



Email Domain Security

Presenters:

India Greene

Joey Cusimano

Summary Upfront: SOA, MX, SPF, DKIM, DMARC

- www.mxtoolbox.com – visit and query your email domain name
- All implemented through domain name service (DNS) records
 - SOA: Source of Authority
 - Who is the authorized domain name service for your public email domain?
 - MX: Mail Exchange
 - Where do I send email to your domain?
 - SPF: Sender Policy Framework
 - What are your authorized email server IP addresses?
 - DKIM: Domain Key Identified Mail
 - What is your public key so I can send you encrypted email?
 - DMARC: Domain Based Authentication, Reporting and Conformance
 - What should you do when you receive my emails?

stacs.net

SOA Lookup

soa:stacs.net

Find Problems

 soa

Type	Domain Name	Primary NS	Responsible Email	TTL
SOA	stacs.net	ns-525.awsdns-01.net	awsdns-hostmaster@amazon.com	15 min

mx:stacs.net

Find Problems

Solve Email Delivery Problems

 mx

Microsoft Outlook.com now requires DMARC - [Get SPF, DKIM and DMARC setup and maintain compliance with Delivery Center](#)

Pref	Hostname	IP Address	TTL	
10	mail.groupassure.net	23.21.187.245 Amazon.com, Inc. (AS14618)	24 hrs	Blacklist Check SMTP Test

spf:stacs.net

Find Problems

Solve Email Delivery Problems

spf

Microsoft Outlook.com now requires DMARC - [Get SPF, DKIM and DMARC setup and maintain compliance with Delivery Center](#)

```
v=spf1 ip4:23.21.187.245 -all
```

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	ip4	23.21.187.245	Pass	Match if IP is in the given range.
-	all		Fail	Always matches. It goes at the end of your record.

dmARC:stacs.net

Find Problems

Solve Email Delivery Problems

dmARC

Microsoft Outlook.com now requires DMARC - [Get SPF, DKIM and DMARC setup and maintain compliance with Delivery Center](#)

```
v=DMARC1;p=quarantine;ruf=mailto:postmaster@stacs.net
```

