CYBERSECURITY AWARENESS MONTH 2023

WaTech
Washington Technology Solutions

Phishing Below the Surface

(Email Security)

Daniel Brown, CISSP, CISM

Cybersecurity Advisor (CSA) for Eastern Washington.

Cybersecurity and Infrastructure Security Agency (CISA)

Agenda

- Foundational technologies:
  - SPF
  - DKIM
  - DMARC
- Authenticated Received Chain (ARC)
- Email Header Analysis
- Tools
- Conclusion/recommendations

Why use SPF, DKIM, DMARC?

- Simple Mail Transfer Protocol (SMTP) permits **any** computer to send email claiming to be from **any** source address.

…..unless you use SPF, DKIM, DMARC for email authentication!!

Sender Policy Framework (SPF)

- Lists all IP addresses or domains that are allowed to send email on behalf of your domain.
- Directs policy enforcement actions (i.e. –all,~all,+all)

- Can be misconfigured to be overly permissive
  - Include "+all" at end of SPF record – allows any IP to send on your behalf
  - Incorrect CIDR notation for networks – allows unintentional IP's to send on your behalf
    - i.e. if intent is to include subnet of 142.0.175.0**/20** and you inadvertently use **/2**…............ Rather than 4096 addresses, you would allow 1,073,741,824 IP's which is 25% of all IPv4 addresses

Components of an SPF Record

- Version number
- Mechanisms – describes authorized mail hosts for a given domain
  - Common mechanisms include – a, mx, include:, ptr, all, exists, ip4, ipv6
- Quantifiers
  - + (PASS result),- (HARDFAIL),~(SOFTFAIL),? (NEUTRAL)
- Modifiers
  - Redirect, exp

Example SPF Records

- **Example 1:**
  - **v=spf1 a include:_spf.googel.com –all**
    - *v* - current version of spf
    - *a* - authorizes the host detected in the A record of the domain to send the emails.
    - *Include* - 3rd party domain authorized to send email on your behalf
    - *-all* - fail - non-authorized emails will be rejected
- **Example 2:**
  - **v=spf1 ip4:40.113.200.201 ip6:2001:db8:85a3:8d3:1319:8a2e:370:7348 include:thirdpartydomain.com -all**
    - *v* - current version of spf
    - all IP's that are authorized to send email on behalf of your domain
    - *Include:* 3rd party domain authorized to send email on your behalf
    - *-all* - fail - non-authorized emails will be rejected

