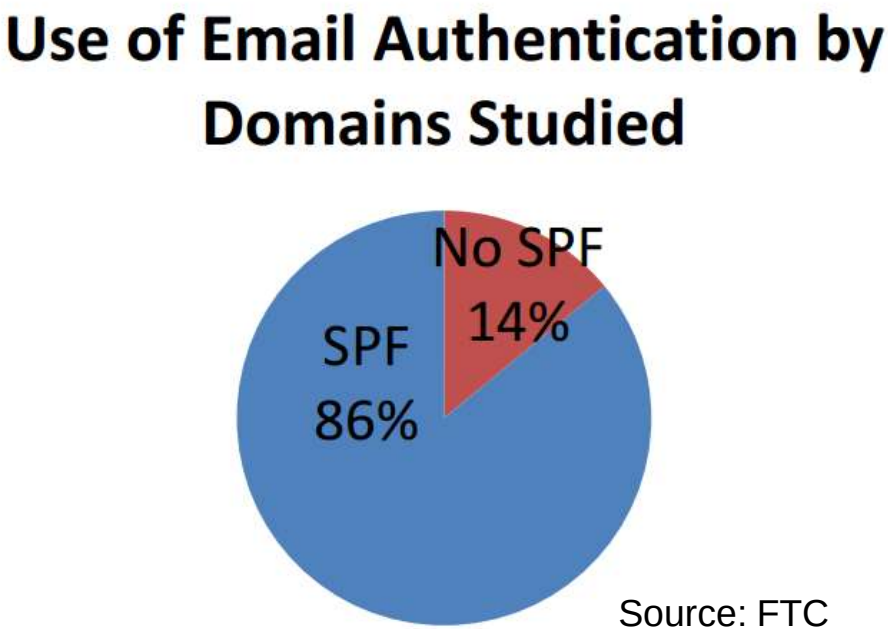
A random example that exceeds the DNS lookup limit:

% nslookup -type=TXT some.edu
redacted.edu text = "v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 ip4:3.4.5.6
include:_spf.google.com include:servers.mcsv.net
include:_spf.academicworks.com include:spf.dynect.net
include:spf.protection.outlook.com include:sharepointonline.com -all"

SPF adoption

Domain spoofing still exists, so how do you explain this stat?

- Published records are broken
  - e.g. DNS lookup limits
- Published policies are not strict
  - “?all” or “~all” instead of “-all”
- Strict policies are not actually enforced by receiving servers
  - Which means that SPF is not a



Source: FTC

Example DKIM

Look at the message headers…

DKIM-Signature: v=1; q=dns/txt; a=rsa-sha256; c=relaxed/relaxed; s=***1000073432***; d=***auth.ccsend.com***;
h=date:mime-version:subject:X-Feedback-ID:message-id:**from**:reply-to:list-unsubscribe:to;
bh=1VUj...fUsk=
From: Wisconsin Union <membership@**union.wisc.edu**>

Receiver looks up the key in DNS and validates the signature to the signing domain - ***not the From domain***!

% nslookup -type=txt 1000073432._domainkey.auth.ccsend.com
1000073432._domainkey.auth.ccsend.com text = "k=rsa; p=MIGfM...DAQAB"

DMARC | Performing SPF alignment process | comparing the sender identity in MAIL FROM field + FROM field