Microsoft Outlook.com now requires DMARC - [Get SPF, DKIM and DMARC setup and maintain compliance with Delivery Center](#)

```
v=DMARC1;p=reject;pct=100;rua=mailto:DMARC_Reports@icf.com,mailto:4313cd5434@rua.easydmarc.us;ruf=mailto:DMARC_Reports@icf.com,mailto:4313cd5434@ruf.easydmarc.us;ri=3600;fo=1
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	reject	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
pct	100	Percentage	Percentage of messages from the Domain Owner's mail stream to which the DMARC policy is to be applied. Valid value is an integer between 0 to 100.
rua	mailto:DMARC_Reports@icf.com,mailto:4313cd5434@rua.easydmarc.us	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.
ruf	mailto:DMARC_Reports@icf.com,mailto:4313cd5434@ruf.easydmarc.us	Forensic Receivers	Addresses to which message-specific failure information is to be reported. Comma separated plain-text list of DMARC URIs.
ri	3600	Reporting Interval	Indicates a request to Receivers to generate aggregate reports separated by no more than the requested number of seconds. Valid value is a 32-bit unsigned integer.
fo	1	Forensic Reporting	Provides requested options for generation of failure reports. Valid values are any combination of characters '01ds' seperated by ':'.

Agenda

- Overview of incidents involving email
- Review anti-spoofing controls for email
 - SPF
 - DKIM
 - DMARC
- Layered email security approach
- Q&A
- Demo

Background

- Recent incidents involving spoofed email
 - Spear Phishing: spoofed employee email to Off Mgr. to change direct deposit
 - Wire Fraud: spoofed Trustee email to Debtor Attorney with wire instructions
- Root Causes:
 - Spoofed email (From: Joey Cusimano <jc@xyz.net> - not stacs.net!)
 - Man-in-the-middle attacks on M365 w/wo MFA
- Prevention: What can I do?
 - Anti-email spoofing measures
 - Be clear about wire transfer acceptance or lack thereof, add to email signature

Anti-email Spoofing Measures

- SPF: Sender Policy Framework
- DKIM: Domain Key Identified Mail
- DMARC: Domain Based Authentication, Reporting and Conformance
- All implemented through domain name service (DNS) records

Helpful Tools

- MXToolBox.com

<https://www.mxtoolbox.com>

- DNS record checks: MX, SPF, DMARC, DKIM, and others
- Blacklisted status and monitoring
- Free blacklist domain monitor, weekly blacklist status

SuperTool Beta7