CYBERSECURITY AWARENESS MONTH 2023

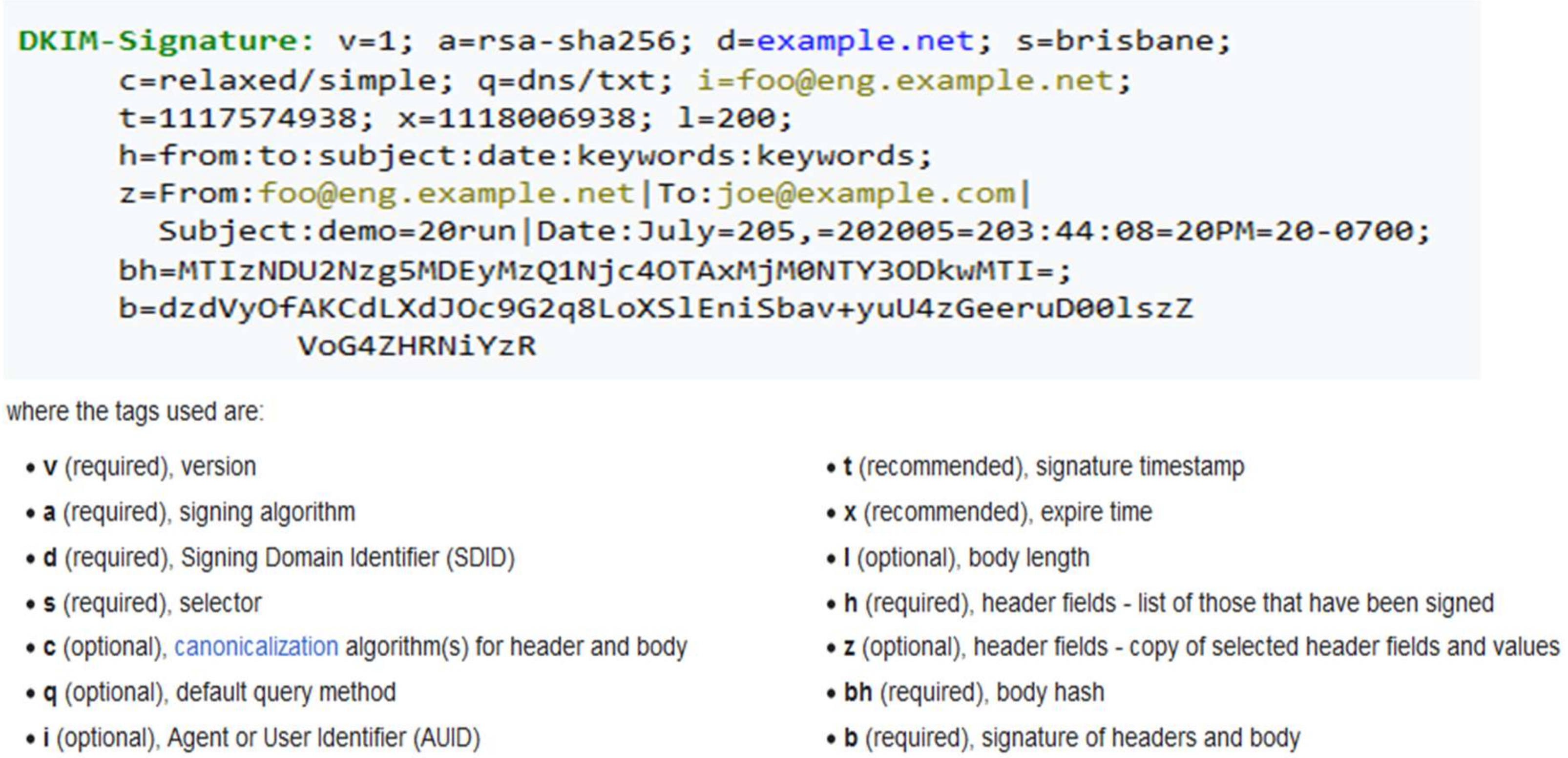
WaTech
Washington Technology Solutions

Questions

DomainKeys Identified Mail (DKIM)

- **Allows for a domain to prove it is responsible for a message and it was not altered as it traveled the delivery path.**
- **Creates and decodes the DKIM signature.**
  - **Sender's public key is published in DNS**
- **DKIM signatures are inserted into the header of an email message.**
- **DKIM is an Internet Standard.[3] It is defined in RFC 6376, dated September 2011, with updates in RFC 8301 and RFC 8463.**

DomainKeys Identified Mail (DKIM) example



```
DKIM-Signature: v=1; a=rsa-sha256; d=example.net; s=brisbane;
     c=relaxed/simple; q=dns/txt; i=foo@eng.example.net;
     t=1117574938; x=1118006938; l=200;
     h=from:to:subject:date:keywords:keywords;
     z=From:foo@eng.example.net|To:joe@example.com|
       Subject:demo=20run|Date:July=205,=202005=203:44:08=20PM=20-0700;
     bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
     b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
              VoG4ZHRNiYzR
```

where the tags used are:

- **v** (required), version
- **a** (required), signing algorithm
- **d** (required), Signing Domain Identifier (SDID)
- **s** (required), selector
- **c** (optional), canonicalization algorithm(s) for header and body
- **q** (optional), default query method
- **i** (optional), Agent or User Identifier (AUID)
- **t** (recommended), signature timestamp
- **x** (recommended), expire time
- **l** (optional), body length
- **h** (required), header fields - list of those that have been signed
- **z** (optional), header fields - copy of selected header fields and values
- **bh** (required), body hash
- **b** (required), signature of headers and body

Domain-based Message Authentication, Reporting & Conformance (DMARC)

- **Improves upon existing security measures provided by DKIM and SPF**
- **Allows a sender’s domain to indicate that their messages are protected by SPF and/or DKIM**
- **Tells a receiver what to do if SPF/DKIM authentication fails:**
  - **Reject**
  - **quarantine**

DMARC records are published in DNS with a subdomain label _dmarc, for example _dmarc.example.com. Compare this to SPF at example.com, and DKIM at selector._domain

Here, v is the version, p is the policy (see below), sp the subdomain policy, pct is the percent of "bad" email on which to apply the policy, and rua is the URI to send aggregate reports to.

