KnowBe4
Human error. Conquered.

Implementing DMARC the Right Way to Keep Phishing Attacks Out of Your Inbox

Roger A. Grimes
Data-Driven Defense Evangelist
rogerg@knowbe4.com

Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

e: rogerg@knowbe4.com
Twitter: @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/

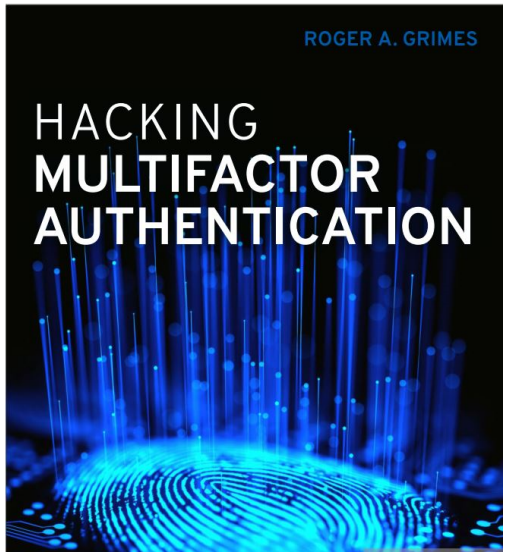
About Roger

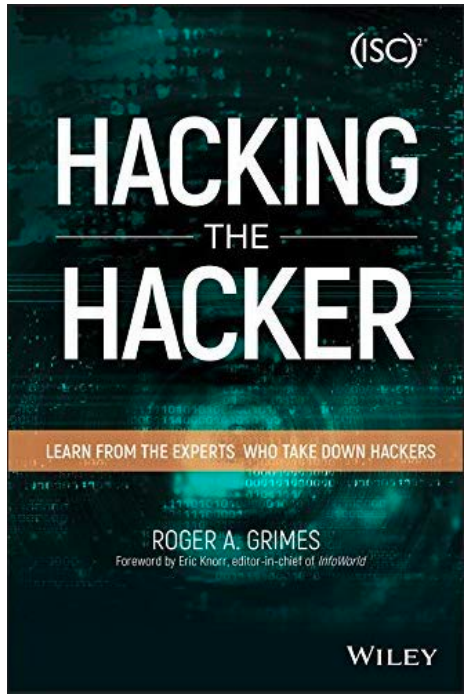
- 30 years plus in computer security, 20 years pen testing
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 13 books and over 1,100 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

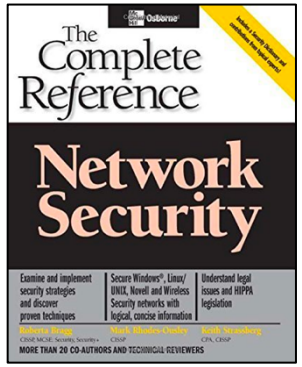
Certification exams passed include:

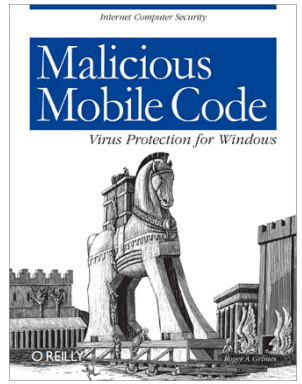
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

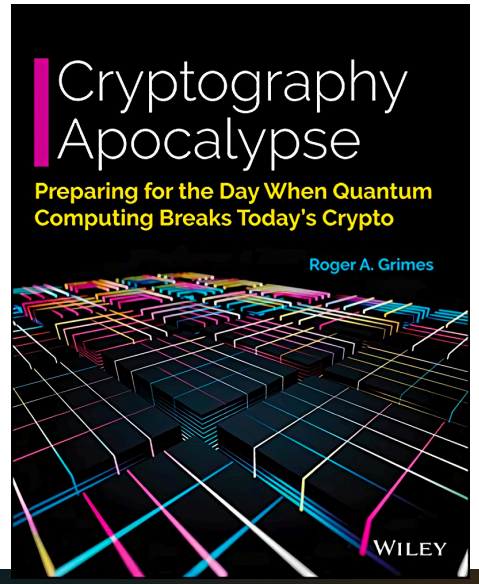
Roger's Books

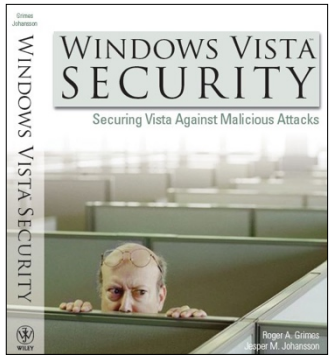


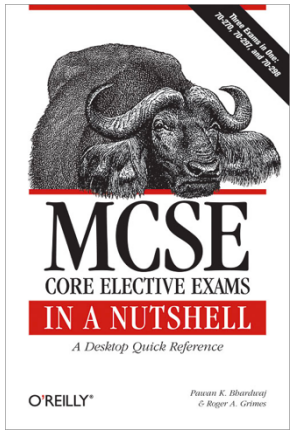


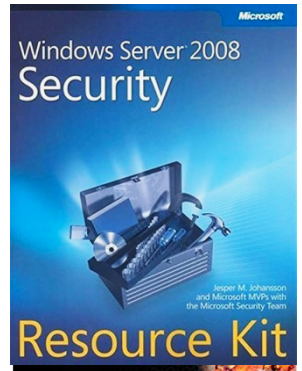


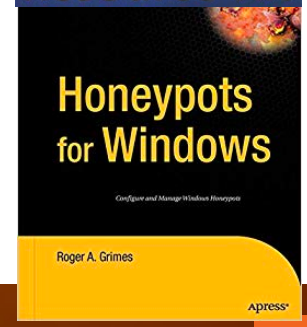












About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- Winner of numerous industry awards

Today's Presentation

- What is DMARC, SPF, and DKIM?
- How to Configure
- Common Mistakes
- Best Practices
- How Phishes Still Get By

Agenda

- **What is DMARC, SPF, and DKIM?**
  - How to Configure
- Best Practices
- How Phishes Get By

DMARC, DKIM, SPF

Global Phishing Protection Standards

- **Sender Policy Framework (SPF)**
- **Domain Keys Identified Mail (DKIM)**
- **Domain-based Message Authentication, Reporting and Conformance (DMARC)**
  - DMARC relies on/uses SPF and/or DKIM
- SPF, DKIM, and DMARC help you protect YOUR domain against spoofing by bad people to others!
- When enabled, receivers can verify whether or not an email that claims to be from your domain is from your domain

DMARC, DKIM, SPF

Global Phishing Protection Standards

- All rely on DNS
  - Use TXT RR (resource records)
  - DKIM requires additional work
- It is usually checked for by most (but not all) email servers
- Sending domain must setup
- Receiving domain checks for DNS records and verifies

***Participants have both to enable/configure sending and receiving**

***You should enable SPF, DKIM, and DMARC**

DMARC, DKIM, SPF

Global Phishing Protection Standards

- 2021 National Defense Authorization Act says DHS must implement DMARC US wide

"…to implement across all US-based email providers…at scale."

SEC. 9006. STRATEGY TO SECURE EMAIL.

(a) IN GENERAL.—Not later than December 31, 2021, the Secretary of Homeland Security shall develop and submit to Congress a strategy, including recommendations, to implement across all United States-based email providers Domain-based Message Authentication, Reporting, and Conformance standard at scale.

(b) ELEMENTS.—The strategy required under subsection (a) shall include the following:

(1) A recommendation for the minimum-size threshold for United States-based email providers for applicability of Domain-based Message Authentication, Reporting, and Conformance.

(2) A description of the security and privacy benefits of implementing the Domain-based Message Authentication, Reporting, and Conformance standard at scale, including recommendations for national security exemptions, as appropriate, as well as the burdens of such implementation and an identification of the entities on which such burdens would most likely fall.

(3) An identification of key United States and international stakeholders associated with such implementation.

(4) An identification of any barriers to such implementation, including a cost-benefit analysis where feasible.

(5) An initial estimate of the total cost to the Federal Government and implementing entities in the private sector of such implementation, including recommendations for defraying such costs, if applicable.

(c) CONSULTATION.—In developing the strategy and recommendations under subsection (a), the Secretary of Homeland Security may, as appropriate, consult with representatives from the information technology sector.

https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf

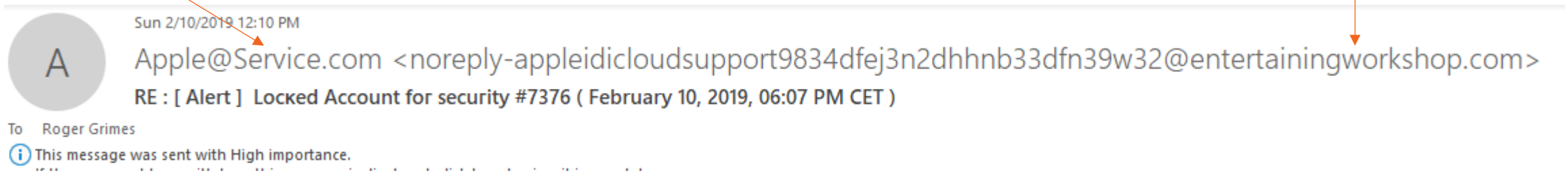
SPF & DKIM

Global Email Authentication Standards

- **Sender Policy Framework (SPF)**
  - Verifies the 5321 **MAIL FROM** domain name address
    - This is the “real” return email address that you may not see

“Friendly From”
Human readable part of “From:” header.

5322.DISPLAY
FROM domain



SPF & DKIM

Global Email Authentication Standards

- **Domain Keys Identified Mail (DKIM)**
  - Uses public/private key pair to add a digital signature to every outgoing email that links the email to it's sending Internet domain
    - Verified domain is found in the DKIM-Signature header
    - DKIM signatures typically cover most of the email message so that people cannot tamper with content of an email
      - However some of the email headers are NOT included in signature -- specifically headers that tend to be modified as email flows across the Internet (like "Received:" and "Return-Path:" headers).