Lookup anything... **MX Lookup**

ABOUT THE SUPERTOOL!

All of your MX record, DNS, blacklist and SMTP diagnostics in one place.

If you already know exactly what you want, you can force a particular lookup (e.g. "blacklist: 127.0.0.2" will do a blacklist lookup)

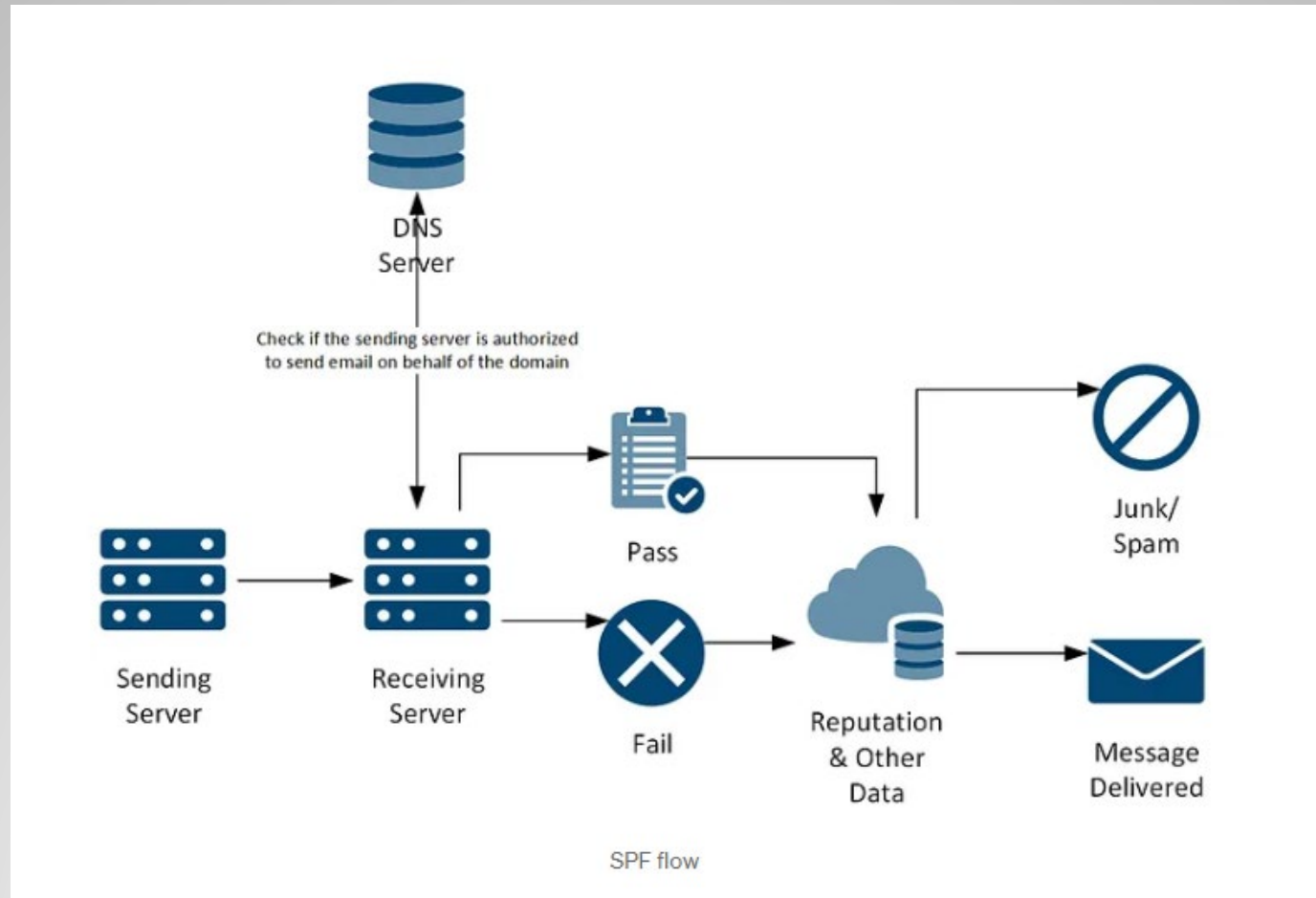
Command	Explanation
blacklist:	Check IP or host for reputation
smtp:	Test mail server SMTP (port 25)
mx:	DNS MX records for domain
a:	DNS A record IP address for host name
spf:	Check SPF records on a domain
txt:	Check TXT records on a domain
ptr:	DNS PTR record for host name
cname:	DNS canonical host name to IP address
whois:	Get domain registration information
arin:	Get IP address block information
soa:	Get Start of Authority record for a domain
tcp:	Verify an IP Address allows tcp connections
http:	Verify a URL allows http connections
https:	Verify a URL allows secure http connections
ping:	Perform a standard ICMP ping
trace:	Perform a standard ICMP trace route
dns:	Check your DNS Servers for possible problems New!

- MX Lookup
- Blacklist Check
- DNS Lookup
- Test Email Server
- Reverse Lookup
- Whois Lookup
- DNS Check
- SPF Record Lookup
- DKIM Lookup
- DMARC Lookup
- AAAA Lookup
- SRV Lookup
- DNSKEY Lookup
- CERT Lookup
- LOC Lookup
- IPSECKEY Lookup
- Domain Health
- ASN Lookup
- RRSIG Lookup
- NSEC Lookup
- DS Lookup
- NSEC3PARAM Lookup

SPF

- Sender Policy Framework (SPF) identifies the IP Addresses of mail servers authorized to send email for a given domain
- If the IP address of the domain the email came from is not in the authorized list, SPF check will fail

SPF: Email Delivery Diagram



Source: <https://medium.com/@pendraggon87/short-primer-on-spf-dkim-and-dmarc-9827eb2f359d>

SPF: Creating the DNS Record

- In your domain's DNS service
 - AWS Route53 shown, other common registrars include GoDaddy, Bluehost, web.com
- A list of IP addresses of authorized email servers for the domain is added as a SPF TXT record

☐	Record name ▼	Type ▼	Value/Route traffic to
☐	stacs.net	TXT	"v=spf1 ip4:23.21.187.245 -all"

SPF: Creating the DNS Record

- Microsoft 365 hosted mail servers use a specific TXT record you can add to your other DNS records:

`v=spf1 include:spf.protection.outlook.com -all`

- Alternatively, exchange servers or other mail servers (cloud or on-premise) need the mail server's public IP address instead:

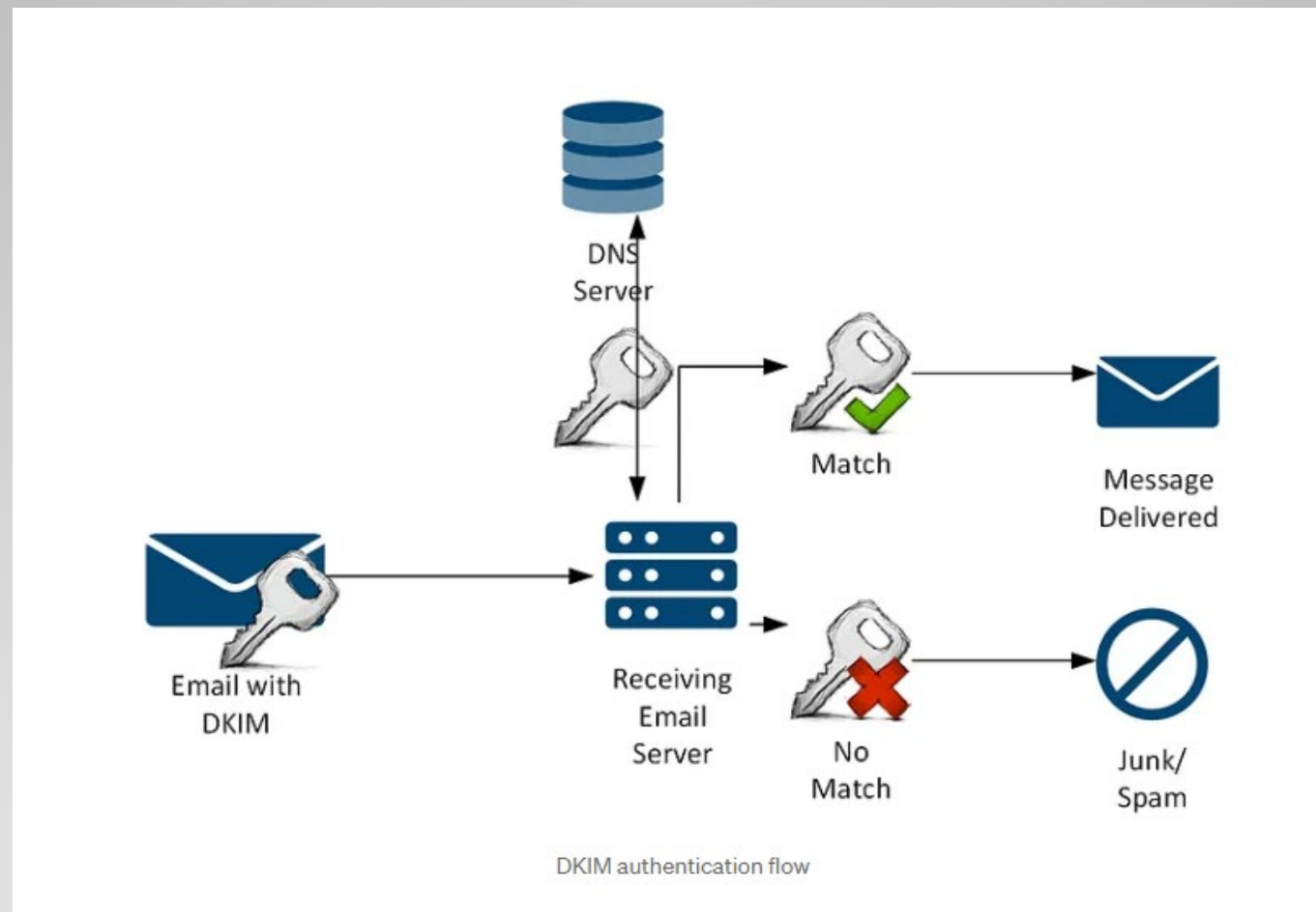