(DMARC) sample config

- DMARC records are published in DNS with a subdomain label _dmarc
- **v=DMARC1;p=none;sp=quarantine;pct=100;rua=mailto:dmarcreports@example.com;**
  - **v** is the version
  - **p** is the policy (none, quarantine, or reject)
  - **sp** the subdomain policy
  - **pct** is the percent of "bad" email on which to apply the policy (optional)
  - **rua** is the URI to send aggregate reports to.

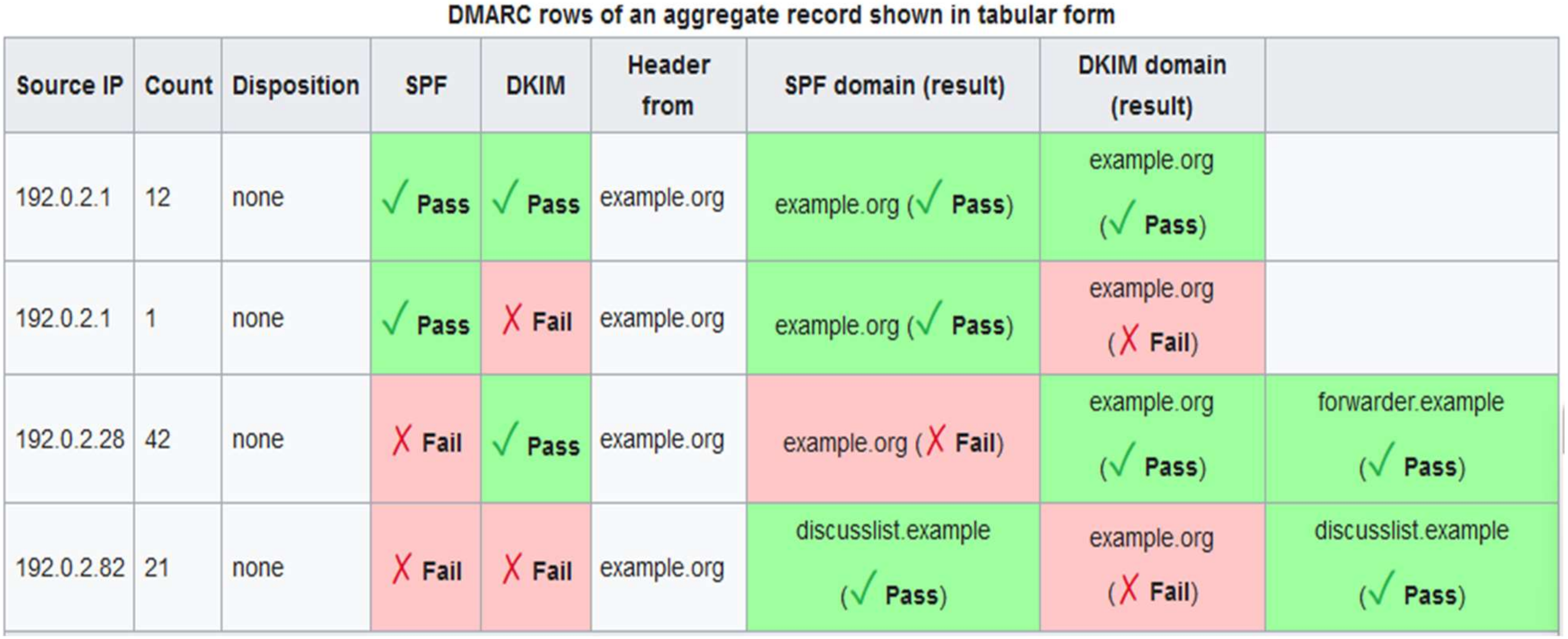
DMARC records are published in DNS with a subdomain label _dmarc, for example _dmarc.example.com. Compare this to SPF at example.com, and DKIM at selector._domain

Here, v is the version, p is the policy (see below), sp the subdomain policy, pct is the percent of "bad" email on which to apply the policy, and rua is the URI to send aggregate reports to.