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=dmarcian.com; s=s2048g1;
        h=subject:to:cc:references:from:message-id:date:user-agent
         :mime-version:in-reply-to:content-language;
        bh=iVrm4GcK3W8w6dNUvDCTJY22HJmChvuZ7JCebDsftOg=;
        b=CVIqiyEdtNmyvl8PAbimb87xBL15wQPS2k89oEg14uz4LugQLf3U/Vw7GpRLciiRO+
         dCpszAlw0WNWBGcRmJKM/dzLwTR6wTth/vwkXpcf8tT2/K9c1Le649YRnwtdnwmNwpxu
         PEqzATj0uj6hiEUmy4UL1/e6tP58Gb5UMCKpsXdV1+J3Qu3Jech7k5250LQRLqsVetAE
         G7fCQ6GFpaAApnRXa2BTOk7gHPB4Ak8BYy7iNT2ckuPi7ETuCaA4bqplKpm5LlpsTKUW
         x/gAsB94w5fv5Q+UTZhiz3LTEz1YMh5UEi8Ix+O2mUMTBXgINpmxV9MqdF0AhVyC1uef
         NTHw==
```

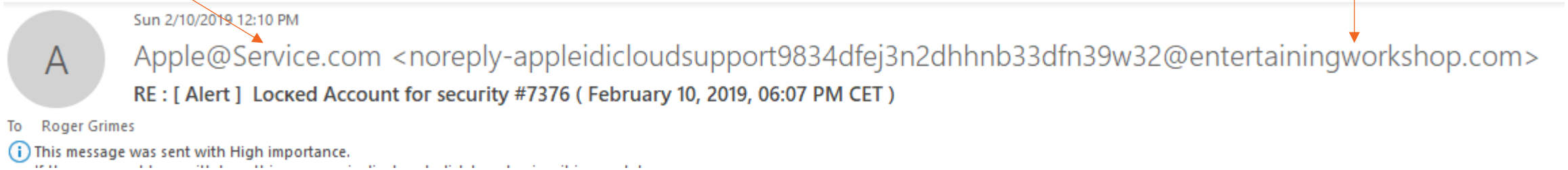
DMARC

Global Email Authentication Standards

- **Domain-based Message Authentication, Reporting and Conformance (DMARC)**
  - Helps to tell receivers how to treat emails that fail SPF and/or DKIM
  - DMARC requires the domains that SPF and/or DKIM verifies to match what is found in the 5322.From address
  - Helps senders with diagnostic reports

"Friendly From"
Human readable part of "From:" header.

5322.DISPLAY
FROM domain



SPF, DKIM, DMARC

Setup – General

Sender

- SPF, DKIM & DMARC – Sender creates DNS record
- DKIM – Sender installs key pair and enables DKIM on email server

Receiver

- SPF, DKIM, & DMARC – Receiver enables verification checking and response

Details of how to configure next

SPF

KnowBe4
Human error. Conquered.

SPF

Sender Policy Framework (SPF)

- Designed to prevent sender email address domain spoofing by receiver verifying the IP address of the mail server the email arrived from matches a list of allowed IP addresses designated by domain's admins
- Checks for domain spoofing in 5321 Mail From/Return-Path field
- Relies on SPF/TXT records in DNS
  - example.com. IN TXT "v=spf1 ip4:192.168.1.1 ~all"
- Sender must have it enabled
- Receiver checks and verifies

SPF

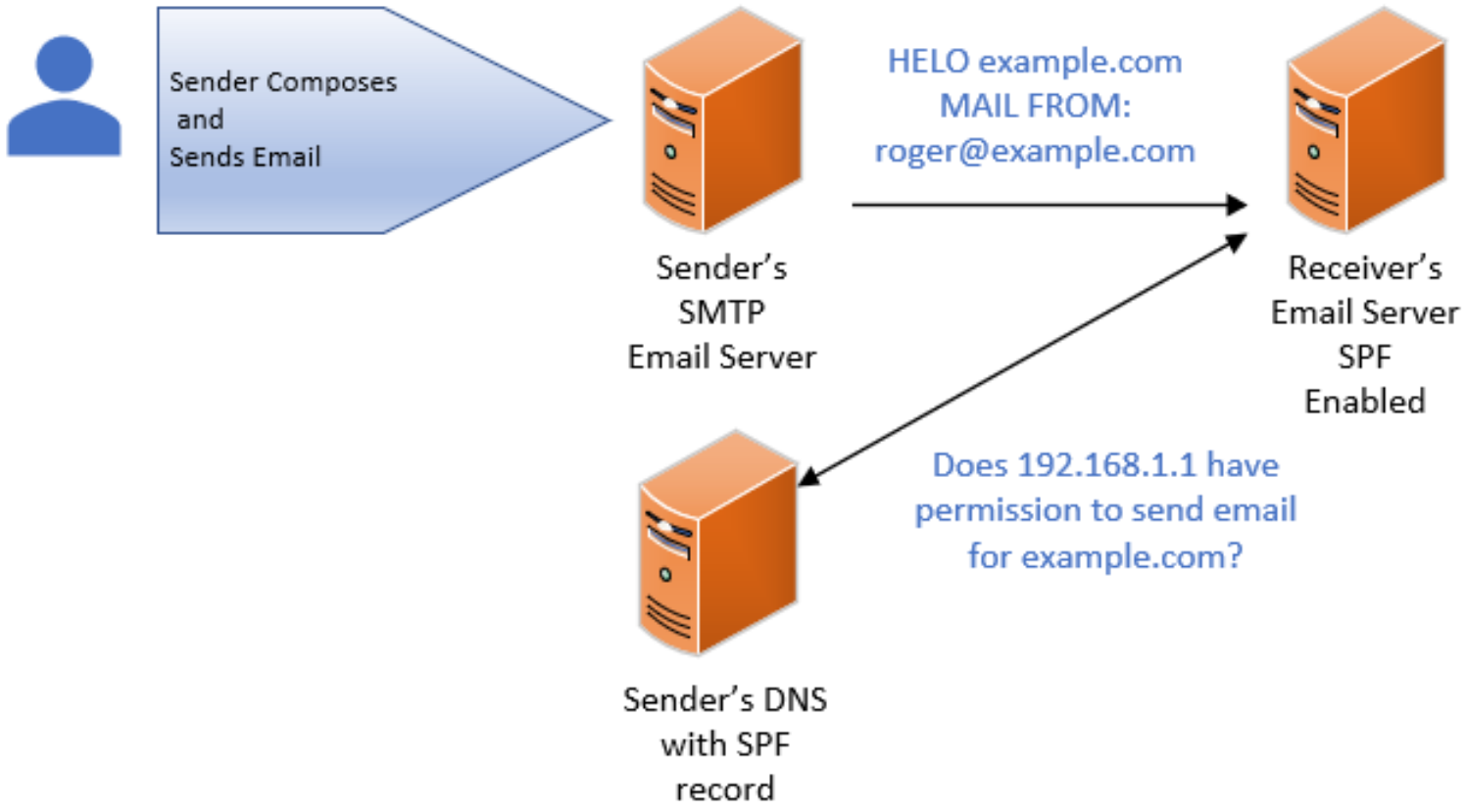
Sender Policy Framework (SPF)

- RFC 7208 (older version 4408)
  - http://www.zytrax.com/books/dns/apd/rfc7208.txt
- When enabled, receiving email server checks MAIL FROM address or the domain's IP address in the HELO handshake against the sender's SPF DNS record
- If it fails, recipient's server can generate a message:
  - 550 5.7.1 Sender ID/SPF failed from IP XXX.XXX.XXX.XXX
- Email server/email inspection/client can decide to react to

SPF

Sender Policy Framework (SPF)

- Basic Overview



Sender Policy Framework (SPF)

Setting Up – Sender Side

- Collect all of the domain names which your organization owns or controls
  - Even those that are not used to send email, to stop hackers from spoofing those domains
- Remember to include any “parked domains” which could later on become active

SPF

Sender Policy Framework (SPF)

Setting Up – Sender Side

- Collect the **PUBLIC** IP addresses of all mail servers which are authorized to send email for your domain(s)
- Consider all email servers which could be involved, including:
  - Your on-premise email server
  - Your ISP's email server
  - Any 3rd party email server that is allowed to send email on behalf of your domain(s)

SPF

Sender Policy Framework (SPF)

Setting Up – Sender Side

Modify your DNS by creating a new TXT record for SPF

Format of SPF txt record

v=spf1[ip4/6:][ipaddressesofemailservers] [include:[3rdpartydomainnames]] –all

- v=spf1 must start it…indicates version number even though only one version was ever released
- Include statement is for any third parties that send email on your behalf
- -all means that your SPF record is inclusive and to reject (hard fail) any other IP addresses or domains that claim they are sending email for your domains (~all indicates you recommend a “soft fail”, +all means no fails)

SPF

Sender Policy Framework (SPF)

v=spf1[ipaddressesofemailservers] [include:[3rdpartydomainnames]] –all

Examples

v=spf1 ip4:192.168.1.1 –all

v=spf1 192.168.1.1 192.168.1.2 192.168.1.3 –all

v=spf1 192.168.1.0/24 –all

v=spf1 192.168.1.1 include:example.com –all

v=spf1192.168.1.1 include:subdomain.example.com –all

v=spf1 192.168.1.1 include:example.com include:example.org –all

v=spf1 mx include:_spf.example.com –all

SPF

Sender Policy Framework (SPF)

Setting Up – Sender Side

If you are a **0365 or Exchange Online** customer:

Your SPF record must include Microsoft's 0365 email sending server's domain

v=spf1 [ipaddressesofemailservers] include:spf.protection.outlook.com

- v=spf1 include:spf.protection.outlook.com
  - No onsite email servers involved
- v=spf1 192.168.1.1 include:spf.protection.outlook.com
  - You use onsite email servers as part of your 0365 setup
- May already be done automatically for you

SPF

Setting up – Receiving side - 0365/Microsoft Exchange Online

- SPF, DKIM, and DMARC checking enabled by default
  - Verify (send an email to the domain and check the header)
- Failing emails will be placed in Quarantine/Junk/Spam folders by default unless *SPF Record Hard Fail* is enabled (covered next)
  - If SPF Record Hard Fail is enabled, Microsoft will reject failing records
- Additional Spoof Intelligence™ checking that goes beyond is enabled by default, relies on analysis of spoofed domains as detected by cloud-based Advance Threat Protection (ATP)
  - https://docs.microsoft.com/en-us/office365/securitycompliance/walkthrough-spoof-intelligence-insight

SPF

Setting up – Receiving side - 0365/Microsoft Exchange Online

To Enable SPF Record Checking/Hard Fail through the 0365 admin center:

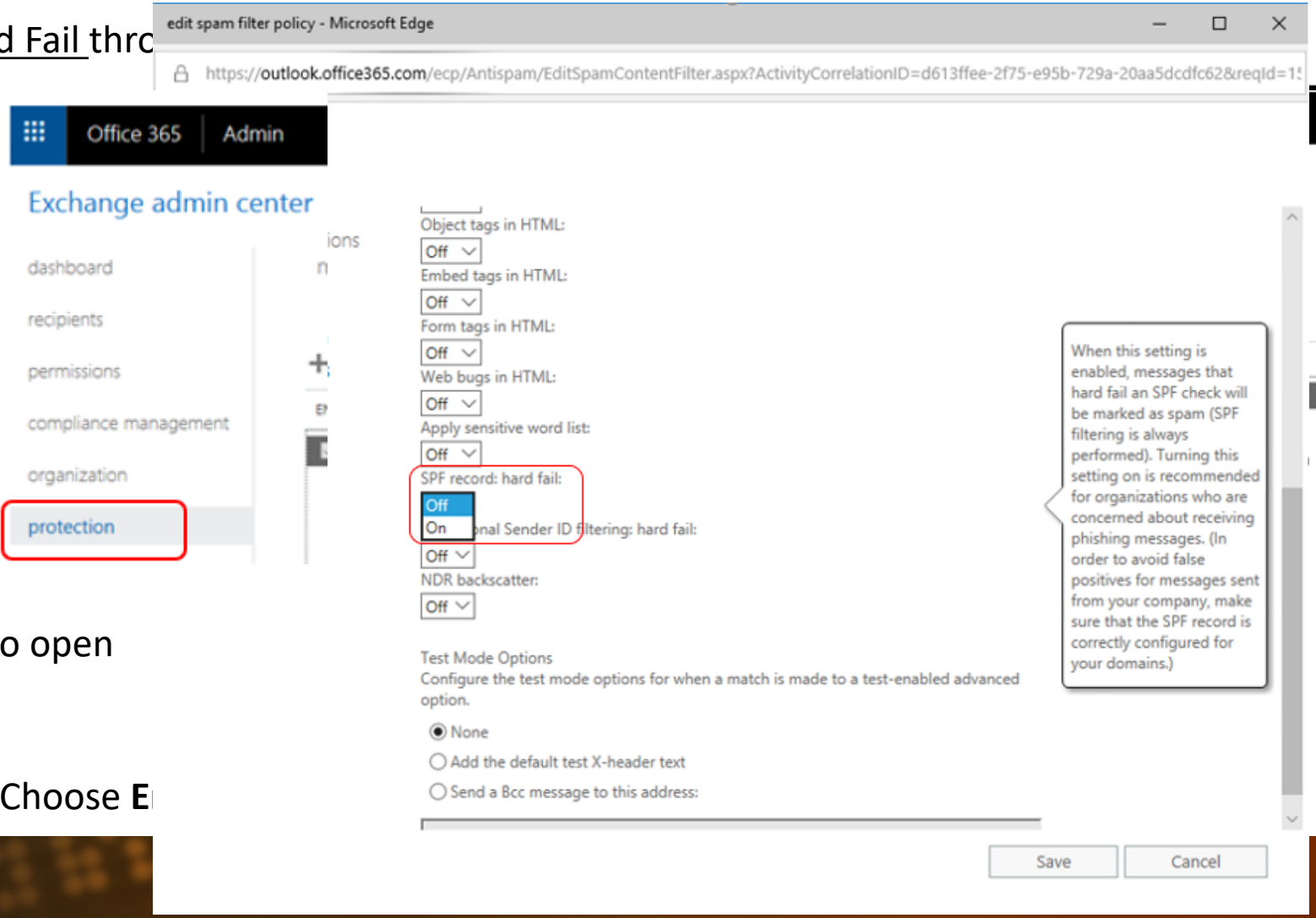
3. Sign into Office 365 with your work or school account
4. Select the app launcher icon in the upper-left and choose Admin
5. In Microsoft 365 admin center, click on Expand or Show all
6. Click on Exchange icon
7. Takes you to Exchange admin center
8. Choose **protection**
9. Choose **spam filter**
10. Choose domain, double-click to open
11. Choose **advanced options**
12. Choose **SPF record: hard fail**:. Choose **Enable**

SPF

Setting up – Receiving side - 0365/Microsoft Exchange Online

To Enable SPF Record Checking/Hard Fail thro

3. Sign into Office 365 with your
4. Select the app launcher icon i
5. In Microsoft 365 admin center
6. Click on Exchange icon
7. Takes you to Exchange admin
8. Choose **protection**
9. Choose **spam filter**
10. Choose domain, double-click to open
11. Choose **advanced options**
12. Choose **SPF record: hard fail**:. Choose **E**



SPF

Sender Policy Framework (SPF)

Setting Up – Sender Side - Gmail

If you are a **Gmail** customer with your MX domain hosted by Gmail:

Your SPF record must include Google's email sending server's domain

v=spf1 include:_spf.google.com ~all

- May already be done automatically for you
- SPF is automatically enabled on Receiving side

SPF

Sender Policy Framework (SPF)

Disabling SenderID Checking

- SenderID is an older protocol, essentially replaced by SPF

Create this TXT record in DNS for your domain(s)

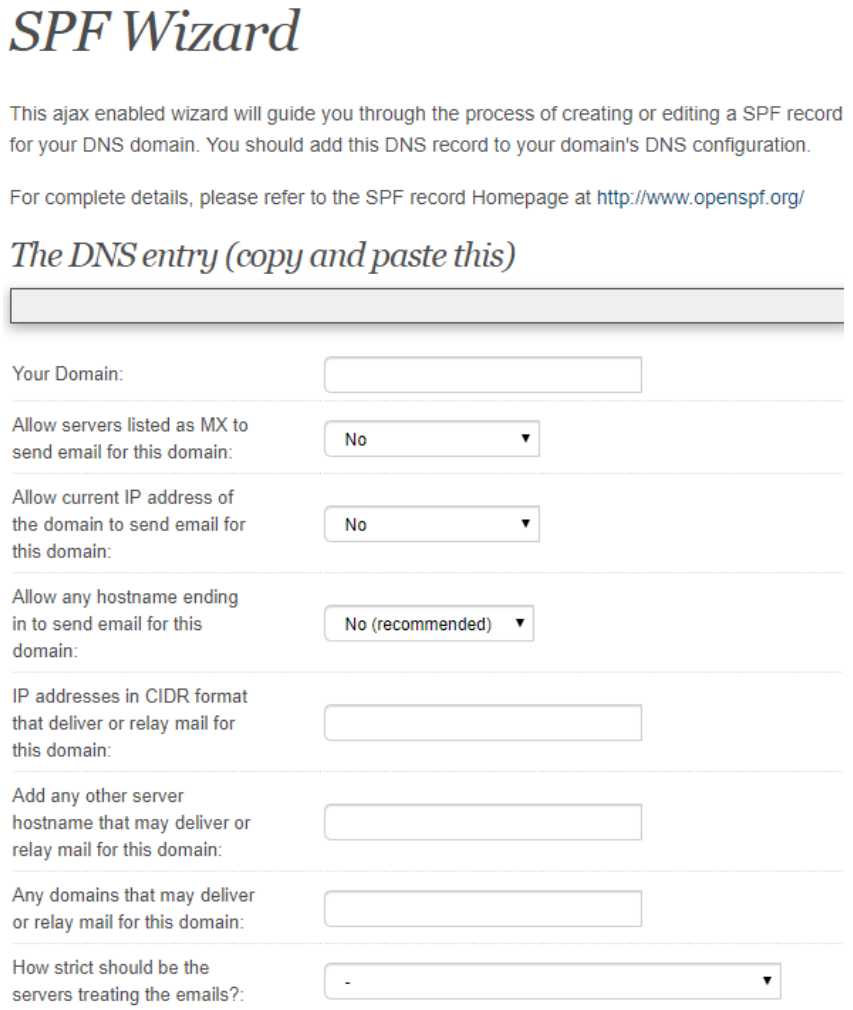
spf2.0/pra ?all

- Not having it can cause false-positives for SenderID checkers
- SenderID checking enabled by default on Exchange and 0365
- Record above essentially creates an “overly permissive” SenderID policy so anyone checking for SenderID will not reject email because of SenderID issues

SPF

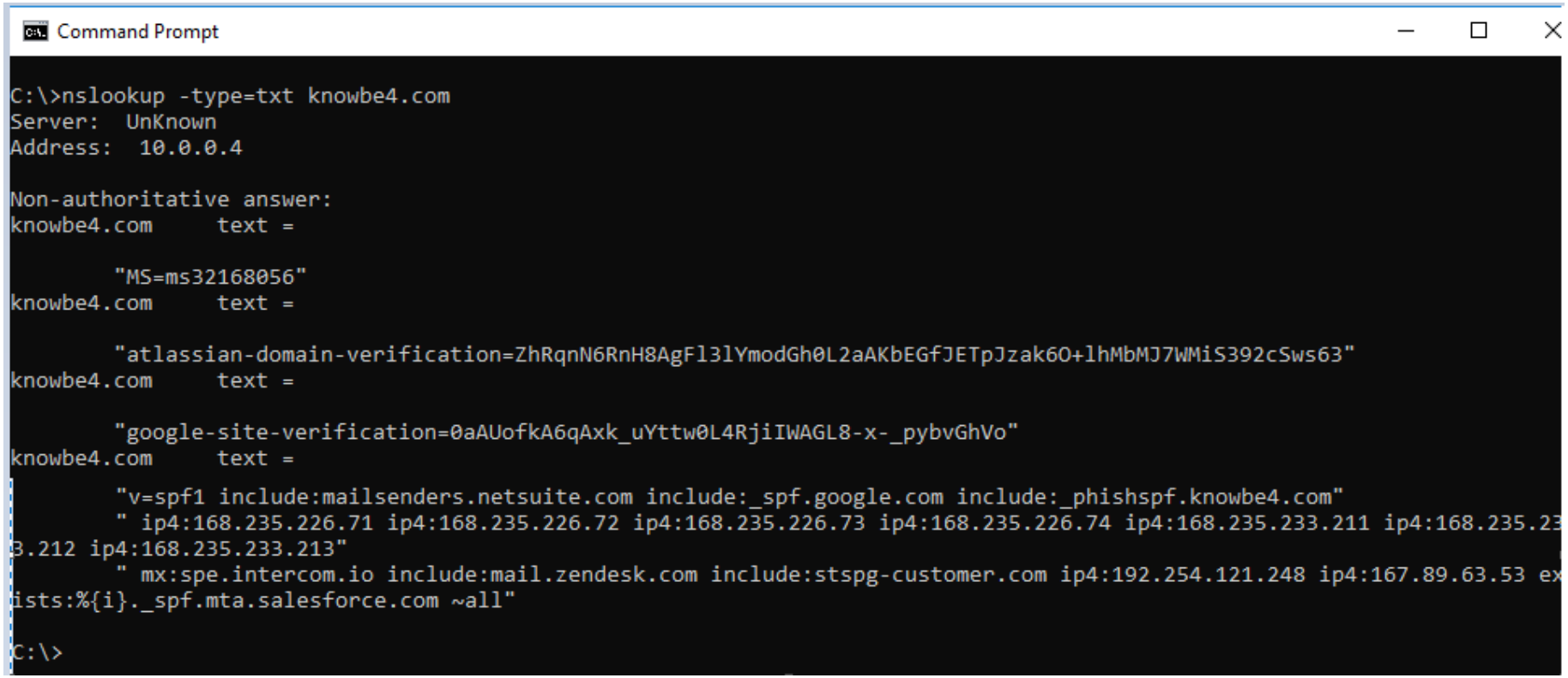
Sender Policy Framework (SPF)

- Site which can help you create your SPF record
- https://www.spfwizard.net/



SPF

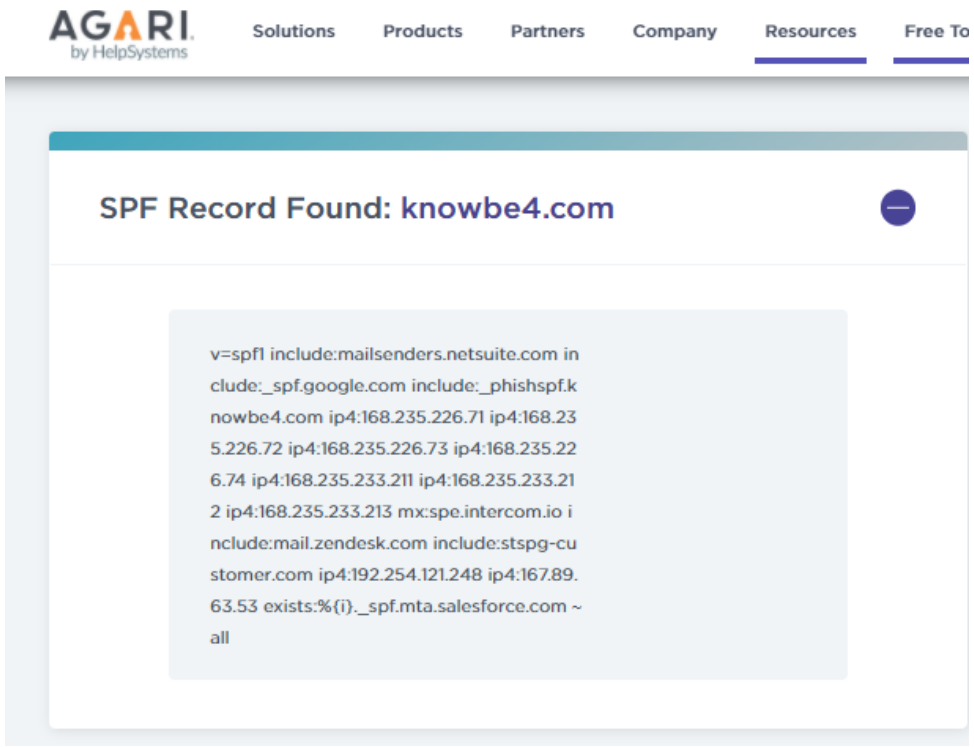
- How to verify in DNS
- Use nslookup –type=txt <domainname>

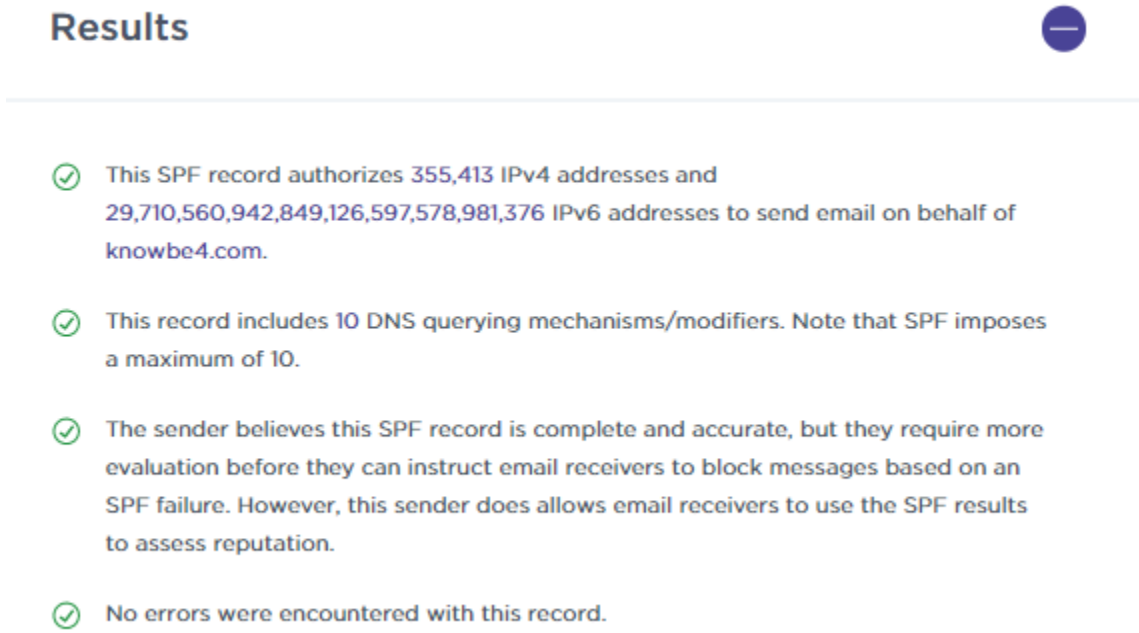


SPF

Lots of DMARC/SPF verification sites, including

- https://dmarcian.com, www.agari.com, https://www.kitterman.com, https://mxtoolbox.com, https://www.dmarcanalyzer.com





SPF

Sender Policy Framework (SPF)

Other Best Practices

- Use ~all qualifier initially for testing to cause “soft failures”
- Avoid creating a SPF DNS record that causes more than 10 DNS lookups
  - SPF verification sites, like https://www.dmarcian.com/ and https://www.dmarcanalyzer.com/spf/checker/ will tell you how many lookups it took

SPF

Sender Policy Framework (SPF)

Setting Up – Receiver Side

If you are a **0365 or Exchange Online** customer:

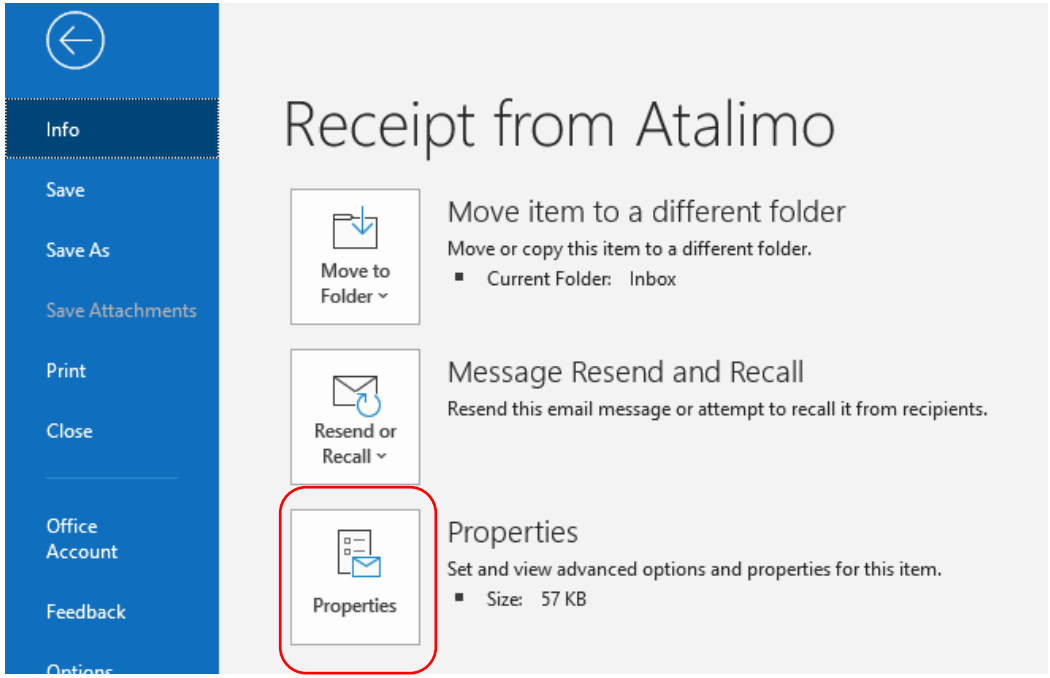
- Should automatically be enabled

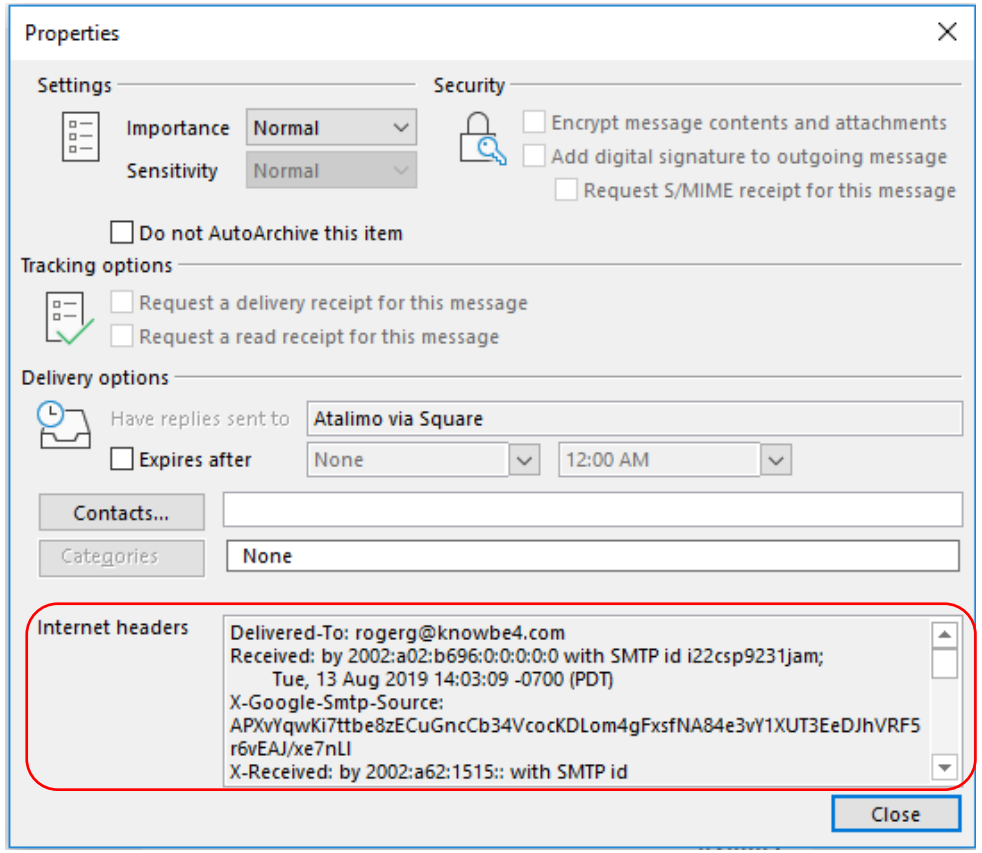
On-Premise - Microsoft Exchange (2010/2013/2016)

- Must be enabled on server using Powershell in Exchange Admin Console
- **& $env:ExchangeInstallPath\Scripts\Install-AntiSpamAgents.ps1**
- **Set-SenderIDConfig -ExternalMailEnabled $false**
  - SenderID not the same as SPF, and will cause too many false-positives

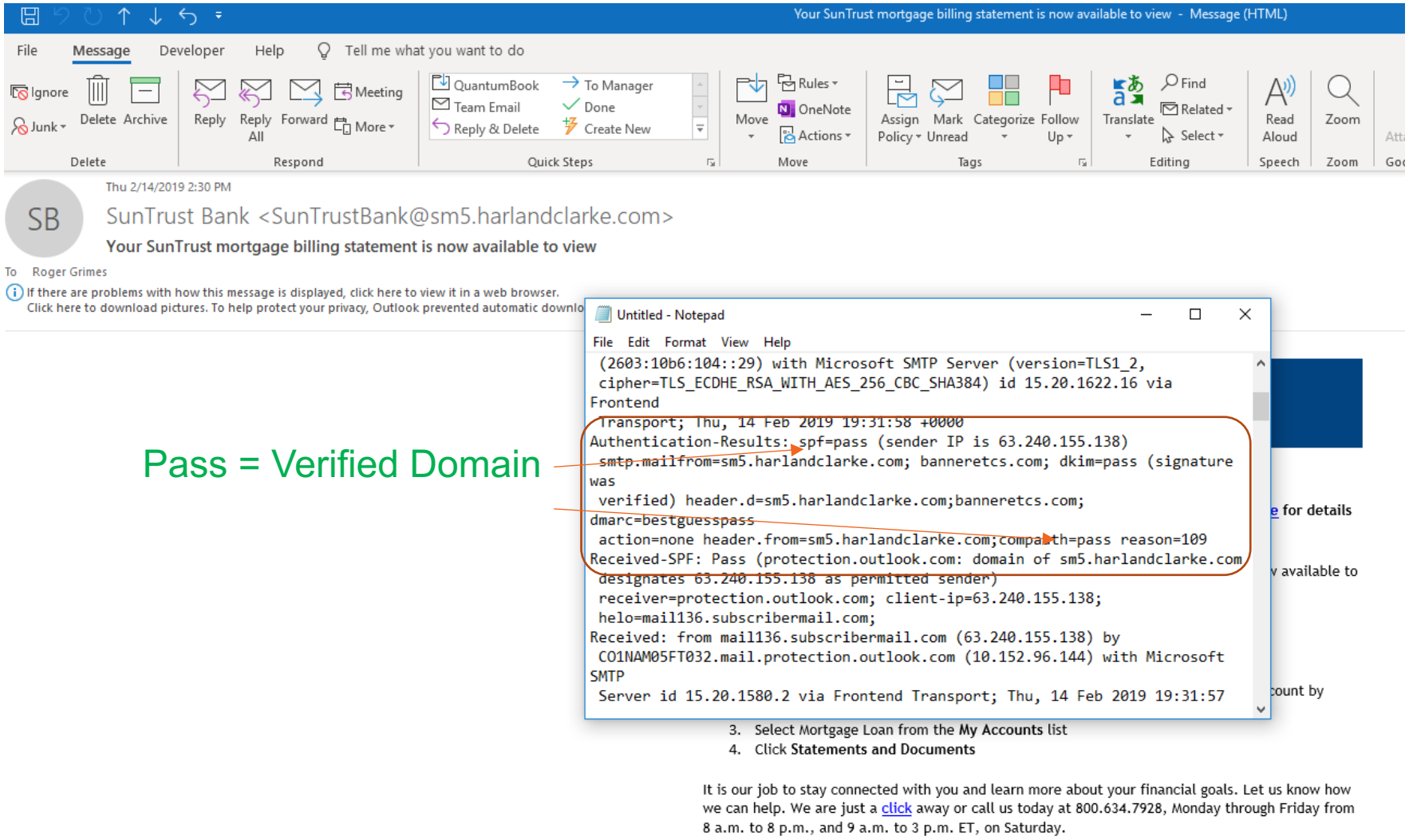
SPF Email Header Review

- You can view individual SPF, DKIM, and DMARC headers in email headers, if they exist
- In Outlook, open a message, choose **File**, **Properties**

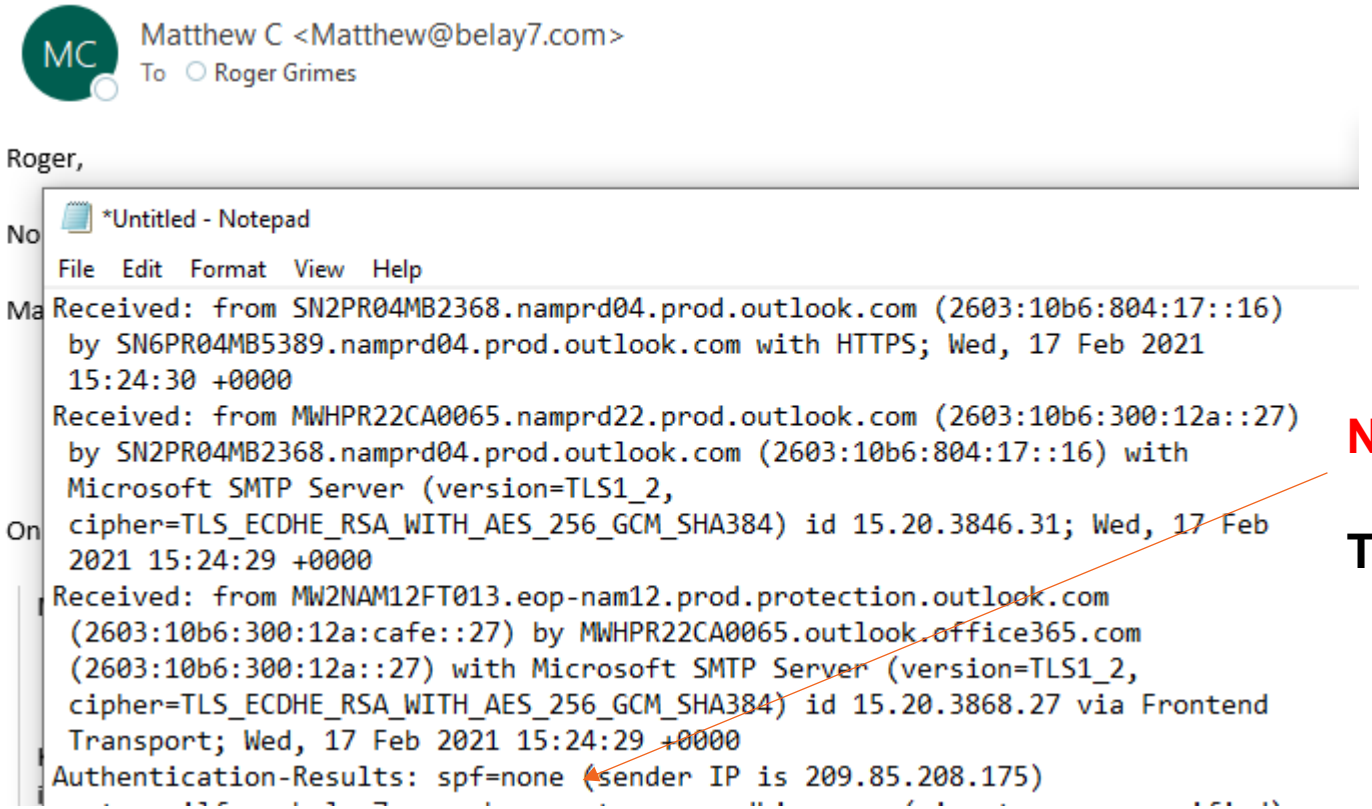




SPF Passes


Your SunTrust mortgage billing statement is now available to view - Message (HTML)
File Message Developer Help Tell me what you want to do
Ignore Junk Delete Archive
Reply Reply All Forward Meeting More
Delete Respond
QuantumBook Team Email Reply & Delete
To Manager Done Create New
Quick Steps
Move Rules OneNote Actions
Move
Assign Policy Mark Unread Categorize Follow Up
Tags
Translate Find Related Select
Editing
Read Aloud
Speech
Zoom
Zoom
Thu 2/14/2019 2:30 PM
SB
SunTrust Bank <SunTrustBank@sm5.harlandclarke.com>
Your SunTrust mortgage billing statement is now available to view
To Roger Grimes
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 downlo
Untitled - Notepad
File Edit Format View Help
(2603:10b6:104::29) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id 15.20.1622.16 via
Frontend
Transport; Thu, 14 Feb 2019 19:31:58 +0000
Authentication-Results: spf=pass (sender IP is 63.240.155.138)
smtp.mailfrom=sm5.harlandclarke.com; banneretcs.com; dkim=pass (signature
was
verified) header.d=sm5.harlandclarke.com;banneretcs.com;
dmarc=bestguesspass
action=none header.from=sm5.harlandclarke.com;compauth=pass reason=109
Received-SPF: Pass (protection.outlook.com: domain of sm5.harlandclarke.com
designates 63.240.155.138 as permitted sender)
receiver=protection.outlook.com; client-ip=63.240.155.138;
helo=mail136.subscribermail.com;
Received: from mail136.subscribermail.com (63.240.155.138) by
CO1NAM05FT032.mail.protection.outlook.com (10.152.96.144) with Microsoft
SMTP
Server id 15.20.1580.2 via Frontend Transport; Thu, 14 Feb 2019 19:31:57
Pass = Verified Domain
for details
available to
count by
3. Select Mortgage Loan from the My Accounts list
4. Click Statements and Documents
It is our job to stay connected with you and learn more about your financial goals. Let us know how we can help. We are just a click away or call us today at 800.634.7928, Monday through Friday from 8 a.m. to 8 p.m., and 9 a.m. to 3 p.m. ET, on Saturday.

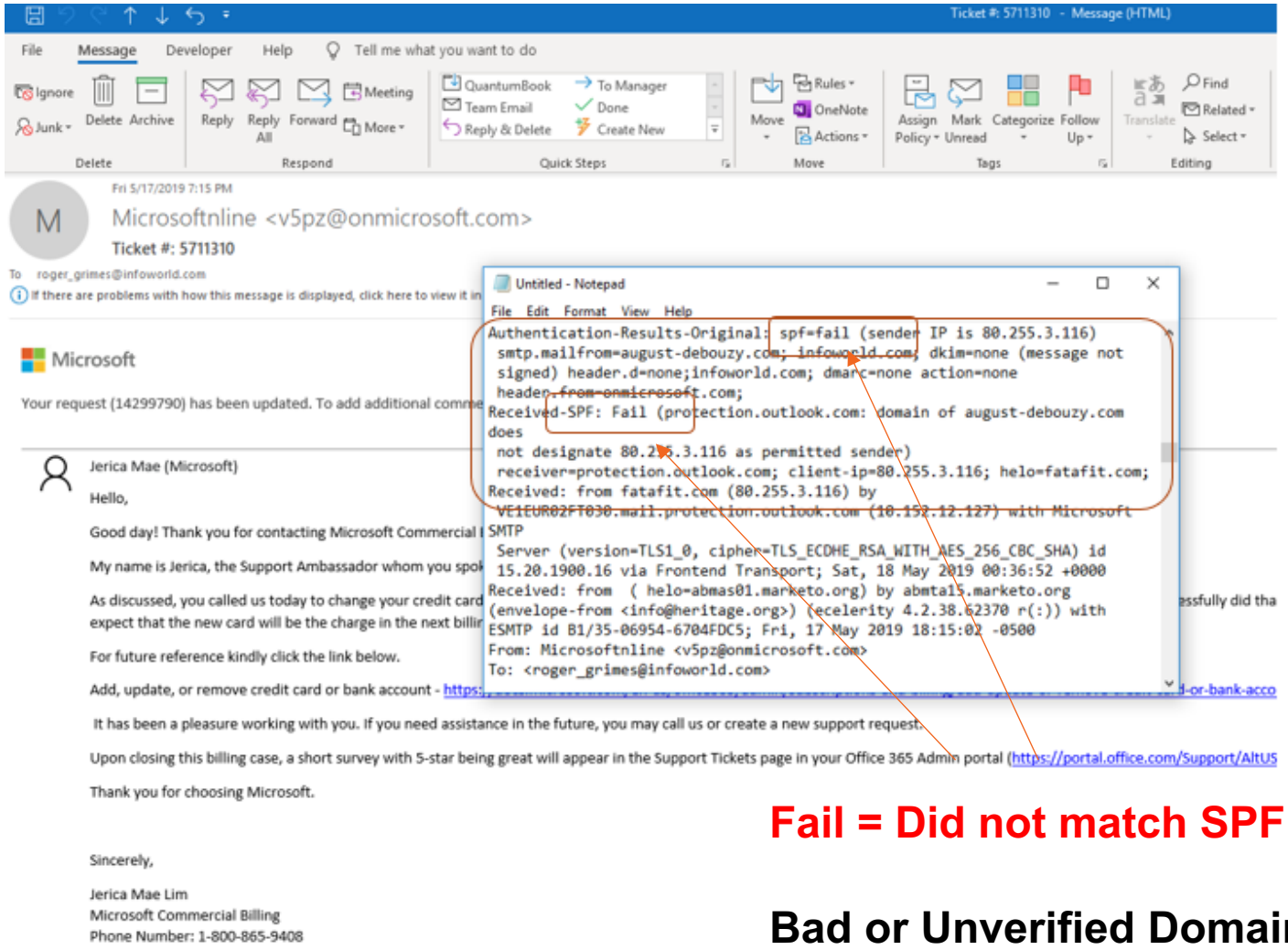
SPF = None



None = No SPF Record Found

Treated as a Fail by DMARC

SPF Fails



Fail = Did not match SPF record

Bad or Unverified Domain

SPF = Neutral

