KnowBe4
Human error. Conquered.

How to Prevent 81% of Phishing Attacks From Sailing Right Through DMARC, SPF, and DKIM

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

Roger A. Grimes

Data-Driven Defense Evangelist
KnowBe4, Inc.

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

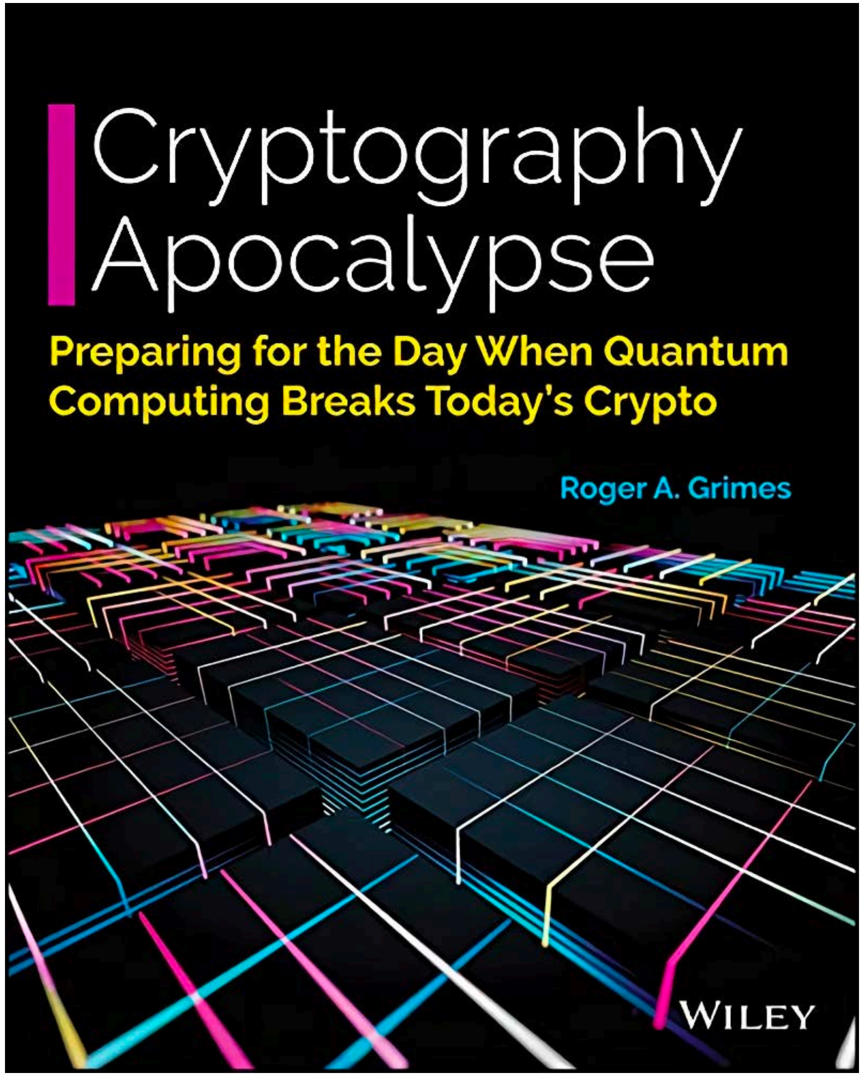
About Roger

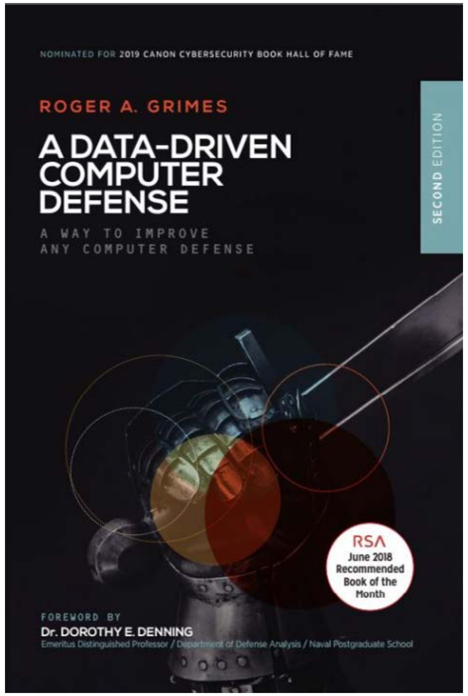
- 30 years plus in computer security
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 11 books and over 1,000 magazine articles
- *InfoWorld* and *CSO* weekly security columnist since 2005
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