CYBERSECURITY AWARENESS MONTH 2023

WaTech Washington Technology Solutions

(DMARC) sample aggregate report



DMARC rows of an aggregate record shown in tabular form

Source IP	Count	Disposition	SPF	DKIM	Header from	SPF domain (result)	DKIM domain (result)	
192.0.2.1	12	none	✓ Pass	✓ Pass	example.org	example.org (✓ Pass)	example.org (✓ Pass)	
192.0.2.1	1	none	✓ Pass	✗ Fail	example.org	example.org (✓ Pass)	example.org (✗ Fail)	
192.0.2.28	42	none	✗ Fail	✓ Pass	example.org	example.org (✗ Fail)	example.org (✓ Pass)	forwarder.example (✓ Pass)
192.0.2.82	21	none	✗ Fail	✗ Fail	example.org	discusslist.example (✓ Pass)	example.org (✗ Fail)	discusslist.example (✓ Pass)

CYBERSECURITY AWARENESS MONTH 2023

WaTech
Washington Technology Solutions

Questions

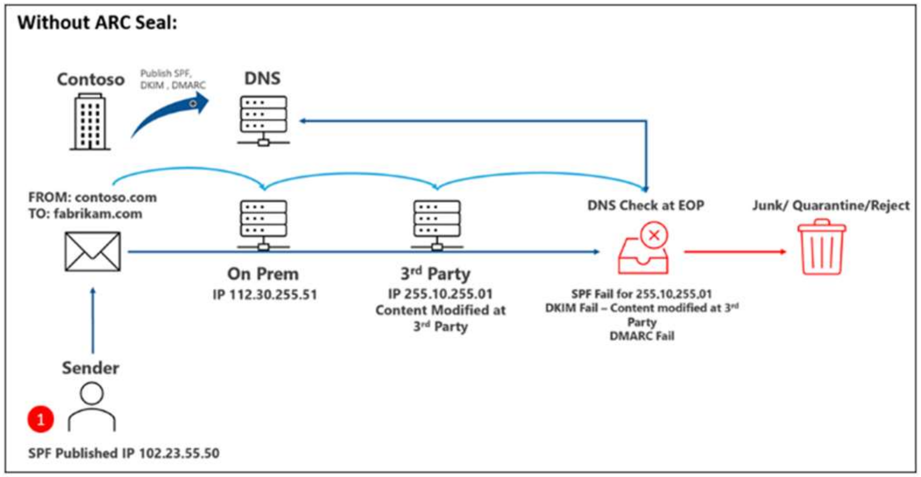
Future/additional options

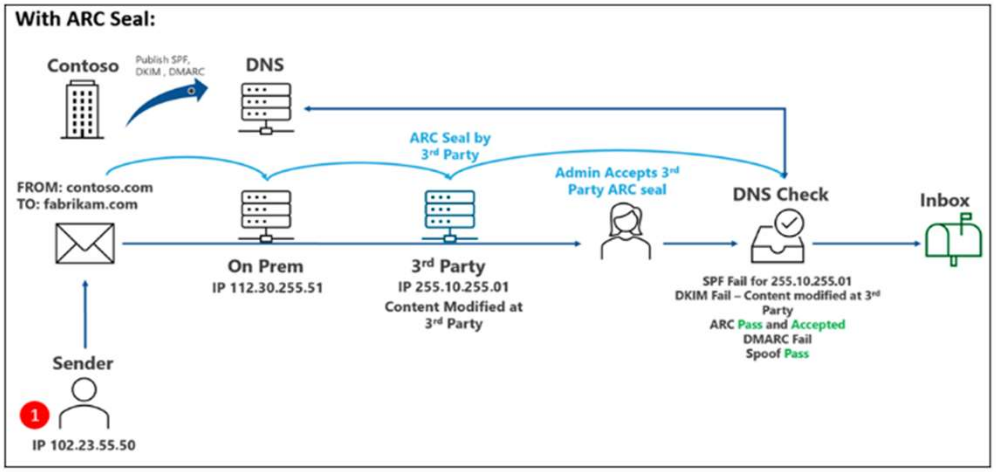
- Brand Indicators for Message Identification (BIMI)
  - Uses DKIM, SPF and DMARC to verify
  - Adds brand logo icons next to the names of email senders as an additional validation
  - Email marketing companies support this option