```
Delivered-To: rogerg@knowbe4.com
Received: by 2002:a02:cb0d:0:0:0:0:0 with SMTP id j13csp566593jap;
        Mon, 22 Feb 2021 10:02:30 -0800 (PST)
X-Google-Smtp-Source: ABdhPJzizfIaf0oCB85ydrqjDUAJEqR2LYzHkrlPZNtv38MaEVVQ3Wb2M2K970WExhzTkWJBgpx2
X-Received: by 2002:a17:90a:4146:: with SMTP id m6mr10355595pjg.118.1614016950581;
        Mon, 22 Feb 2021 10:02:30 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1614016950; cv=none;
        d=google.com; s=arc-20160816;
        b=PutKKsziPfZXLFfY/Zvd3jxPjYCgc1kGqe0EoFLQwMGMOzHTg5jTDku5bD2ilIU21k
         /fLyuB7WM815Z/AO0azaw0KOjMGwevN/L7VQ/eNnPVxcLYvaGRlrbb1Zqd80/70U51TP
         EM/5QKWknb4AxmFdSncEVZuOqRoFNsm6pioMfKUCn6Z9CwzdqsgXtCYDyEiZMiUaM/u5
         fNrBpoeoM0b2tRLDU/cbG4EX6PbJPkQK9I1NVoRXwM3yqWEKBFGeUKgWkVuXUl132B0A
         2Zuw0P0k5ahfjTK5Ffe4U9gzxvrrabglw1Ct7MAf/YeGz6rWFL8KZp+FgdoTcXU7T/FT
         u5nA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=message-id:in-reply-to:to:references:date:subject:mime-version:from;
        bh=pqDzm9GiaHmkn/x0wdp1W7dQgmO3jk+6aZYGuJ3mA7M=;
        b=IT2z/34d1hPGUknJljSJqSVV2msIxPX1x+hr0ODk5bm0WQQuVxYf/sdIkofjTcK3ev
         yF6BSa1i9ZAt0so71ZoTX20kC/HfuGpHY9jUqHi59AE+IINJT/dpBVYb11cs2SGhEO6s
         Nj1fCs3+8l+MBOdq42pnwtq7d2bITjA0NbywMmdhyb89Ni2xSxcSAj9EfK5053mbGm8H
         M7bH0UCjhAHQsa8yljGIFOgjeCVtZBHTPUb1/PkAWr5yROPgiiLJvFKgGesFWGbtzDH9
         C96PC7sTGAT6PNpst/VGMIJBIQQ7VZkJgXrfZ8vttvuwVPIC3lyezl2Jr32Qs1pY8o9I
         WPsQ==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=neutral (google.com: 68.178.252.239 is neither permitted nor denied by best guess record for domain of alison@eleveneventsbbg.com)
```

Neutral = Bad or Unverified Domain

?all in SPF record will cause

Can be pass or fail in DMARC depending on how configured

SPF Passes and Fails

Received: from DM6PR12MB2921.namprd12.prod.outlook.com (2603:10b6:208:178::46)
by MN2PR12MB4534.namprd12.prod.outlook.com with HTTPS via
MN2PR19CA0033.NAMPRD19.PROD.OUTLOOK.COM; Mon, 27 Apr 2020 14:02:50 +0000
Received: from DM5PR05CA0018.namprd05.prod.outlook.com (2603:10b6:3:d4::28) by
DM6PR12MB2921.namprd12.prod.outlook.com (2603:10b6:5:182::17) with Microsoft
SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
15.20.2937.22; Mon, 27 Apr 2020 14:02:48 +0000
Received: from DM6NAM11FT067.eop-nam11.prod.protection.outlook.com
(2603:10b6:3:d4:cafe::7f) by DM5PR05CA0018.outlook.office365.com
(2603:10b6:3:d4::28) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.2958.14 via Frontend
Transport; Mon, 27 Apr 2020 14:02:48 +0000
Authentication-Results: spf=fail (sender IP is 199.192.65.7)
smtp.mailfrom=241394m.knowbe4.com [redacted]; dkim=fail (body hash
did not verify) header.d=241394m.knowbe4.com; [redacted]
dmarc=temperror action=none header.from=knowbe4.com;compauth=softpass
reason=201
Received-SPF: Fail (protection.outlook.com: domain of 241394m.knowbe4.com does
not designate 199.192.65.7 as permitted sender)
receiver=protection.outlook.com; client-ip=199.192.65.7;
helo=mailgwsf03.accessabacus.com;
Received: from mailgwsf03.accessabacus.com (199.192.65.7) by
DM6NAM11FT067.mail.protection.outlook.com (10.13.172.76) with Microsoft SMTP
Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
15.20.2937.15 via Frontend Transport; Mon, 27 Apr 2020 14:02:46 +0000
Received: from pps.filterd (mailgwsf03.accessabacus.com [127.0.0.1])
by mailgwsf03.accessabacus.com (8.16.0.27/8.16.0.27) with SMTP id 03RDx221011772
[redacted] Mon, 27 Apr 2020 10:02:46 -0400
Authentication-Results-Original: accessabacus.com; spf=pass
smtp.mailfrom=1axb3295csw37978378madwezr9grr3ggjcwdk@241394m.knowbe4.com
Received: from pgg3nm.241394m.knowbe4.com (pgg3nm.241394m.knowbe4.com [54.174.60.48])
by mailgwsf03.accessabacus.com with ESMTP id 30ny0truv2-1
(version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128 verify=NOT)
[redacted] Mon, 27 Apr 2020 10:02:44 -0400

"Last mile", receiver-side inspection engine forwarded email and it fails SPF because it is not a permitted sender

Original sender SPF passed

DKIM

KnowBe4
Human error. Conquered.

DKIM

Domain Keys Identified Mail (DKIM)

- Designed to prevent sender email address domain spoofing by receiver verifying the digital signature of the mail server domain sent with each email
- Checks for domain spoofing related to what is in 5322 Display Name field
- RFC 6376 (old one is 5585) (http://www.dkim.org/specs/rfc6376.pdf)
- Relies on DKIM/TXT records in DNS
- Sender must have public/private key pair
- Server signs each outgoing email
- Receiver side: All validation is done before email gets to end-user

DKIM

Setting up – General Process – Sender Side

- Plan, decide, and document DKIM settings
- Get Private/Public (Asymmetric Key) for sending email server(s)

For onsite sending email servers*:

- Install key pair on sending email server
- Enable DKIM DNS record on DNS servers (one for each key pair used)
- Enable DKIM on email server
- Verify and test

*for offsite email services, contact your provider

DKIM

Setting up – General Process – Receiver side

- Enable DKIM checking on email server (if possible)
- Gmail and 0365 do DKIM checks (and SPF and DMARC) by default
- Verify and test

*for offsite email services, contact your provider

DKIM

Domain Keys Identified Mail (DKIM)

DKIM DNS Record Format

- **selector._domainkey.[domainname] IN TXT “v=DKIM1;p=xxxxx”**
- Where p is the public key of email server in Base64 format

Example:

- selector._domainkey.example.com IN TXT “v=DKIM1;p=RAG…123”

DKIM

Setting up – Sending side - 0365/Microsoft Exchange Online

1. You do not need to create or get a private/public key pair, Microsoft does this part for you
2. Publish DNS CNAME records (you'll need at least two per domain)

Examples:

selector1._domainkey =
selector1-example-com._domainkey.example.onmicrosoft.com
selector2._domainkey =
selector2- example-com._domainkey.example.onmicrosoft.com

DKIM

Setting up – Sending side - 0365/Microsoft Exchange Online

To Enable DKIM signing for your domain through the 0365 admin center:

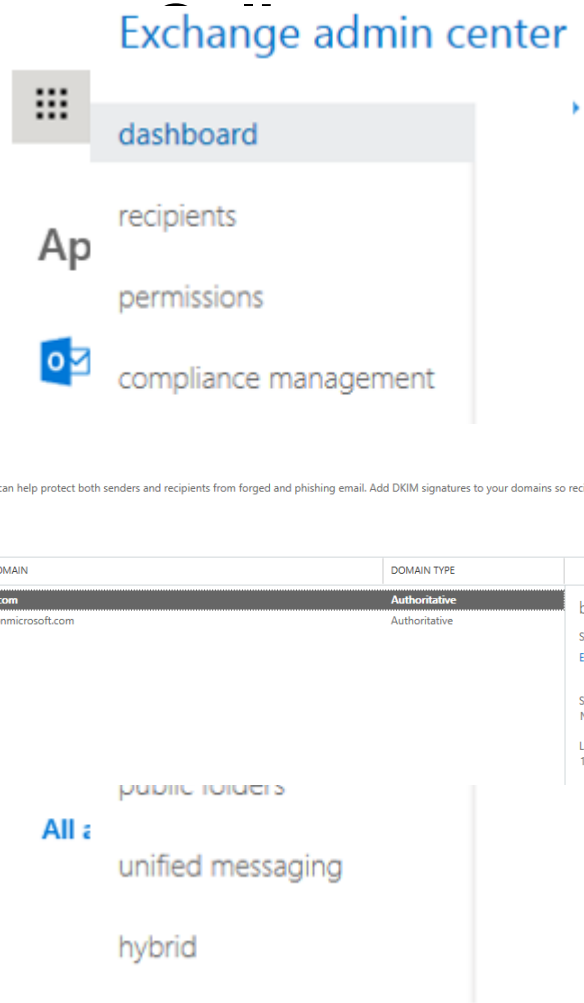
3. Sign into Office 365 with your work or school account
4. Select the app launcher icon in the upper-left and choose Admin
5. In Microsoft 365 admin center, click on Expand or Show all
6. Click on Exchange icon
7. Takes you to Exchange admin center
8. Choose **protection**
9. Choose **dkim**
10. Choose domain you want to enable or view DKIM status on
11. Choose **Enable**

DKIM

Setting up – Sending side - 0365/Microsoft Exch

To Enable DKIM signing for your domain through the 0365 admin center:

3. Sign into Office 365 with your work or school account
4. Select the app launcher icon in the upper-left and choose Admin
5. In Microsoft 365 admin center, click on Expand or Show all
6. Click on Exchange icon
7. Takes you to Exchange admin center
8. Choose **protection**
9. Choose **dkim**
10. Choose domain you want to enable or view DKIM status on
11. Choose **Enable**



DKIM

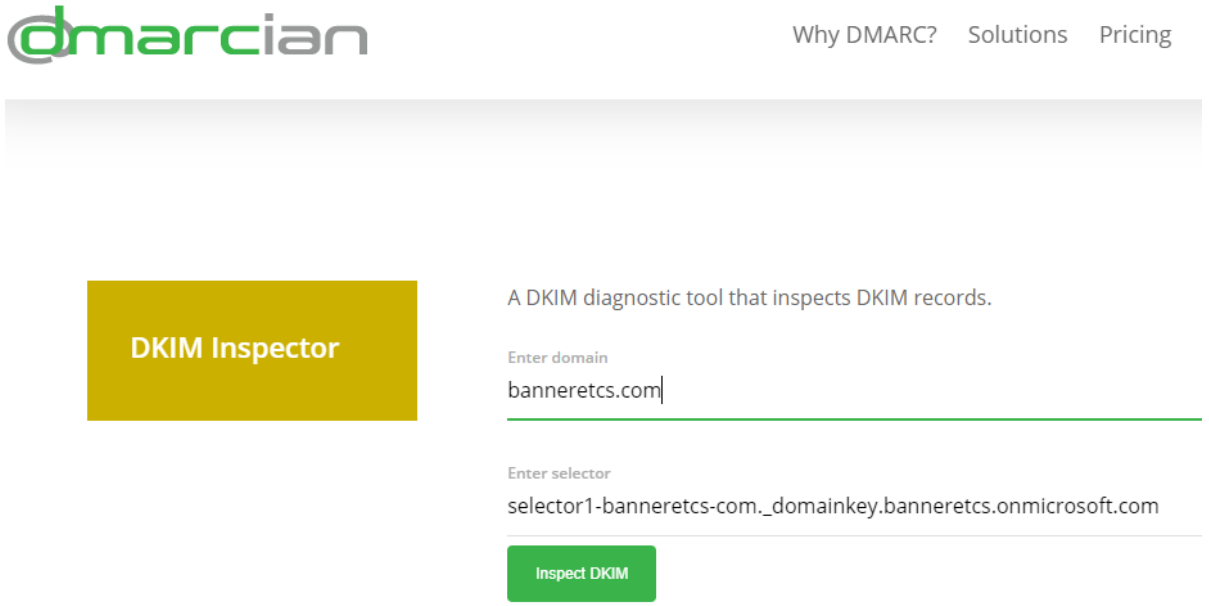
Domain Keys Identified Mail (DKIM)

Setting up – Sending Side - On-Premise Microsoft Exchange

- Exchange does not natively support DKIM
- Must use an SMTP gateway inline with Exchange that does
- Manually install your key pair on gateway and enable DKIM/SPF/DMARC

Domain Keys Identified Mail (DKIM)

Verify DKIM is Setup Correctly – Lots of verification sites

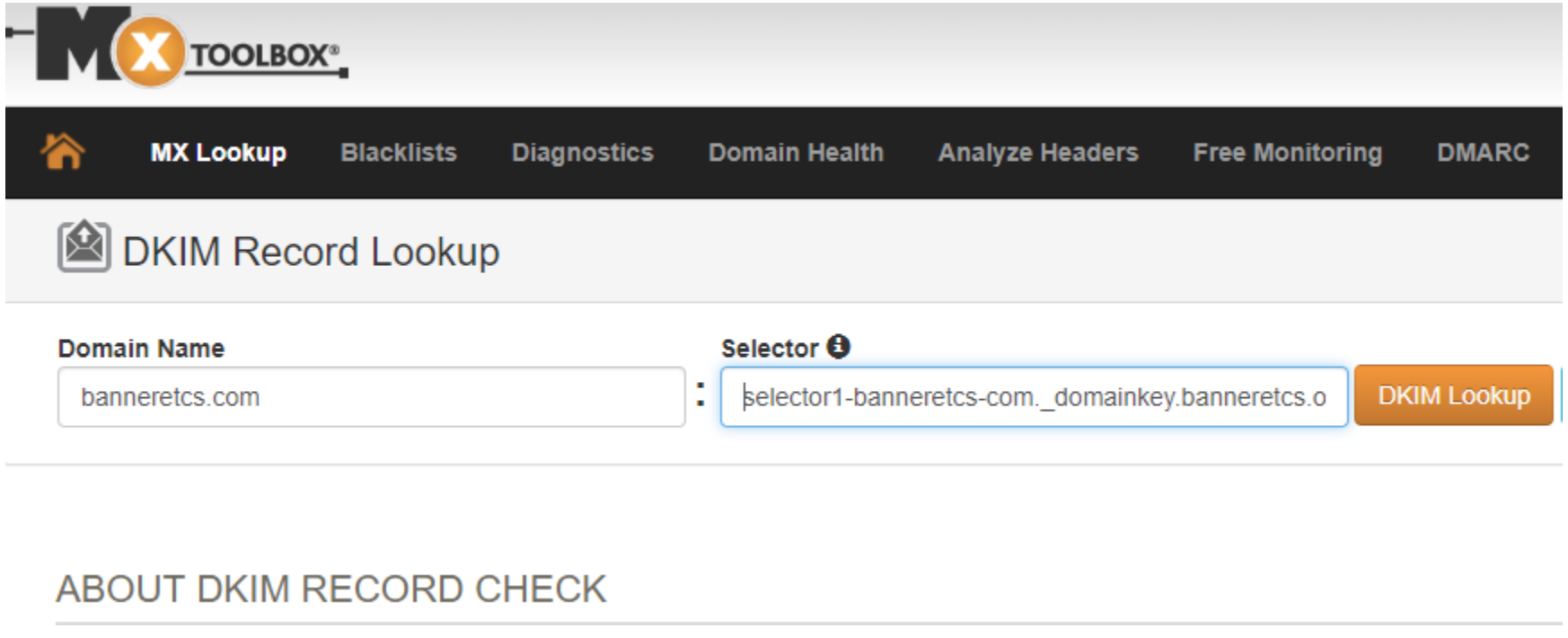


https://dmarcian.com/dkim-inspector/

DKIM

Domain Keys Identified Mail (DKIM)

Verify DKIM is Setup Correctly – Lots of verification sites



https://mxtoolbox.com/dkim.aspx

DKIM

Domain Keys Identified Mail (DKIM)

Example DKIM Signature in Email Header