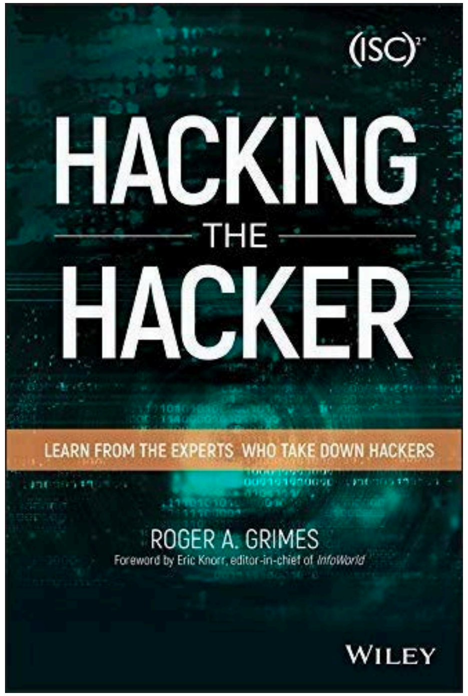
Certification exams passed include:

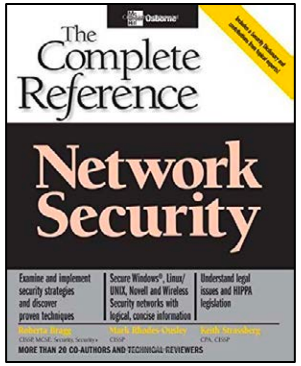
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

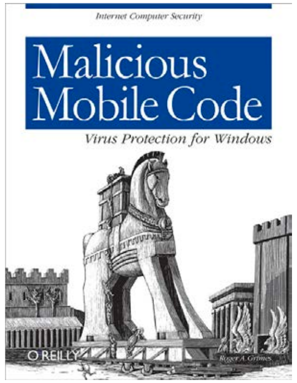
Roger's Books

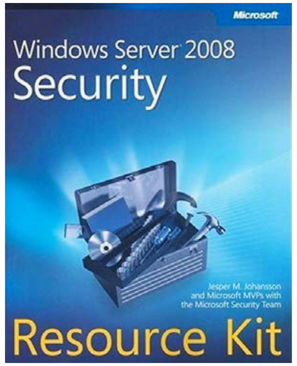

Cryptography Apocalypse
Preparing for the Day When Quantum Computing Breaks Today's Crypto
Roger A. Grimes
WILEY

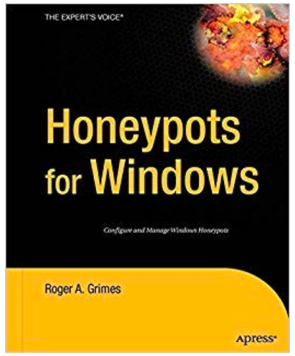

NOMINATED FOR 2019 CANON CYBERSECURITY BOOK HALL OF FAME
ROGER A. GRIMES
A DATA-DRIVEN COMPUTER DEFENSE
A WAY TO IMPROVE ANY COMPUTER DEFENSE
SECOND EDITION
RSA June 2018 Recommended Book of the Month
FOREWORD BY Dr. DOROTHY E. DENNING
Emeritus Distinguished Professor / Department of Defense Analysis / Naval Postgraduate School

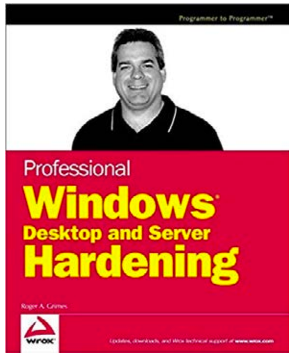

(ISC)²
HACKING THE HACKER
LEARN FROM THE EXPERTS WHO TAKE DOWN HACKERS
ROGER A. GRIMES
Foreword by Eric Knorr, editor-in-chief of InfoWorld
WILEY