`v=spf1 ip4:76.0.1.230 ip4:76.0.1.231 -all`

- “-all” tells receiving servers to reject messages that fail SPF check

DKIM

- DomainKeys Identified Mail
 - Uses public-key cryptography to ensure integrity and authenticity
 - Public key is added as TXT record for the domain
 - Private key is used to sign emails as they are sent from the server
 - Recipient uses public key from DKIM DNS record to verify email came from the authentic domain

DKIM: Email Delivery Diagram



Source: <https://medium.com/@pendraggon87/short-primer-on-spf-dkim-and-dmarc-9827eb2f359d>

DKIM: Creating the DNS Record

- Hosted service providers sometimes provide tools (potentially at a cost)
 - AWS Easy DKIM (for Amazon Simple Mail Service)
 - Microsoft 365 Defender, Exchange Online Protection

Type	Name *	TTL
TXT	20200308._domainkey	Auto
Content *		
<pre>v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArmHfIKqja+NzjjfnNYMjl8tw4xjztaj5KxJFOzH9ttPIQh1RbKXhWvwWxZWHRiNR QwilZn02a2MXu55HpCaTD8lSmsJbTkcmF1xskTkILQWlyjSOfiH02hAus48H3tiXuN8K0iaX/OU75mfk9QrgPWWZB4LtJBXh4u1KnVllyLKTXuD P838KCK/41u0w6VVr9NTgJY+mFDfDxIsCY9Q6oRM0oyLL0pHtGXw</pre>		

Example DKIM TXT record. Source: <https://www.linuxbabe.com/redhat/set-up-opendkim-centos-8-rhel-8>

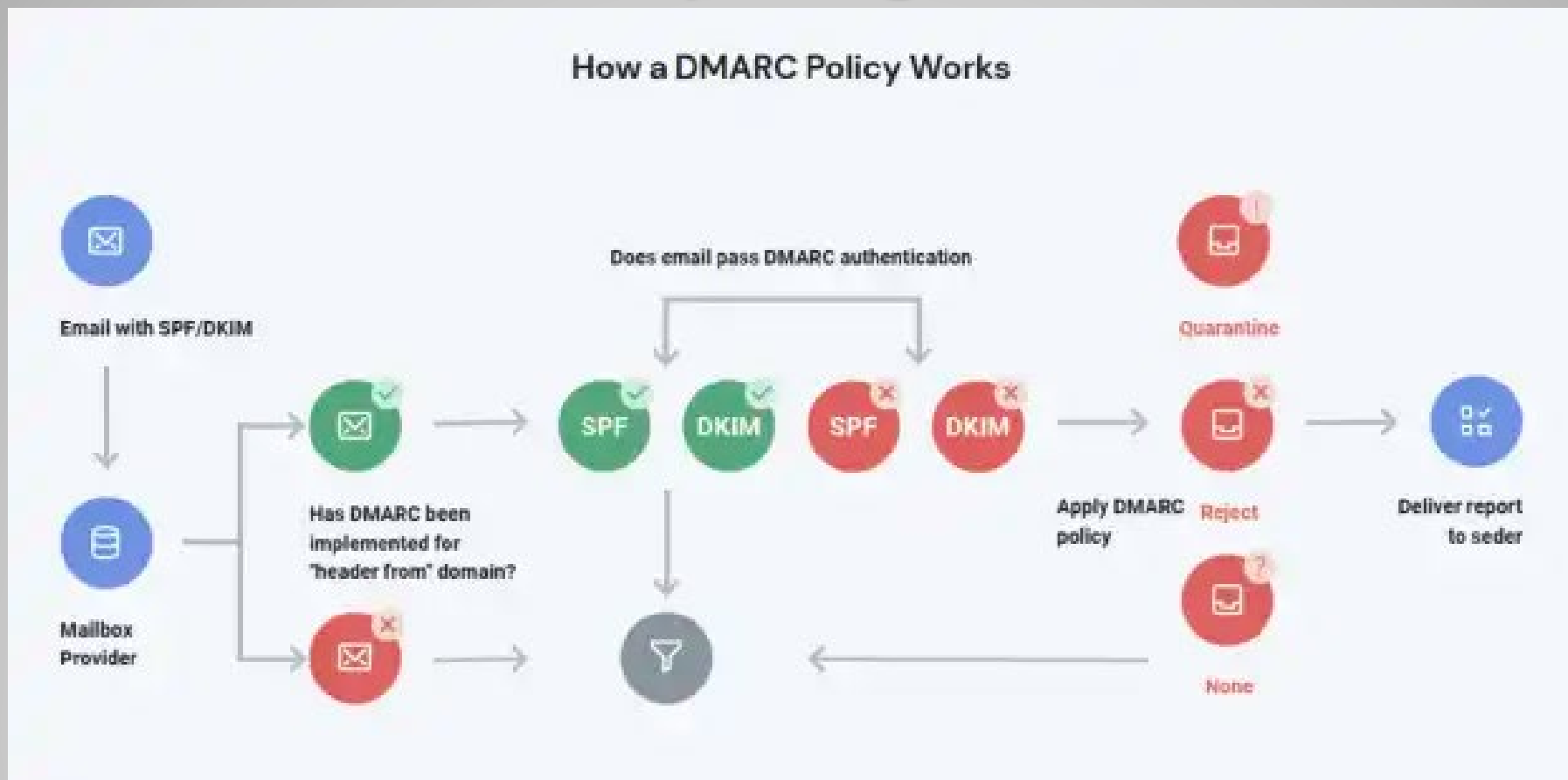
DKIM: Configure Mail Server with Private Key

- DKIM requires configuring mail service to use private key
 - Hosted mail services usually do this automatically
- If using your own mail server, DKIM private key will need to be generated and installed into your mail service
- This process will vary by email service and operating system

DMARC

- Domain Based Authentication, Reporting and Conformance (DMARC)
 - Check if your domain is being used to send spam
 - Instruct receiving servers what to do with email from my organization that fail SPF or DKIM (none, quarantine, reject)
 - Minimizes blacklisting of your email domain
- Receive delivery reports from recipient mail servers
 - Periodic delivery reports (rua tag)
 - Per-instance failure reports (ruf tag)

DMARC: Email Delivery Diagram

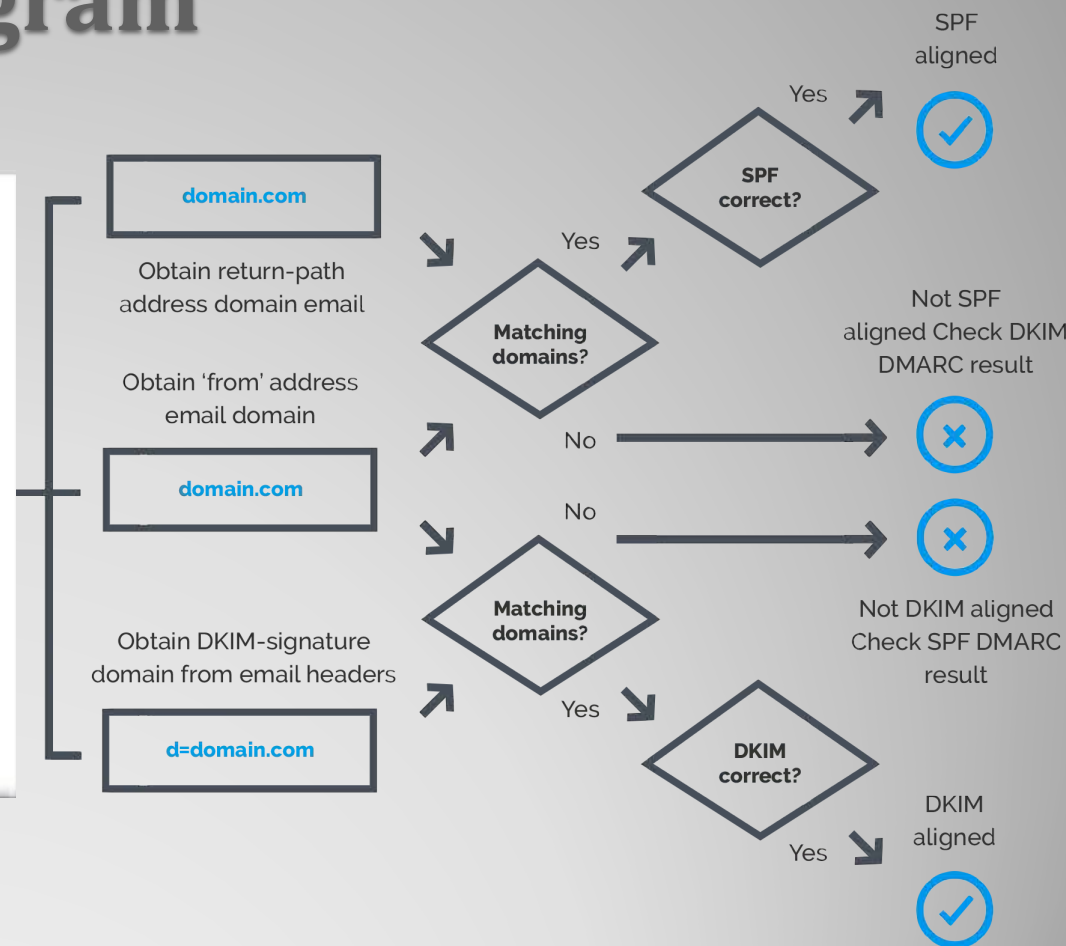


Source: <https://www.mailgun.com/blog/deliverability/email-authentication-your-id-card-sending/>

DMARC: Email Delivery Diagram

Return-Path: <bounce@EUDAEMON.net> 2
Delivered-To: fred@example.com