```
DomainKey-Signature: q=dns; a=rsa-sha1; c=nofws;
        s=dkim2014q3; d=sm5.harlandclarke.com;
        h=DKIM-Signature:MIME-Version:Message-ID:X-SM-Email-Key:Content-Type:X-
mid:X-ppid:Subject:Reply-To:To:From:X-appid:List-Unsubscribe:Date:X-dit;
        b=FmR71Faj+TueNTwhVx5uHkANPkWiTltfr/iJ1nmHI407FxLOriqPsrTCC6Vg2Uxf
        soFpUlpO23VDnzRhhvsB6vbt7TNU1D6vynx3+zRmXOnzw/T3u5dfo00ctwm/0fxq
        ksQqXuGHIn6bZ3V67IRJcbDUrD9FtgaTED/WLaTYNFQ=
DKIM-Signature: v=1; a=rsa-sha1; d=sm5.harlandclarke.com; s=dkim2014q3;
c=relaxed/simple;
        q=dns/txt; i=@sm5.harlandclarke.com; t=1550172717;
        h=From:Subject:Date;
        bh=xcDeDjuUmtqYwVNulH/MIi6s53k=;
        b=XSBvB3TppRpjoEkKt0vCEWqpcDFyNglKjTAlDJpJm9RfpJtD7NjY4zoqczwwxyMW
        H4r+LdAJFNfvufjm+mbbzU8RHo7pM7C32MPRBt8BSKfEi/OOKxR78U5aUBJUlaTf
        2WW0mvZTbsEEvKC3khL6b2or7LXVqYsO3qkfWvxbkok=;
```

DKIM Passes

Domain Keys Identified Mail (DKIM)

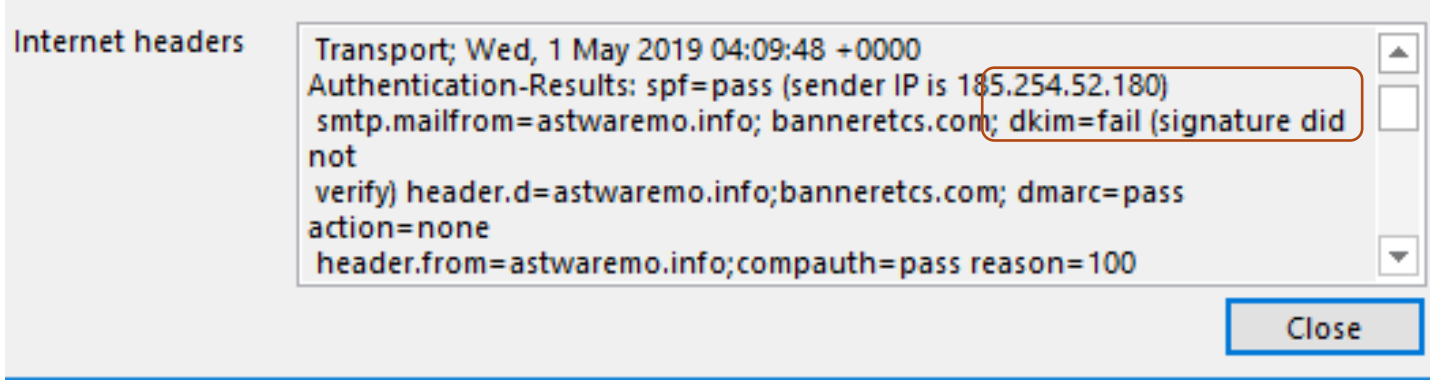
Example DKIM Email Header Verification Results