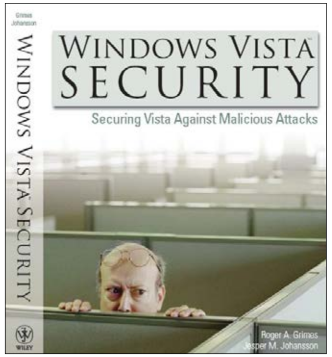


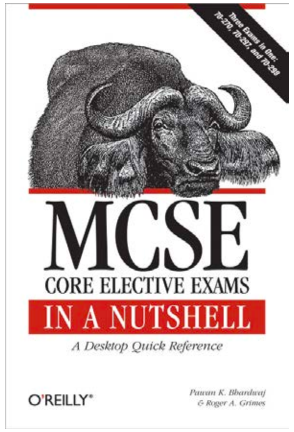


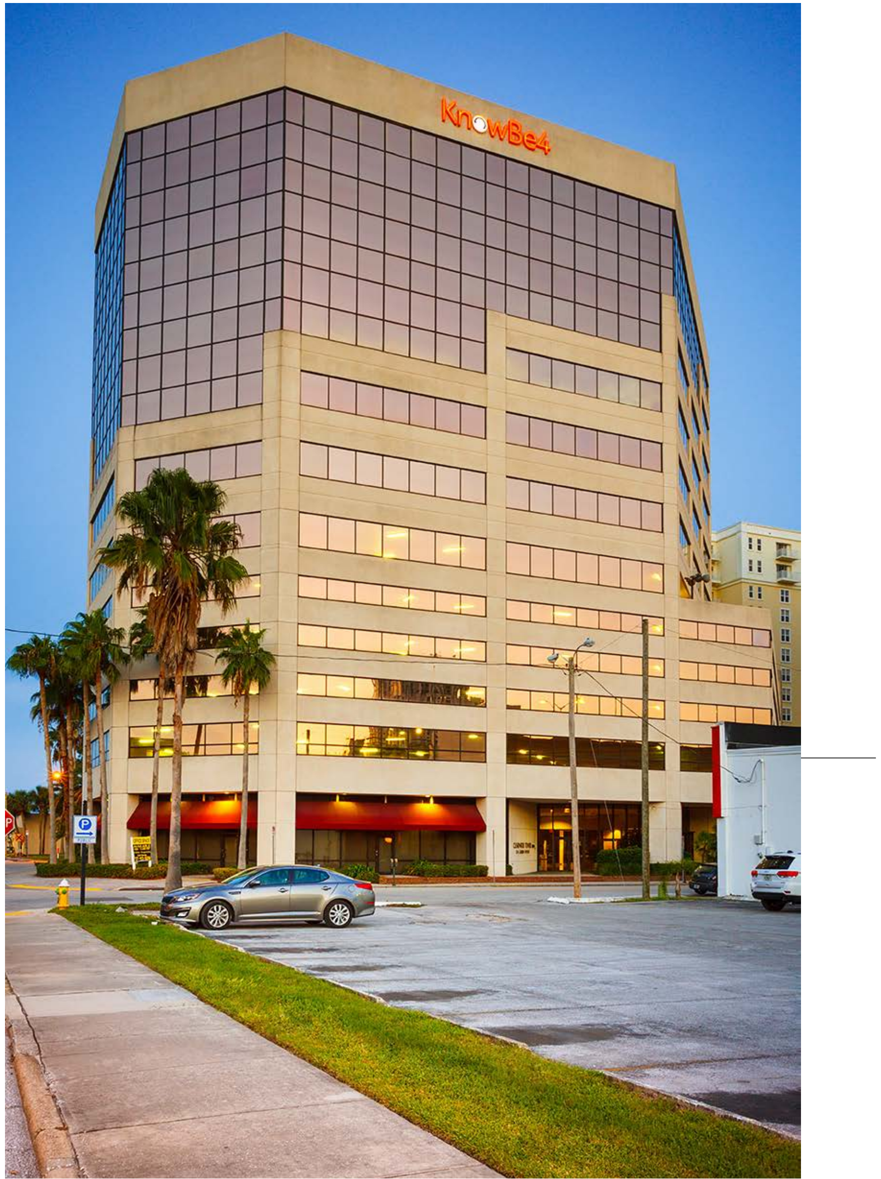

Microsoft
Windows Server 2008 Security
Resource Kit
Jesper M. Johansson and Microsoft MVPs with the Microsoft Security Team