- New security features launched by Google 10/23, Yahoo 02/24
  - Bulk senders that send more than 5,000 messages will have new authentication requirements.
  - Senders required to process unsubscribe requests within 2 days

- Authenticated Received Chain (ARC)
  - Make a list of trusted ARC Senders to trust legitimate indirect mailflows

Trusted Authenticated Received Chain (ARC) sealer mailflow





* In Microsoft 365 Defender, ARC will help reduce SPF, DKIM, and DMARC delivery failures that happen due to legitimate indirect mailflows
* Helps to keep message from being modified in transit
* Adds a list of trusted intermediaries into the MS Defender portal

Message Header Analysis

- Source for identifying message properties
  (Note - Email must be forwarded to maintain header information)
- Header includes:
  - Sender
  - Recipient
  - Date
  - Subject
  - Authentication check
  - Return Path
  - Transport Layer Security (TLS)
  - Authenticated Received Chain (ARC)
  - Route through Mail Transfer Agents (MTA's)
  - SPF, DKIM, DMARC info

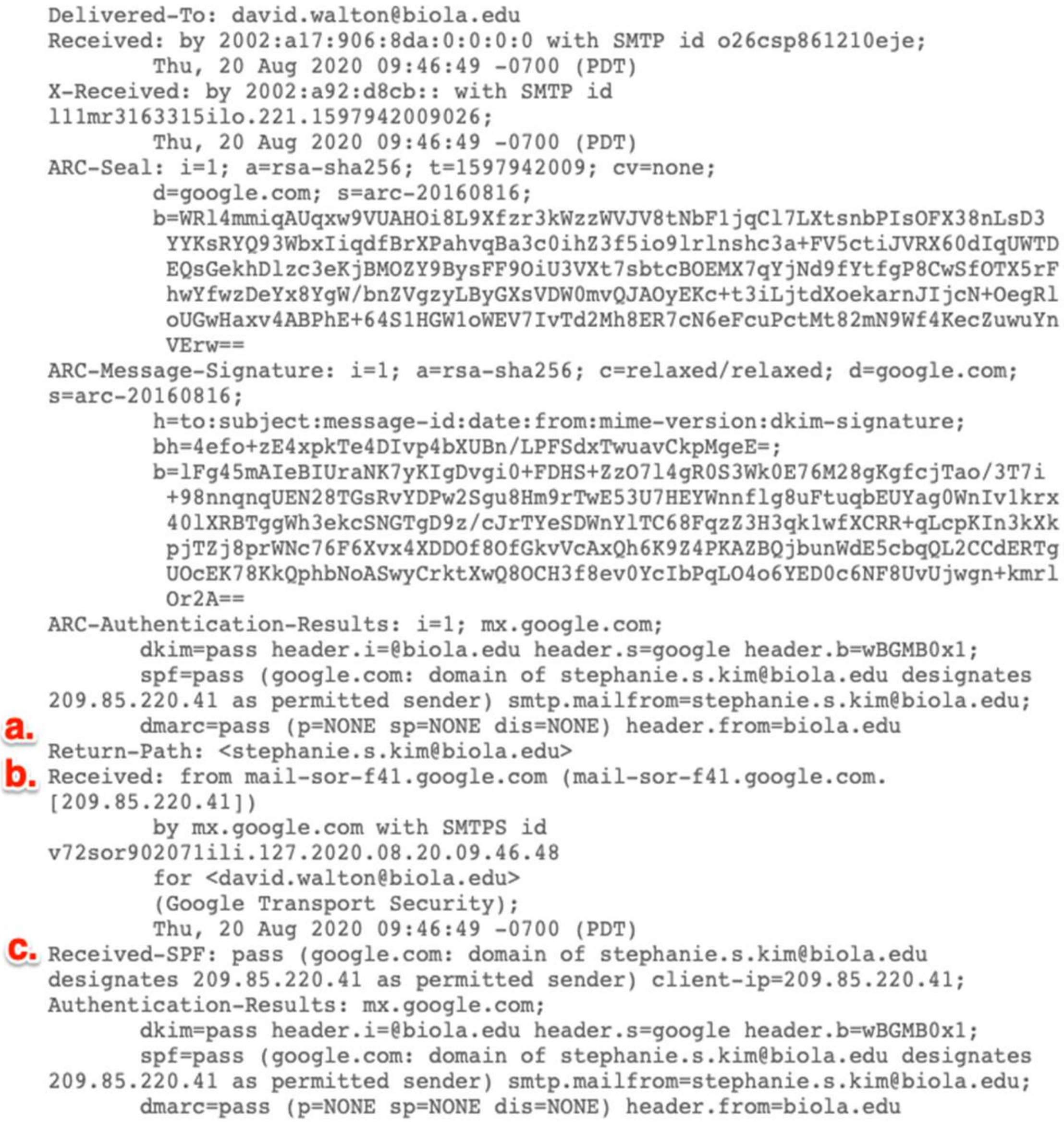
Message Header Analysis - continued

where to find them

- **Outlook**
  - With Message Open - File>Info>Properties>Delivery Options>Internet Headers
- **Google**
  - click on the three dots in the top right corner of any email message you have, then select “Show Original”
- **Apple Mail**
  - With Message Open – View menu, then All Headers. The headers will the display at the top of the message.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

Message Header



```
   Delivered-To: david.walton@biola.edu
   Received: by 2002:a17:906:8da:0:0:0:0 with SMTP id o26csp861210eje;
           Thu, 20 Aug 2020 09:46:49 -0700 (PDT)
   X-Received: by 2002:a92:d8cb:: with SMTP id
   111mr3163315ilo.221.1597942009026;
           Thu, 20 Aug 2020 09:46:49 -0700 (PDT)
   ARC-Seal: i=1; a=rsa-sha256; t=1597942009; cv=none;
           d=google.com; s=arc-20160816;
           b=WRl4mmiqAUqxw9VUAHOi8L9Xfzr3kWzzWVJV8tNbF1jqCl7LXtsnbPIsOFX38nLsD3
            YYKsRYQ93WbxIiqdfBrXPahvqBa3c0ihZ3f5io9lrlnshc3a+FV5ctiJVRX60dIqUWTD