```
Received: from CO1NAM05FT032.eop-nam05.prod.protection.outlook.com
 (2a01:111:f400:7e50::207) by CO2PR04CA0151.outlook.office365.com
 (2603:10b6:104::29) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id 15.20.1622.16 via Frontend
 Transport; Thu, 14 Feb 2019 19:31:58 +0000
Authentication-Results: spf=pass (sender IP is 63.240.155.138)
 smtp.mailfrom=sm5.harlandclarke.com; banneretcs.com; dkim=pass (signature was
 verified) header.d=sm5.harlandclarke.com;banneretcs.com; dmarc=bestguesspass
 action=none header.from=sm5.harlandclarke.com;compauth=pass reason=109
```

DKIM Fails

Domain Keys Identified Mail (DKIM)

Example DKIM Email Header Verification Results



DMARC

KnowBe4
Human error. Conquered.

DMARC

- **Domain-based Message Authentication, Reporting and Conformance**
- Sender can indicate whether they use SPF and/or DKIM, which the receiver can verify and rely on, and how a receiver should treat failed messages

TXT IN "v=DMARC1;p=quarantine;pct=100;rua=mailto:dmarc@example.com;"

P =

- None – Take no special treatment for failed emails
- Quarantine – Treat as suspicious
- Reject – Reject email at server before it gets to client

PCT=percentage of emails to apply DMARC policy to

DMARC

p=quarantine

- What happens depends on the receiving server and/or client

It can mean:

- Put in spam, quarantine, or other folder to be further investigated
- Forward to another service or server for more automated inspection
- Notify user that email was quarantined and allow them to inspect
- Notify user that email was quarantined and allow IT to inspect
- Ignore and just treat like normal email (sadly)

DMARC – Other DNS options

- **Adkim -** Indicates strict or relaxed DKIM identifier alignment. The default is relaxed.
- **aspf** - Indicates strict or relaxed SPF identifier alignment. The default is relaxed.
  - For both, strict means that the DKIM and/or SPF DNS check, the domain shown in the email must exactly (not different at all) match what is shown in DNS
  - Relaxed (the default) – the check will accept different sub-domains under the same domain as valid.

- **Rf** - format for message failure reports. The default is Authentication Failure Reporting Format, or "AFRF."
- **Ri** - the number of seconds elapsed between sending aggregate reports to the sender. The default value is 86,400 seconds or a day.

DMARC – Other DNS options

fo tag

- Dictates what type of authentication and/or alignment vulnerabilities are reported back

There are four values to fo: (0 (default) , 1, d, s)

- **0**: Generate a DMARC failure report if all underlying authentication mechanisms fail to produce an aligned “pass” result. (Default)
- **1**: Generate a DMARC failure report if any underlying authentication mechanism produced something other than an aligned “pass” result.
- **d**: Generate a DKIM failure report if the message had a signature that failed evaluation, regardless of its alignment.
- **s**: Generate an SPF failure report if the message failed SPF evaluation, regardless of its alignment.
- The default is “fo=0”. Use fo:1 to generate the most comprehensive failure reports, providing that much more detail, especially during initial testing and troubleshooting

Info from: https://blog.returnpath.com/demystifying-the-dmarc-record/,

DMARC

- Sender can indicate whether they use SPF and/or DKIM, which the receiver can verify and rely on, and how a receiver should treat failed messages

TXT IN "v=DMARC1;p=quarantine;pct=100;rua=mailto:dmarc@example.com;"

- rua: Indicates where aggregate DMARC reports emailed to
- ruf: Indicates where forensic DMARC reports should be emailed to

DMARC

DMARC Reports

- DMARC reports - Aggregate and Forensic
- When enabled will be sent to you at least daily from big ISPs and emailers
- Some are sent in XML-format and some text-based formats
- May be in a zip file
- Many services and tools around the Internet to help you parse and more easily read them, including:
  - DMARC Analyzer (https://www.dmarcanalyzer.com)
  - RdDMARC (https://www.taugh.com/rddmarc/)
  - DMARC Reports Parser (https://github.com/techsneeze/dmarcts-report-parser)

DMARC Reports

DMARC (RUA) Aggregate Reports

- Sent daily about daily cumulative results relating to your DMARC'd domains from participating DMARC receivers who get emails claiming to be from your domains

Includes:

- How many emails they received claiming to be from your domain
- How many failed DMARC checking
- How many passed DMARC checking

DMARC

DMARC Aggregate Report - Example

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <report_metadata>
    <org_name>google.com</org_name>
    <email>noreply-dmarc-support@google.com</email>
extra_contact_info>[removed]</extra_contact_info>
    <report_id>7241837801886321635</report_id>
    <date_range>
      <begin>1431388880</begin>
      <end>1431475203</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>example.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>none</p>
    <sp>none</sp>
    <pct>100</pct>
  </policy_published>
```

```
<record>
  <row>
    <source_ip>example.com</source_ip>
    <count>2</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>pass</dkim>
      <spf>pass</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>example.com</header_from>
  </identifiers>
  <auth_results>
    <dkim>
      <domain>example.com</domain>
      <result>pass</result>
    </dkim>
    <spf>
      <domain>example.com</domain>
      <result>pass</result>
    </spf>
  </auth_results>
</record>
'feedback>
```