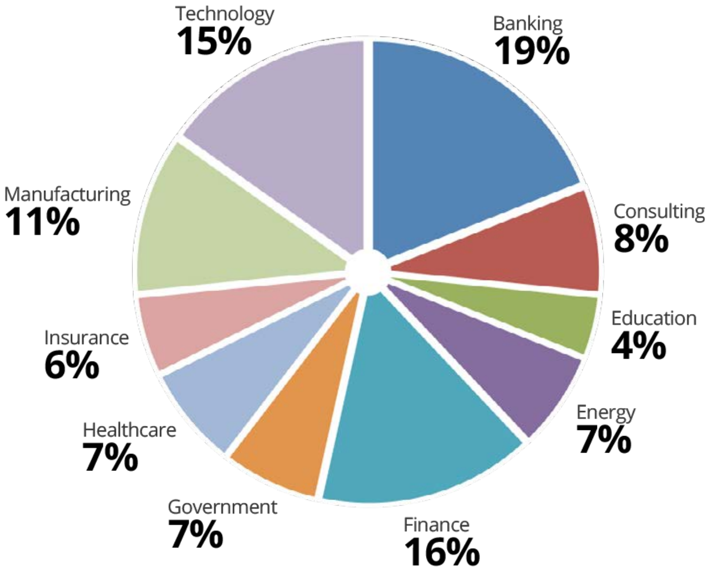



MCSE
CORE ELECTIVE EXAMS IN A NUTSHELL
A Desktop Quick Reference
O'REILLY
Pawan K. Bhardwaj & Roger A. Grimes



KnowBe4, Inc.

- The world’s most popular integrated Security Awareness Training and Simulated Phishing platform
- Based in Tampa Bay, Florida, founded in 2010
- CEO & employees are ex-antivirus, IT Security pros
- 200% growth year over year
- We help tens of thousands of organizations manage the problem of social engineering



Today's Presentation

- What is DMARC, SPF, and DKIM?
- How to Configure
- Common Mistakes
- Best Practices
- How Phishes 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 DKIM
- Important point: 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
- Once DNS setup is done, it is usually checked for and enabled by most (but not all) email servers
- Sending domain must setup
- Receiving domain checks and verifies

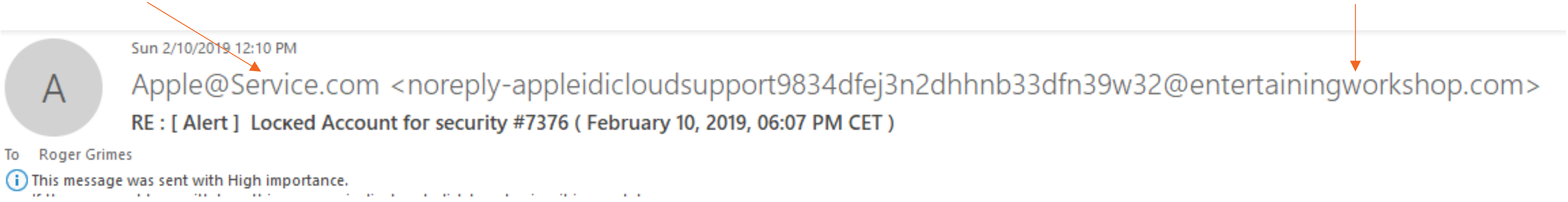
SPF & DKIM

Global Phishing Protection 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
- **Domain Keys Identified Mail (DKIM)**
  - Verifies the 5322 **Display From** domain address
    - This is the email address you always see

DKIM
5322 domain

SPF
5321 domain



Sun 2/10/2019 12:10 PM

Apple@Service.com <noreply-appleidicloudsupport9834dfej3n2dhhnb33dfn39w32@entertainingworkshop.com>

RE : [Alert] Locked Account for security #7376 (February 10, 2019, 06:07 PM CET)

To Roger Grimes

This message was sent with High importance.

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 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 To field
- Relies on SPF/TXT records in DNS
  - example.com. IN TXT "v=spf1 -all"
  - example.com. IN TXT “v=spf1 ip4:192.168.1.1 ~all”
- Sender must have it enabled
- Receiver checks and verifies