            EQsGekhDlzc3eKjBMOZY9BysFF9OiU3VXt7sbtcBOEMX7qYjNd9fYtfgP8CwSfOTX5rF
            hwYfwzDeYx8YgW/bnZVgzyLByGXsVDW0mvQJAOyEKc+t3iLjtdXoekarnJIjcN+OegRl
            oUGwHaxv4ABPhE+64S1HGW1oWEV7IvTd2Mh8ER7cN6eFcuPctMt82mN9Wf4KecZuwuYn
            VErw==
   ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com;
   s=arc-20160816;
           h=to:subject:message-id:date:from:mime-version:dkim-signature;
           bh=4efo+zE4xpkTe4DIvp4bXUBn/LPFSdxTwuavCkpMgeE=;
           b=lFg45mAIeBIUraNK7yKIgDvgi0+FDHS+ZzO7l4gR0S3Wk0E76M28gKgfcjTao/3T7i
            +98nnqnqUEN28TGsRvYDPw2Sgu8Hm9rTwE53U7HEYWnnflg8uFtuqbEUYag0WnIv1krx
            40lXRBTggWh3ekcSNGTgD9z/cJrTYeSDWnYlTC68FqzZ3H3qk1wfXCRR+qLcpKIn3kXk
            pjTZj8prWNc76F6Xvx4XDDOf8OfGkvVcAxQh6K9Z4PKAZBQjbunWdE5cbqQL2CCdERTg
            UOcEK78KkQphbNoASwyCrktXwQ8OCH3f8ev0YcIbPqLO4o6YED0c6NF8UvUjwgn+kmrl
            Or2A==
   ARC-Authentication-Results: i=1; mx.google.com;
          dkim=pass header.i=@biola.edu header.s=google header.b=wBGMB0x1;
          spf=pass (google.com: domain of stephanie.s.kim@biola.edu designates
   209.85.220.41 as permitted sender) smtp.mailfrom=stephanie.s.kim@biola.edu;
a.        dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=biola.edu
   Return-Path: <stephanie.s.kim@biola.edu>
b. Received: from mail-sor-f41.google.com (mail-sor-f41.google.com.
   [209.85.220.41])
           by mx.google.com with SMTPS id
   v72sor902071ili.127.2020.08.20.09.46.48
           for <david.walton@biola.edu>
           (Google Transport Security);
           Thu, 20 Aug 2020 09:46:49 -0700 (PDT)
c. Received-SPF: pass (google.com: domain of stephanie.s.kim@biola.edu
   designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41;
   Authentication-Results: mx.google.com;
          dkim=pass header.i=@biola.edu header.s=google header.b=wBGMB0x1;
          spf=pass (google.com: domain of stephanie.s.kim@biola.edu designates
   209.85.220.41 as permitted sender) smtp.mailfrom=stephanie.s.kim@biola.edu;
          dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=biola.edu
```