Authentication-Results: mail.example.com; spf=pass (example.com: domain of bounce@eudaemon.net designates 4.5.6.7 as permitted sender) smtp.mail=bounce@eudaemon.net; dkim=pass header.i=@eudaemon.net
Received: from ..
DKIM-Signature: v=1; a=rsa-sha; c=relaxed/relaxed; d=EUDAEMON.net 3
s=key456; i=@eudaemon.net; q=dns/txt; h= .. ; bh= .. ; b= ..
Date: Wed, 19 Feb 2021 12:39:06 -0500
From: "Human Resources" <hr@EXAMPLE.com> 1
To: "Fred Smith" <fred@example.com>
Subject: Work From Home Policy Update

Staff, please click through the read the latest policies regarding working from home. Click Here



DMARC Analyzer - Trusted Email. Delivered.

Source: <https://community.mimecast.com/s/article/dmarc-analyzer-improving-deliverability-using-dmarc>

DMARC: Record, Policy, & Reporting



_dmarc.stacs.net

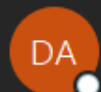
TXT

"v=DMARC1;p=quarantine;ruf=mailto:postmaster@stacs.net"

- v: The version of DMARC being used.
- p: policy, implement and test from none, quarantine, to reject.
 - none: does not quarantine or reject mail; good for initial testing
 - quarantine: recipient's server sends emails that fail DMARC checks to junk/quarantine folders
 - reject: recipient's server completely reject emails that fail DMARC checks
- rua: email address where aggregate reports from participating mailbox providers (Comcast, Microsoft, etc.) are sent
 - Recommend a dedicated mailbox or folder
- ruf: email address where failure reports are sent when an email that appears to be from your domain fails a DMARC check
- ri: reporting interval for DMARC reports

DMARC: Aggregate Reports

[Preview] Report Domain: stacs.net Submitter: enterprise.protection.outlook.com Report-ID: ...



DMARC Aggregate Report <dmarcreport@stacs.net>

To postmaster@stacs.net



Reply

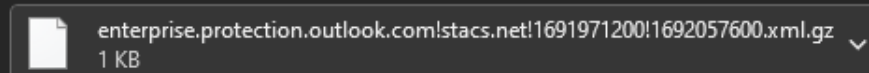
Reply All

Forward



Wed 8/16/2023 8:49 AM

External Sender - Caution: This message originated from outside of ICF. Be careful when responding to or taking actions based on this message.



This is a DMARC aggregate report from Microsoft Corporation. For Emails received between 2023-08-14 00:00:00 UTC to 2023-08-15 00:00:00 UTC.

You're receiving this email because you have included your email address in the 'rua' tag of your DMARC record in DNS for stacs.net. Please remove your email address from the 'rua' tag if you don't want to receive this email.