SPF

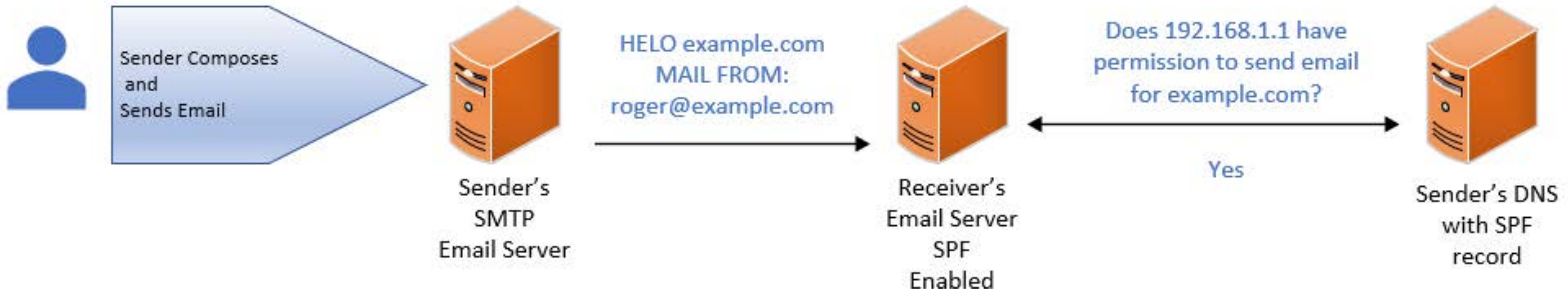
Sender Policy Framework (SPF)

- RFC 4408
  - http://www.zytrax.com/books/dns/apd/rfc4408.txt
- When enabled, receiving email server checks the domain’s IP address in the HELO handshake against the sender’s SPF DNS record
- If it fails, recipient’s server will 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



SPF

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 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 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)

<u>Setting Up – Sender Side</u>

Modify your DNS by creating a new TXT record for SPF

<u>Format of SPF txt record</u>

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

<u>Examples</u>

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 include:example.com –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

Sender Policy Framework (SPF)

Setting Up – Sender Side

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

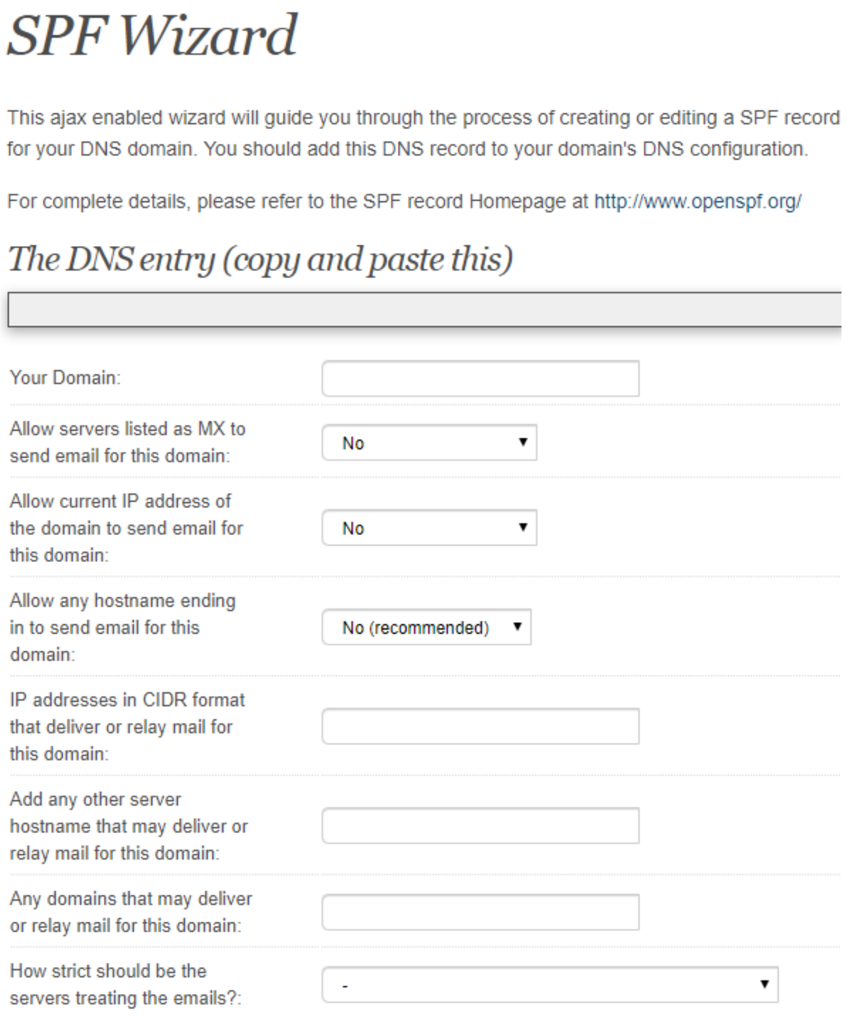
v=spf1 include:_spf.google.com ~all

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

SPF

Sender Policy Framework (SPF)

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



SPF Wizard

This ajax enabled wizard will guide you through the process of creating or editing a SPF record for your DNS domain. You should add this DNS record to your domain's DNS configuration.