MAIL FROM: John@o365info.com

=

FROM: John@o365info.com

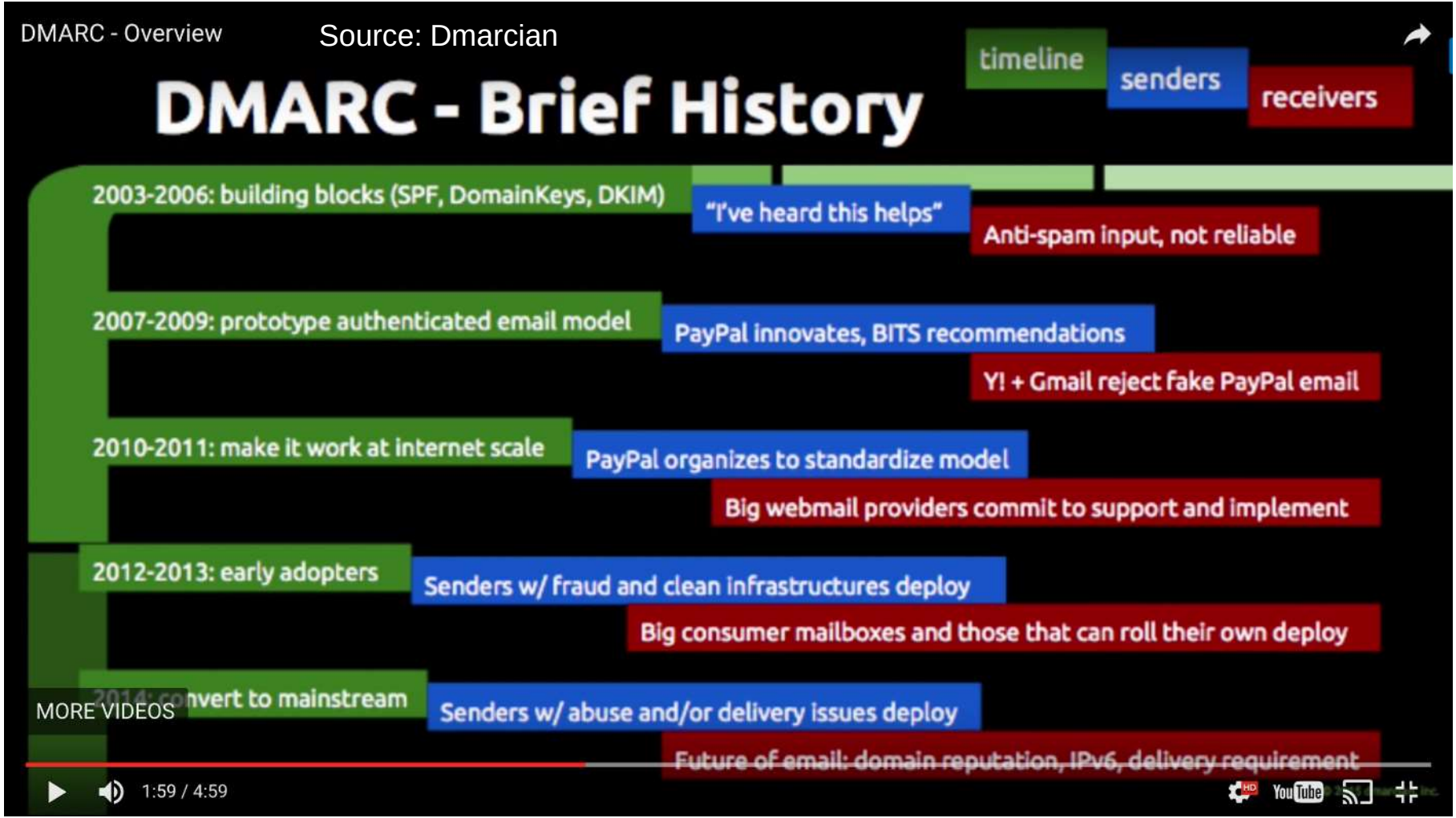
Source: o365info.com

This is a scenario in which the SPF alignment verification is "OK" (**dmarc=pass**)

This scenario considered as **Aligned**

DMARC - Overview

Source: Dmarcian



MORE VIDEOS

1:59 / 4:59

Enable DMARC Reports

% dig +short TXT _dmarc.wisc.edu

"v=DMARC1; p=none; rua=mailto:dmarc-reports@wisc.edu; ruf=mailto:dmarc-forensics@wisc.edu; fo=1;"