DMARC Reports

DMARC (RUF) Forensic Reports

- Diagnostic info sent for each failed email, text-based in an email

Includes (among many fields):

- Reason(s) for failure (SPF, DKIM, DMARC)
- DKIM Signature if included
- IP address message was sent from
- Time message was received
- Domain HELO info/MAIL FROM
- Subject Line

DMARC

DMARC Forensic Report Example

Content-Type: text/plain; charset="us-ascii"
MIME-Version 1.0
Content-Transfer-Encoding: 7bit

This is a spf/dkim authentication-failure report for an email message received from IP 192.168.1.1 on Wed, 14 Aug 2019 10:24:11 -0500
Below is some detail information about this message:

1. SPF-authenticated Identifiers: none;
2. DKIM-authenticated Identifiers:none;
3. DMARC Mechanism Check Result: Identifier non-aligned, DMARC mechanism check failures;

For more information please check Aggregate Reports or mail to dmarc@exampleparticipatingISP.com
--==========431124115425462452425432 5====
Content-Type: message/feedback-report
MIME-Version 1.0
Feedback-Type: auth-failure
User-Agent: ExampleISP/1.0
Version: 1
Original-Mail-From: <DMARCUsingDomain.com>
Arrival-Date: Wed, 14 Aug 2019 10:24:11 -0500
Source-IP: 192.168.1.1
Reported-Domain: example.com
Original-Envelope-Id: badguy.domain
Authentication-Results: exampleparticipatingISP.com; dkim=non; spf=fail smtp.mail-from=user@example.com
Delivery-Result: reject
--==========431124115425462452425432 5====
Content-Type: text/rfc822-headers; charset="us-ascii"
MIME-Version 1.0
Content-Transfer-Encoding: 7bit
Received: from badguydomain.com ([10.1.1.0])
by exampledomain.com with SMTP id 23m41mqtq322Fv.1
for <receivingusername@goodguydomain.com>; Wed, 14 Aug 2019 10:24:11 -0500
Date: Wed, 14 Aug 2019 10:24:02 -0500
From: "FakeName@Example.com" <fakename@example.com>
To: receivingusername@goodguydomain.com
Subject: Need to change wiring instructions ASAP!
X-Priority: 3
Mime-Version: 1.0
Message-ID: fakename@example.com
Content-Type: multipart/mixed;

DMARC

Example DMARC Reports from Tools and Services

DMARC Reports

Start Date	End Date	Domain	Reporting Organization	Report ID	Messages
Mon, 11 Dec 2017 07:00:00 +0700	Tue, 12 Dec 2017 06:59:59 +0700	ui.ac.id	Yahoo! Inc.	1513043116.781040	11,769
Mon, 11 Dec 2017 07:00:00 +0700	Tue, 12 Dec 2017 07:00:00 +0700	ui.ac.id	emailsrvr.com	a25965a5-dc32-4611-b4d1-da07f074265e	9
Mon, 11 Dec 2017 07:00:00 +0700	Tue, 12 Dec 2017 07:00:00 +0700	ui.ac.id	linkedin.com	linkedin.com!ui.ac.id!1512950400!1513036800!coffee	7
Tue, 12 Dec 2017 07:00:00 +0700	Wed, 13 Dec 2017 07:00:00 +0700	ui.ac.id	linkedin.com	linkedin.com!ui.ac.id!1513036800!1513123200!star	7
Tue, 12 Dec 2017 07:00:00 +0700	Wed, 13 Dec 2017 07:00:00 +0700	ui.ac.id	linkedin.com	linkedin.com!ui.ac.id!1513036800!1513123200!chips	16
				Sum:	11,808

Brought to you by TechSneeze.com - dave@techsneeze.com

DMARC

Example DMARC Reports from Tools and Services

DMARC Reports

Start Date	End Date	Domain	Reporting Organization	Report ID	Messages
Wed, 20 May 2015 16:46:46 +0000	Fri, 23 Oct 2015 09:00:18 +0000	tachtler.net	[redacted]	[redacted]	16
Thu, 22 Oct 2015 02:00:00 +0000	Fri, 23 Oct 2015 01:59:59 +0000	tachtler.net	google.com	[redacted]	22
Thu, 22 Oct 2015 09:00:00 +0000	Fri, 23 Oct 2015 09:00:00 +0000	tachtler.net	[redacted]	[redacted]	1
Fri, 23 Oct 2015 08:57:41 +0000	Fri, 23 Oct 2015 09:00:07 +0000	tachtler.net	[redacted]	[redacted]	2