Please do not respond to this e-mail. This mailbox is not monitored and you will not receive a response. For any feedback/suggestions, kindly mail to dmarcreportfeedback@microsoft.com.

Microsoft respects your privacy. Review our Online Services [Privacy Statement](#).
One Microsoft Way, Redmond, WA, USA 98052.

DMARC: Creating a DMARC Record - MXToolbox

- Generate the record using a free generator tool
 - Mxtoolbox, dmarcian

 DMARC Record Generator SPF Record Generator

Domain or Host Name

email@gobblygook.com

Check DMARC Record

Solve Email Delivery Problems

HOW TO CREATE A DMARC RECORD

Answer the questions below and we'll generate a record for you in the correct format. For more details about each question or option list, click on the "Help" link beside it for more detailed information.

1. How do you want mail that fails DMARC to be treated by the recipient?
We recommend that you start with a policy of "none" - which is "Reporting Mode".

None

[Help](#)

2. What email address(s) should aggregate DMARC reports be sent to?
*If adding multiple email addresses, please use a comma to separate each one.

263a2167@mxtoolbox.dmarc-report.com

[Help](#)

3. What email address(s) would you like to receive forensic DMARC failure reports?
*If adding multiple email addresses, please use a comma to separate each one.

263a2167@forensics.dmarc-report.com

[Help](#)

Would you like to have MxToolbox automatically process your DMARC reports for analysis and delivery insights?

Yes

[Help](#)

[Show Advanced](#)

Created Record Output:
The below record is updated as you modify the fields on the left.

Once you have finished creating your record in this editor, visit your DNS hosting provider and create a new record with the values presented below.

Type: TXT

Host/Name: _DMARC.email@gobblygook.com

Value: v=DMARC1; p=none; rua=mailto:263a2167@mxtoolbox.dmarc-report.com; ruf=mailto:263a2167@forensics.dmarc-report.com; fo=1

* Note: For many DNS hosting providers, you'll just type "_DMARC" as the host/name and the tool add/append your domain name automatically.

Current Record:

Setup DMARC Reports

Invalid Input. 'dmarc' requires a Fully Qualified Domain Name. 'email@gobblygook.com' is invalid.

DMARC Record Lookup

SPF, DKIM, DMARC Record Check

- MXToolbox has a tool to check various types of records for a domain

spf:stacs.net [Find Problems](#) [Solve Email Delivery Problems](#)