Tools

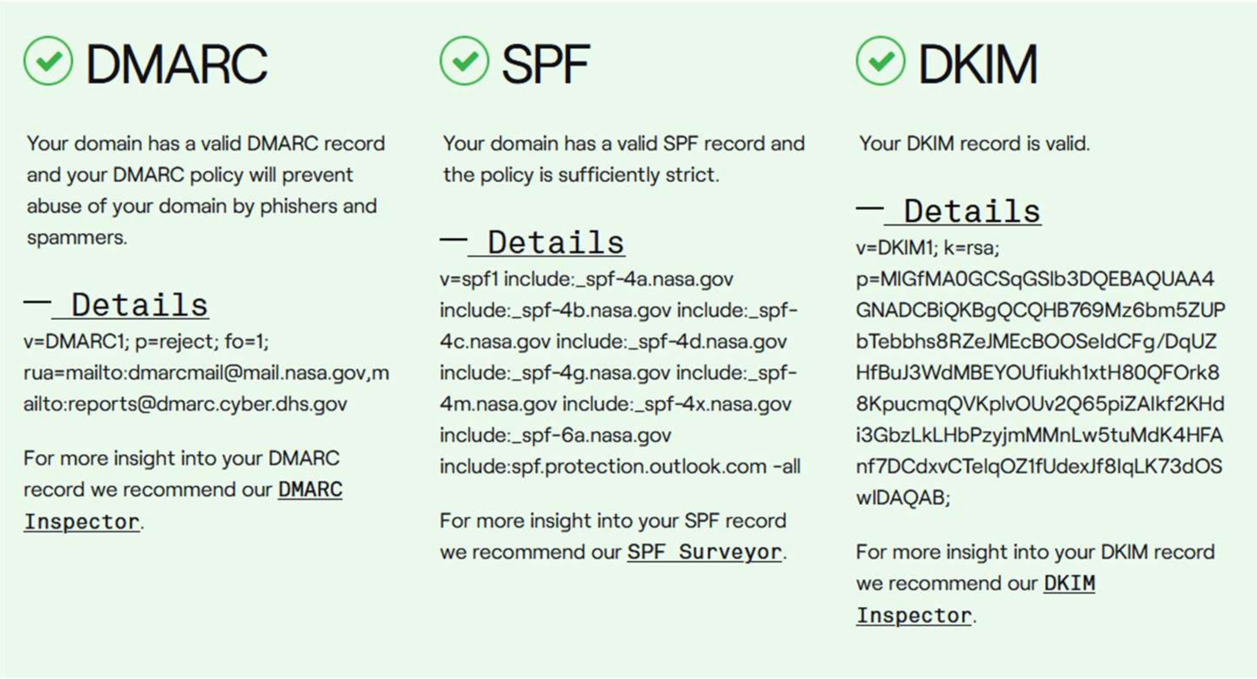
- Both paid and free versions of many tools
- Search “SPF tools” or “spf dkim/dmarc check”
- Some tools are better in different areas
- Can verify config and check:
  - SPF
  - DKIM
  - DMARC
  - Status on known blacklists