Thu, 22 Oct 2015 02:00:00 +0000

IP Address	Host Name	Message Count	Disposition	Reason	DKIM Domain	DKIM Result	SPF Domain	SPF Result
0.0.0.0	0.0.0.0	1	none		tachtler.net	pass	googlemail.com	pass
0.0.0.0	0.0.0.0	1	none		tachtler.net	pass	listen.jpberlin.de	neutral
0.0.0.0	0.0.0.0	1	none		tachtler.net	pass	srs.smtpin.rzone.de	none
94.186.131.102	mx12.globalways.net	1	none		tachtler.net	pass	listen.jpberlin.de	neutral
148.251.78.214	mail.ambiente.one	2	none		tachtler.net	pass	tachtler.net	neutral
162.209.70.180	593490-www8.www8.vividracing.com	1	none				tachtler.net	neutral
162.209.70.219	674731-www5.vividracing.com	3	none				tachtler.net	neutral
209.85.213.177	mail-ig0-f177.google.com	1	none				gmail.com	pass
209.85.223.173	mail-io0-f173.google.com	1	none				gmail.com	pass
209.85.223.180	mail-io0-f180.google.com	1	none				gmail.com	pass
209.85.223.182	mail-io0-f182.google.com	1	none				gmail.com	pass
212.227.17.12	mout.web.de	1	none		tachtler.net	fail	listen.jpberlin.de	neutral
213.203.238.6	ilpostino.jpberlin.de	7	none		tachtler.net	pass	listen.jpberlin.de	pass

Brought to you by TechSneeze.com - dave@techsneeze.com

DMARC

Example DMARC Reports from Tools and Services

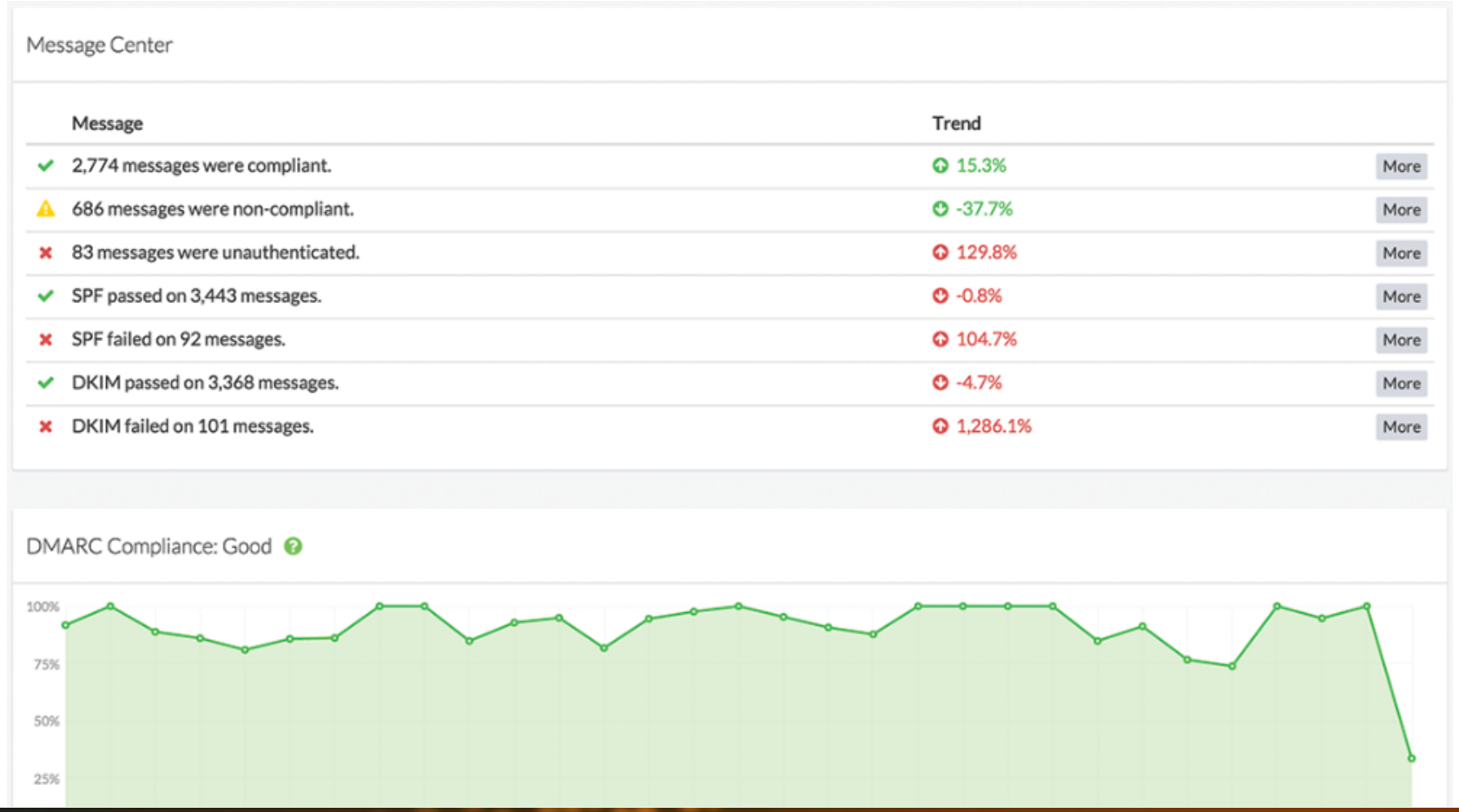
DMARC Reports

Hostname(s): on off
Sort order: ascending decending
Domain(s): [all]
Organisation(s): [all]
Time: 2018-05

Start Date	End Date	Domain	Reporting Organization	Report ID	Messages
Tue, 01 May 2018 17:00:00 -0700	Wed, 02 May 2018 16:59:59 -0700	techsneeze.com	FastMail Pty Ltd	[redacted]	1
Tue, 01 May 2018 17:00:00 -0700	Wed, 02 May 2018 16:59:59 -0700	example.com	google.com	[redacted]	1
Tue, 01 May 2018 17:00:00 -0700	Wed, 02 May 2018 16:59:59 -0700	techsneeze.com	google.com	[redacted]	11
Tue, 01 May 2018 17:00:00 -0700	Wed, 02 May 2018 17:00:00 -0700	techsneeze.com	AMAZON-SES	[redacted]	1
Tue, 01 May 2018 17:00:00 -0700	Wed, 02 May 2018 17:00:00 -0700	techsneeze.com	AMAZON-SES	[redacted]	2
Tue, 01 May 2018 22:00:04 -0700	Wed, 02 May 2018 22:00:05 -0700	techsneeze.com	IPD2IPORT03P-mgmt.target.com	[redacted]	1
Tue, 01 May 2018 22:00:05 -0700	Wed, 02 May 2018 22:00:05 -0700	techsneeze.com	Ipd2iport01.Target.com	[redacted]	1
Wed, 02 May 2018 17:00:00 -0700	Thu, 03 May 2018 16:59:59 -0700	techsneeze.com	FastMail Pty Ltd	[redacted]	1
Wed, 02 May 2018 17:00:00 -0700	Thu, 03 May 2018 16:59:59 -0700	techsneeze.com	google.com	[redacted]	13
Wed, 02 May 2018 17:00:00 -0700	Thu, 03 May 2018 16:59:59 -0700	example.com	Yahoo! Inc.	[redacted]	2
Wed, 02 May 2018 17:00:00 -0700	Thu, 03 May 2018 17:00:00 -0700	techsneeze.com	AMAZON-SES	[redacted]	3
Wed, 02 May 2018 17:00:00 -0700	Thu, 03 May 2018 17:00:00 -0700	techsneeze.com	AMAZON-SES	[redacted]	6
Wed, 02 May 2018 17:00:00 -0700	Thu, 03 May 2018 17:00:00 -0700	techsneeze.com	AMAZON-SES	[redacted]	2
Wed, 02 May 2018 22:00:05 -0700	Thu, 03 May 2018 22:00:06 -0700	techsneeze.com	Ipd2iport01.Target.com	[redacted]	1
Wed, 02 May 2018 22:00:05 -0700	Thu, 03 May 2018 22:00:06 -0700	techsneeze.com	Tezpiport02p.target.com	[redacted]	1
Wed, 02 May 2018 22:00:05 -0700	Thu, 03 May 2018 22:00:07 -0700	techsneeze.com	Tezpiport01p.target.com	[redacted]	1
Wed, 02 May 2018 22:00:06 -0700	Thu, 03 May 2018 22:00:07 -0700	techsneeze.com	Ipd2iport02.target.com	[redacted]	1
Thu, 03 May 2018 17:00:00 -0700	Fri, 04 May 2018 16:59:59 -0700	techsneeze.com	google.com	[redacted]	30
Thu, 03 May 2018 17:00:00 -0700	Fri, 04 May 2018 16:59:59 -0700	example.com	Yahoo! Inc.	[redacted]	1

DMARC

Example DMARC Reports from Tools and Services



DMARC Service Vendors

Try three before you buy to find the best fit for your enterprise, some to try:

- Dmarcian
- Agari
- 250OK
- DmarcAnalyzer
- Dmarcly
- GoDmarc
- Logix
- Uriports
- Valimail

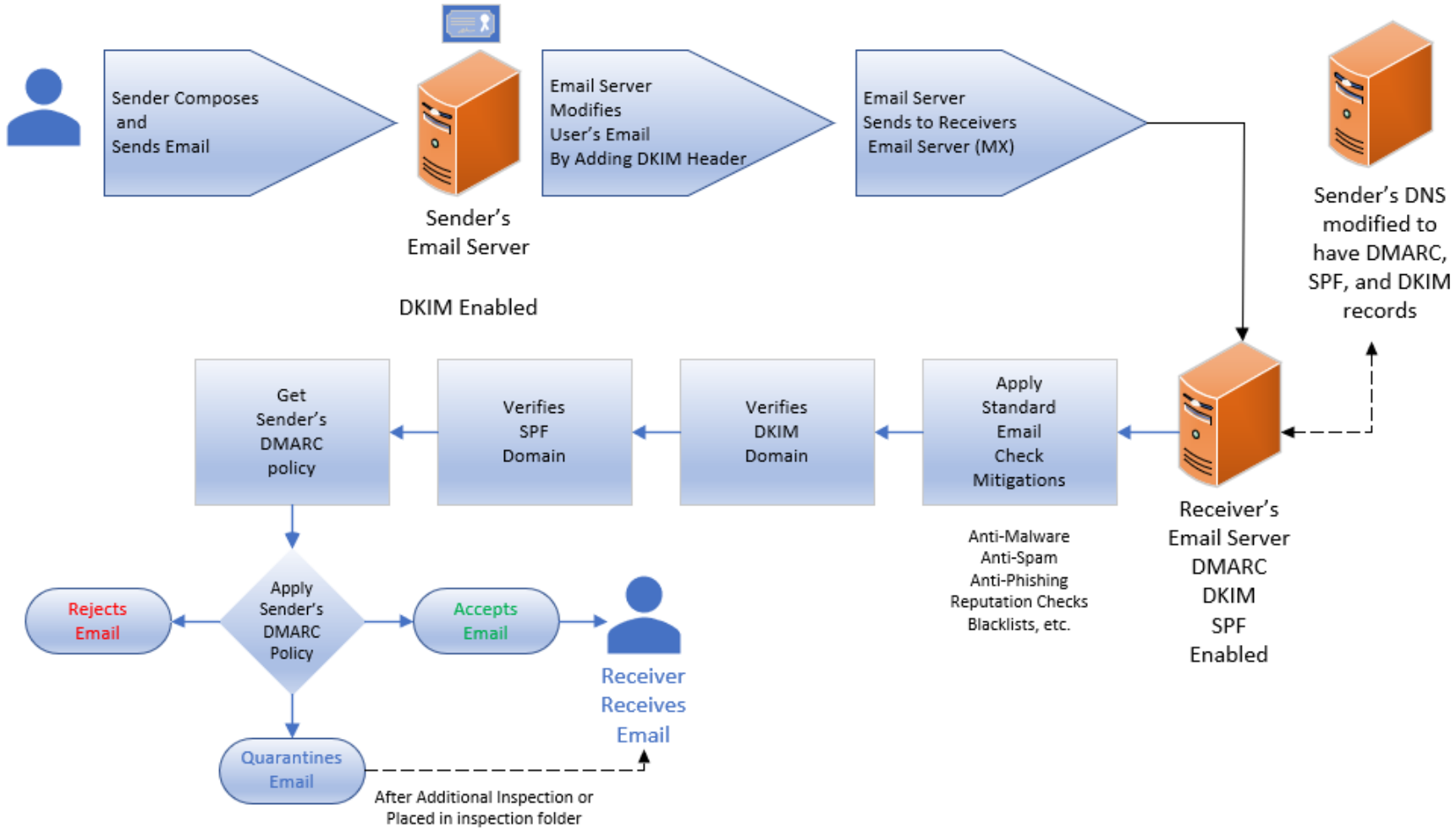
DMARC Reports

DMARC Reports – Caveats

- Some ISPs and big email providers, like Microsoft, do not send reports
- Be aware that if you use email proxies that parse the DMARC RFC, the proxies will get your reports
- DMARC (RUF) Forensics reports can contain PII, and for that reason are not generated that much these days

SPF, DKIM, and DMARC

Putting it all together



DMARC

Other Resources

- https://dmarc.org/overview/
- https://dmarcian.com
- https://en.wikipedia.org/wiki/DMARC
- https://blog.returnpath.com/demystifying-the-dmarc-record/
- https://blog.returnpath.com/build-your-dmarc-record-in-15-minutes-v2/
- http://www.gettingemaildelivered.com/how-to-set-up-dmarc-email-authentication

Agenda

- What is DMARC, SPF, and DKIM?
  - How to Configure
- **Best Practices**
- How Phishes Get By

DMARC

Best Practices

- Set DMARC to None so that will get you reports to see if you've got anything messaged up
- Then set to Quarantine and see how you manage that
- Maybe move to Reject as your infrastructure matures

DMARC

Best Practices

- Set DMARC p=None
- Receiving domains will handle all email saying it's from your domain normally
- But participating ISPs will send you daily reports, including:
  - How many emails they received claiming to be from your domain
  - How many failed DMARC checking
  - How many passed DMARC checking

DMARC

Best Practices

- Set DMARC p=quarantine
- Receiving domains will send failed email to further inspection folder (e.g. spam/junk/quarantine, etc.)