```
v=spf1 ip4:23.21.187.245 -all
```

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	ip4	23.21.187.245	Pass	Match if IP is in the given range.
-	all		Fail	Always matches. It goes at the end of your record.

SuperTool Beta7

[SPF Record Lookup](#)

spf:gobblygook.com [Find Problems](#) [Solve Email Delivery Problems](#)

	Test	Result
✖	SPF Record Published	No SPF Record found

SPF, DKIM, DMARC Record Check - Gmail

- Gmail lists them neatly if you click “Show Original” to view the email headers

Original Message

Message ID	<ph7C9vzqP0zjODI2fP73myzSNAH7Ovv4SaTXi9fJxo@www.stacs.net>
Created at:	Tue, Aug 29, 2023 at 6:07 PM (Delivered after 0 seconds)
From:	STACS Support <support@stacs.net> Using PHPMailer 6.8.0 (https://github.com/PHPMailer/PHPMailer)
To:	@gmail.com
Subject:	test 2
SPF:	PASS with IP 23.21.187.245 Learn more
DKIM:	'PASS' with domain stacs.net Learn more
DMARC:	'PASS' Learn more

SPF, DKIM, DMARC Record Check - MXToolbox

- For Outlook, you can obtain headers and use a tool on MXToolbox

The image shows two overlapping windows. The background window is the MXToolbox 'Email Header Analyzer' web application. It has a dark header with navigation links: SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, and Email Health. The main content area is titled 'Email Header Analyzer' and contains a 'Paste Header:' section with three email headers pasted in. Below the headers is an orange 'Analyze Header' button. At the bottom, there is an 'ABOUT EMAIL HEADERS' section explaining that the tool parses headers according to RFC 822. The foreground window is the Outlook 'Properties' dialog box, specifically the 'Settings' tab. It shows fields for Importance (Normal), Sensitivity (Normal), and checkboxes for security and tracking options. At the bottom, the 'Internet headers' section displays the same three email headers that were pasted into the MXToolbox tool.

SuperTool MX Lookup Blacklists DMARC Diagnostics Email Health

Email Header Analyzer

Paste Header:

Received: from DM6PR14MB3903.namprd14.prod.outlook.com (2603:10b6:5:20d::9) by DM6PR14MB2652.namprd14.prod.outlook.com with HTTPS; Tue, 29 Aug 2023 22:07:23 +0000

Received: from SA9PR13CA0057.namprd13.prod.outlook.com (2603:10b6:806:22::32) by DM6PR14MB3903.namprd14.prod.outlook.com (2603:10b6:5:20d::9) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6745.18; Tue, 29 Aug 2023 22:07:20 +0000

Received: from SA2PEPF000015C7.namprd03.prod.outlook.com (2603:10b6:806:22:cafe::2b) by SA9PR13CA0057.outlook.office365.com (2603:10b6:806:22::32) with Microsoft SMTP Server (version=TLS1_2,

Analyze Header

ABOUT EMAIL HEADERS

This tool will make email headers human readable by parsing them according to RFC 822. Email your email headers, [just read this tutorial](#).

File Message Help Acrobat

Delete Archive Reply Reply All Forward Respond Share to Teams Move to: To Manager Team Email Quick Steps Move Tags Editing Immersive

test 2

STACS Support <support@stacs.net>

Properties

Settings

Importance Normal

Sensitivity Normal

Security

☐ Encrypt message contents and attachments

☐ Add digital signature to outgoing message

☐ Request S/MIME receipt for this message

☐ Do not AutoArchive this item

Tracking options

☐ Request a delivery receipt for this message

☐ Request a read receipt for this message

Delivery options

Have replies sent to:

☐ Expires after: None 12:00 AM

Contacts...

Categories None

Internet headers

Received: from DM6PR14MB3903.namprd14.prod.outlook.com (2603:10b6:5:20d::9) by DM6PR14MB2652.namprd14.prod.outlook.com with HTTPS; Tue, 29 Aug 2023 22:07:23 +0000

Received: from SA9PR13CA0057.namprd13.prod.outlook.com (2603:10b6:806:22::32)

Close

Layered Email Security Approach

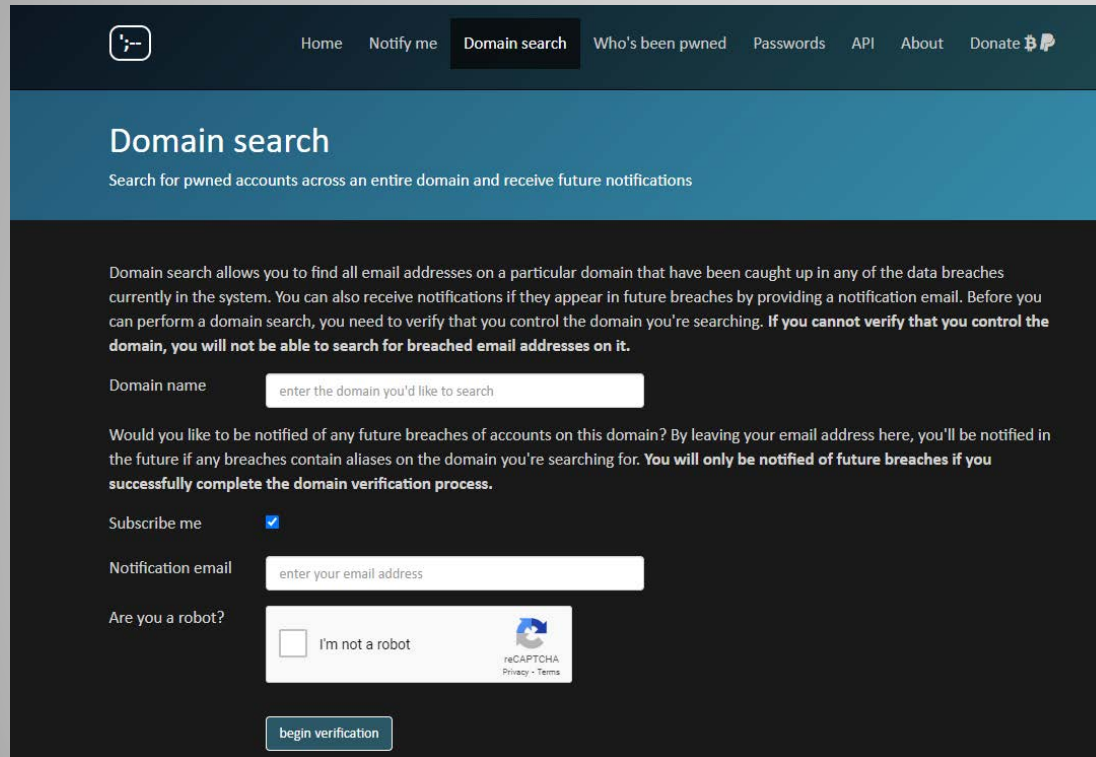
- Implement spam filtering services for inbound and outbound email