Evaluation of an SPF record can return any of these results:

Result	Explanation	Intended Action
Pass	The SPF record designates the host to be allowed to send	Accept
Fail	The SPF record has designated the host as NOT being allowed to send	Reject
SoftFail	The SPF record has designated the host as NOT being allowed to send but is in transition	Accept but mark
Neutral	The SPF record specifies explicitly that nothing can be said about validity	Accept
None	The domain does not have an SPF record or the SPF record does not evaluate to a result	Accept
PermError	A permanent error has occurred (eg. badly formatted SPF record)	Unspecified
TempError	A transient error has occurred	Reject

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

Tool example with all 3 properly configured (free version)



✓ DMARC

Your domain has a valid DMARC record and your DMARC policy will prevent abuse of your domain by phishers and spammers.

— Details

```
v=DMARC1; p=reject; fo=1;
rua=mailto:dmarcmail@mail.nasa.gov,m
ailto:reports@dmarc.cyber.dhs.gov
```

For more insight into your DMARC record we recommend our DMARC Inspector.

✓ SPF

Your domain has a valid SPF record and the policy is sufficiently strict.

— Details

```
v=spf1 include:_spf-4a.nasa.gov
include:_spf-4b.nasa.gov include:_spf-
4c.nasa.gov include:_spf-4d.nasa.gov
include:_spf-4g.nasa.gov include:_spf-
4m.nasa.gov include:_spf-4x.nasa.gov
include:_spf-6a.nasa.gov
include:spf.protection.outlook.com -all
```

For more insight into your SPF record we recommend our SPF Surveyor.

✓ DKIM

Your DKIM record is valid.

— Details

```
v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4
GNADCBiQKBgQCQHB769Mz6bm5ZUP
bTebbhs8RZeJMEcBOOSeldCFg/DqUZ
HfBuJ3WdMBEYOUfiukh1xtH80QFOrk8
8KpucmqQVKplvOUv2Q65piZAlkf2KHd
i3GbzLkLHbPzyjmMMnLw5tuMdK4HFA
nf7DCdxvCTelqOZ1fUdexJf8IqLK73dOS
wIDAQAB;
```

For more insight into your DKIM record we recommend our DKIM Inspector.

Conclusion

- Review existing config – use tools and check DNS
  - Add/modify/update
- Review client settings to enable security features
- Research new email trends and technologies
  - Email Service Provider (ESP) blogs/podcasts
    - "Deliverability" professionals
    - Bulk senders (i.e. marketing)
    - Reputation score improvement
  - AI and analytics being used by providers to filter spam

CYBERSECURITY AWARENESS MONTH 2023

WaTech
Washington Technology Solutions

Questions

SECURE OUR WORLD

CYBERSECURITY AWARENESS MONTH

https://www.cisa.gov/cybersecurity-awareness-month

Christopher Callahan, CISSP, GICSP
Region 10 (Western WA, OR, ID, AK)
Chief of Cybersecurity
(206) 601-4575
Christopher.Callahan@cisa.dhs.gov

Ian Moore, CISSP
Region 10 (WA)
Cybersecurity State Coordinator for Washington State
(360) 594-1832
Ian.Moore@cisa.dhs.gov

Daniel Brown, CISSP, CISM
Region 10 (Eastern Washington)
Cybersecurity Advisor
(509) 981-9920
Daniel.Brown@cisa.dhs.gov

https://www.cisa.gov/cyber-resource-hub

Ron Watters, CISSP, GSLC
Region 10 (Western WA, OR, ID, AK)
Cybersecurity Advisor
(206) 348-4071
Ronald.Watters@cisa.dhs.gov

Alexander Salazar, CISSP
Region 10 (WA, King County Area)
Cybersecurity Advisor
(206) 225-5546
Alexander.Salazar@cisa.dhs.gov

For inquiries or further information,
contact cyberadvisor@cisa.dhs.gov