DMARC

Best Practices

- Set DMARC p=reject
- Receiving domains will reject failed email
- Caution enabling this setting

- Check reports periodically to make sure you aren't generating false positives (legitimate email from your domain that is being rejected)

Agenda

- What is DMARC, SPF, and DKIM?
  - How to Configure
- Best Practices
- **How Phishes Get By**

How Phishes Get By

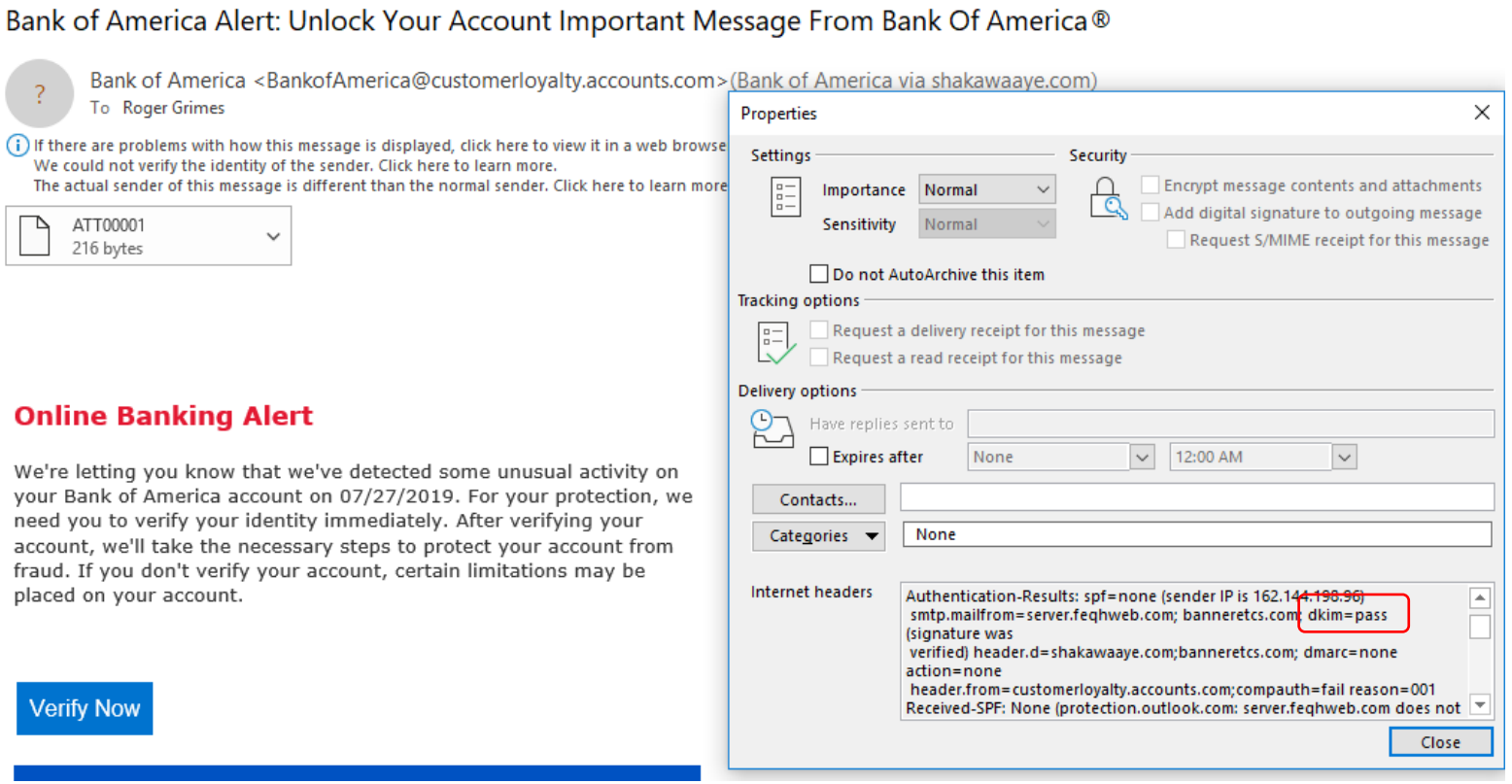
Summary

- Phishers use DMARC
- Misconfiguration
- Quarantine Doesn't Quarantine
- Email Service May Ignore Settings
- It's Domain Verification (not email address verification)
- Phish Can Be Sent by Compromised Computer/Domain
- Sound-alike, Look-a-Like Domains

How Phishes Get By

Phishers Use SPF, DKIM, and DMARC

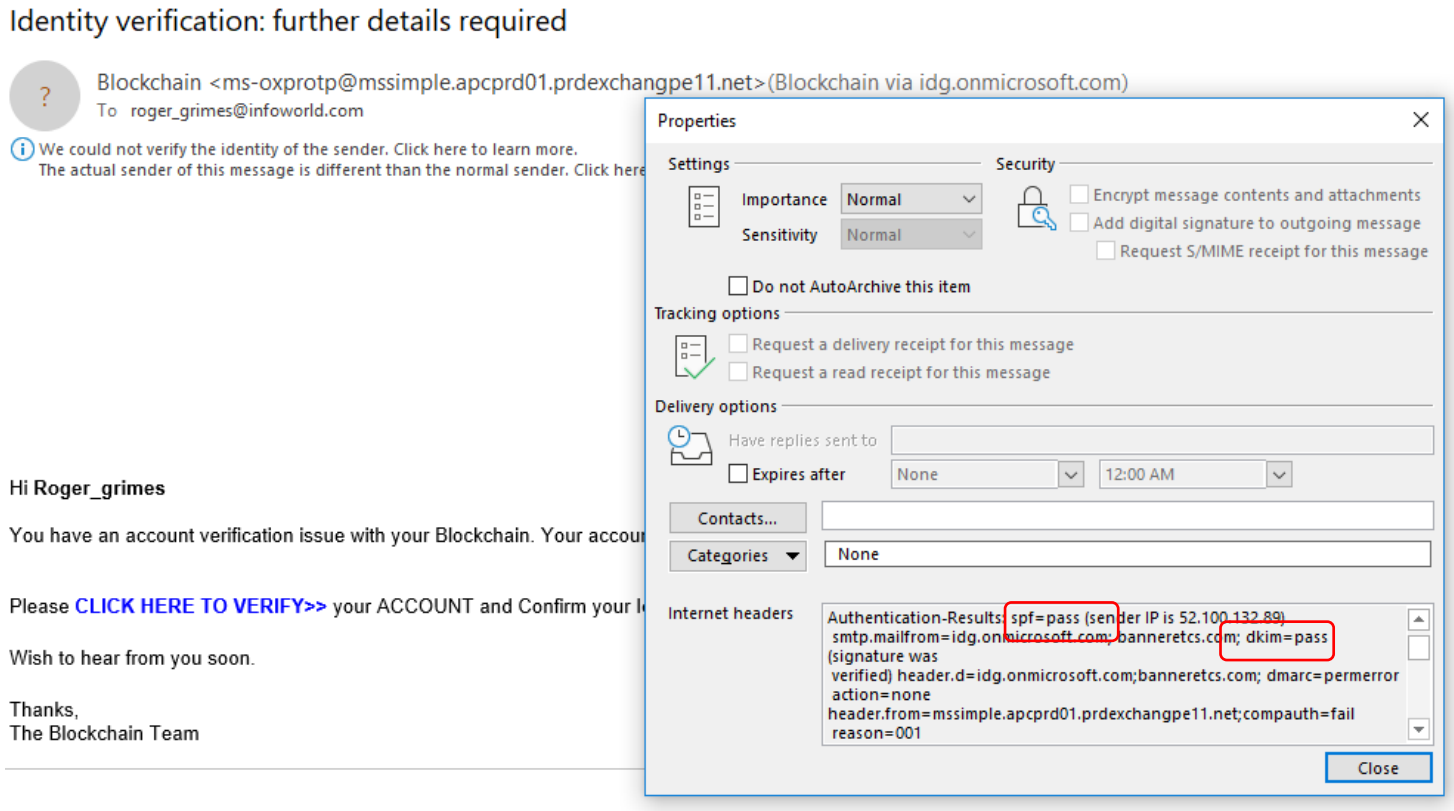
- Examples



How Phishes Get By

Phishers Use SPF, DKIM, and DMARC

- Examples



How Phishes Get By

Misconfiguration

- SPF, DKIM, and DMARC is widely misconfigured
- Missing records
- Old, not updated key pairs
- Bad IP addresses
- Missed domains
- Email proxies invalidate use

How Phishes Get By

Quarantine Doesn’t Quarantine

- DMARC is set to Quarantine, but receiving server doesn’t check or ignores instruction

How Phishes Get By

Email Service May Ignore Settings

- Many public email services don’t participate in DMARC or do, but essentially set DMARC’s p=none

How Phishes Get By

It’s Domain Verification

- It's Domain Verification (not email address verification)
- Email could have fake sender from within valid domain
    - Domain could be gmail.com, Hotmail.com, etc.

How Phishes Get By

Compromised Domain

- Phish Can Be Sent by Compromised Computer/Domain
- 3rd party compromised phishing is on the rise
- Doesn't prevent emails coming from real domain from being sent

How Phishes Get By

Fake Domains

- Sound-alike, Look-a-Like Domains

Who would catch?:

- llnkedin.com, llinkedin.com
- gmail.com.emaildomain.biz

How Phishes Get By

They Will Get By Your Technical Controls

- So why do it at all? Why waste the time and energy?

Because:

- It will block some percentage of rogue emails
- It will let you scrutinize rogue incoming emails a bit more easily
- At the very least you'll know who is sending rogue emails claiming to be from your domains
- It will give you information and more information is never bad

How Phishes Get By

They Will Get By Your Technical Controls

- So you must do security awareness training!

The KnowBe4 Security Awareness Program WORKS

Baseline Testing
Use simulated phishing to baseline assess the Phish-prone™ percentage of your users.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.

See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!

Generating Industry-Leading Results and ROI

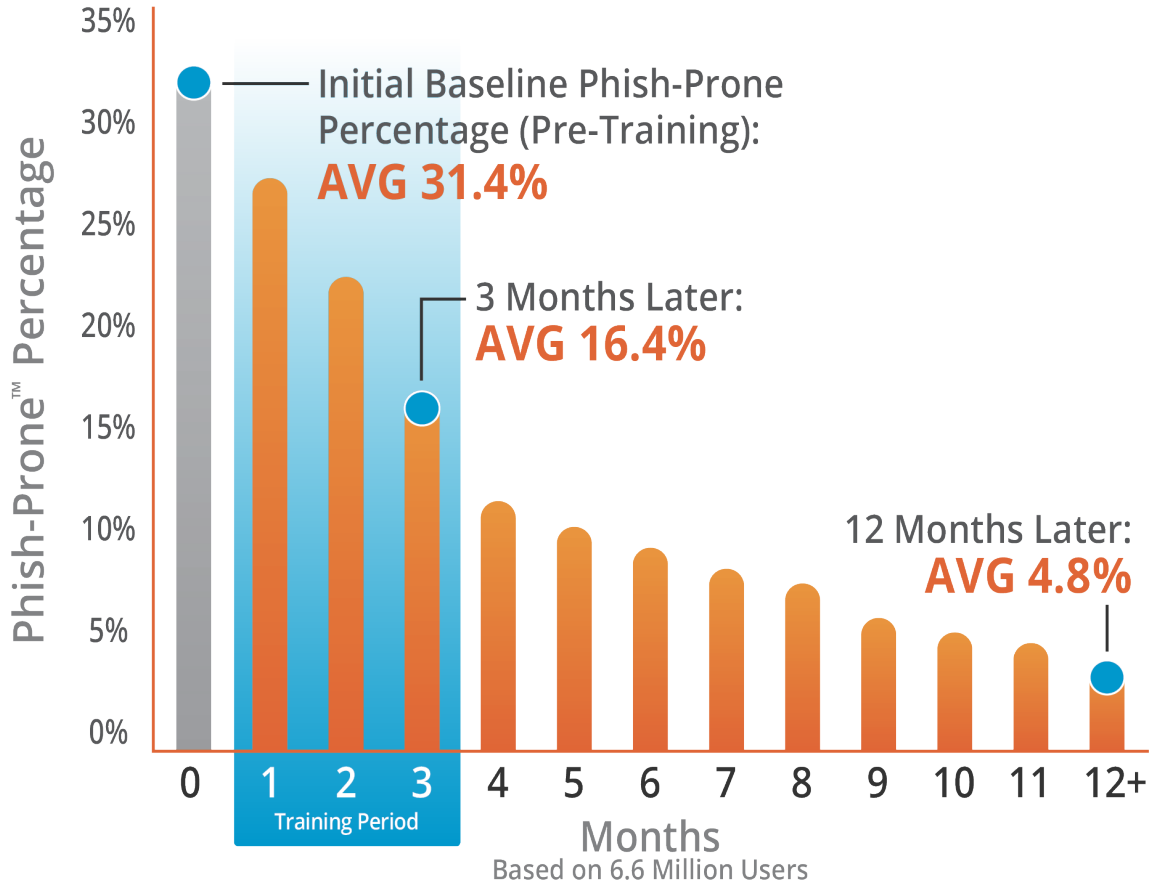
- Reduced Malware and Ransomware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

84% Average Improvement

Across all industries and sizes from baseline testing to one year or more of ongoing training and testing

Note: The initial Phish-Prone percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 platform prior to the evaluation. Subsequent time periods reflect Phish-Prone percentages for the subset of users who received training with the KnowBe4 platform.

The KnowBe4 System Really Works



Source: 2021 KnowBe4 Phishing by Industry Benchmarking Report

Questions?

Roger A. Grimes
Data-Driven Defense Evangelist, KnowBe4

rogerg@knowbe4.com
Twitter: @RogerAGrimes
https://www.linkedin.com/in/rogeragrimes/