 - Barracuda, SpamAssassin, etc.
 - Check with vendor for SPF/DKIM/DMARC support (On-premises Exchange)
- Microsoft 365 Defender (free 90-day trial available)
 - Safe Links
 - Scans destination of URL for suspicious content/properties before allowing user to connect
 - Checks against list of known malicious URLs
 - Safe Attachments
 - Uses a virtual environment to check attachments in email messages before they're delivered to recipients
 - If deemed safe, allows email to move to inbox – else, quarantine or reject based on setting

Layered Email Security Approach

- Securing User access to email services
 - Require https and MFA for webmail access
 - Disable legacy email protocols (POP, IMAP)
 - Use SSL/TLS (POP/S, IMAP/S) or other encryption supported by email vendor
- User security awareness training
 - Ninjio
 - Hackers targeting email account access
 - Call to verify sensitive or financial critical requests

Layered Email Security Approach

Monitor Email Domain for Compromised Accounts



The screenshot shows the 'Domain search' page on the HaveIBeenPwned website. The page has a dark blue header with navigation links: Home, Notify me, Domain search (highlighted), Who's been pwned, Passwords, API, About, and Donate. Below the header, the 'Domain search' section has a subtitle: 'Search for pwned accounts across an entire domain and receive future notifications'. The main content area explains that domain search finds email addresses on a particular domain caught in data breaches. It includes a text input field for 'Domain name' with the placeholder 'enter the domain you'd like to search'. Below this, it asks if the user wants to be notified of future breaches, with a 'Subscribe me' checkbox checked. There is another text input field for 'Notification email' with the placeholder 'enter your email address'. At the bottom, there is a reCAPTCHA 'Are you a robot?' section with an unchecked checkbox and a 'begin verification' button.

- HaveIBeenPwned
 - <https://haveibeenpwned.com>
- Change password of account wherever it is used
- Consider password managers to prevent password reuse and increased damage in case of compromise

MXToolbox Blacklist Monitor

BLACKLIST:STACS.NET ✎

blacklist:stacs.net

Last 7 Days Up: 100% Down: 0 seconds Alerts sent: 0

Last 30 days Up: 100% Down: 0 seconds Alerts sent: 1

Ok

[Postmaster Blacklists](#)

Outages

[History](#)

[Edit](#)

OUTAGES

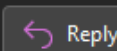
No outages to display

MxToolbox Blacklist Summary

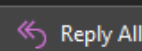


noreply@mxtoolbox.com

To: Cusimano, Joey



Reply



Reply All

External Sender - Caution: This message originated from outside of ICF. Be careful when responding to or taking action on this message. If there are problems with how this message is displayed, click here to view it in a web browser. Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures.

All Blacklist Monitors

MxWatch is currently configured to monitor the following servers for Blacklist Activity.

	IP/Domain	MxRep	Name	Current Status	Duration
I	104.130.102.232	100	blacklist:104.130...	Not Blacklisted	Up for 6 months

Questions?

You can send questions in chat window too.

Resources

- MXToolbox Email Header Analyzer
 - <https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx>
- SPF
 - <https://support.google.com/a/answer/33786?hl=en#to-do>
- DKIM
 - <https://support.google.com/a/answer/174124?sjid=7693783944620326383-NA>
- DMARC
 - [https://support.google.com/a/answer/2466580?hl=en#:~:text=Sender%20Policy%20Framework%20\(SPF\)%3A,actually%20came%20from%20your%20organization.](https://support.google.com/a/answer/2466580?hl=en#:~:text=Sender%20Policy%20Framework%20(SPF)%3A,actually%20came%20from%20your%20organization.)
- DMARC Alignment
 - <https://dmarcian.com/alignment/>