For complete details, please refer to the SPF record Homepage at http://www.openspf.org/

The DNS entry (copy and paste this)

Your Domain:

Allow servers listed as MX to send email for this domain: No

Allow current IP address of the domain to send email for this domain: No

Allow any hostname ending in to send email for this domain: No (recommended)

IP addresses in CIDR format that deliver or relay mail for this domain:

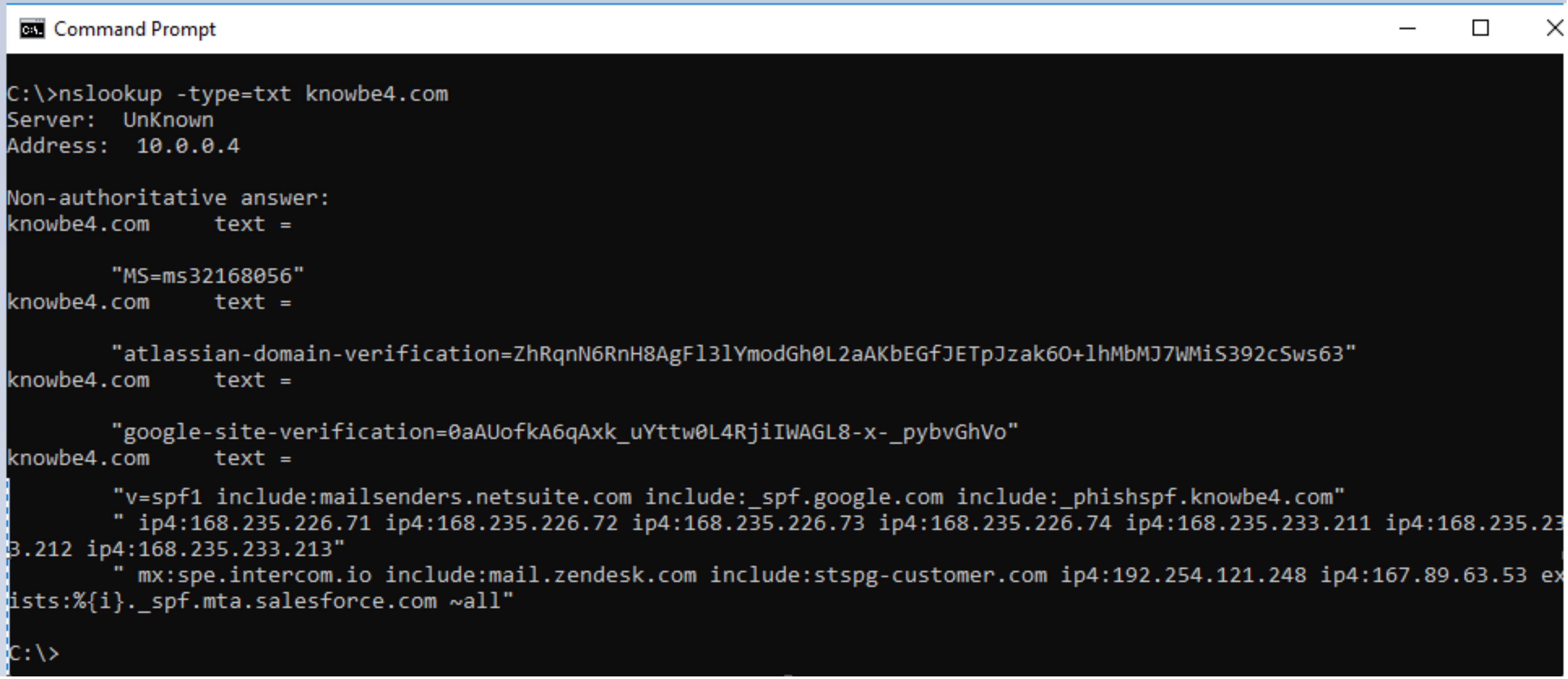
Add any other server hostname that may deliver or relay mail for this domain:

Any domains that may deliver or relay mail for this domain:

How strict should be the servers treating the emails?: -

SPF

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

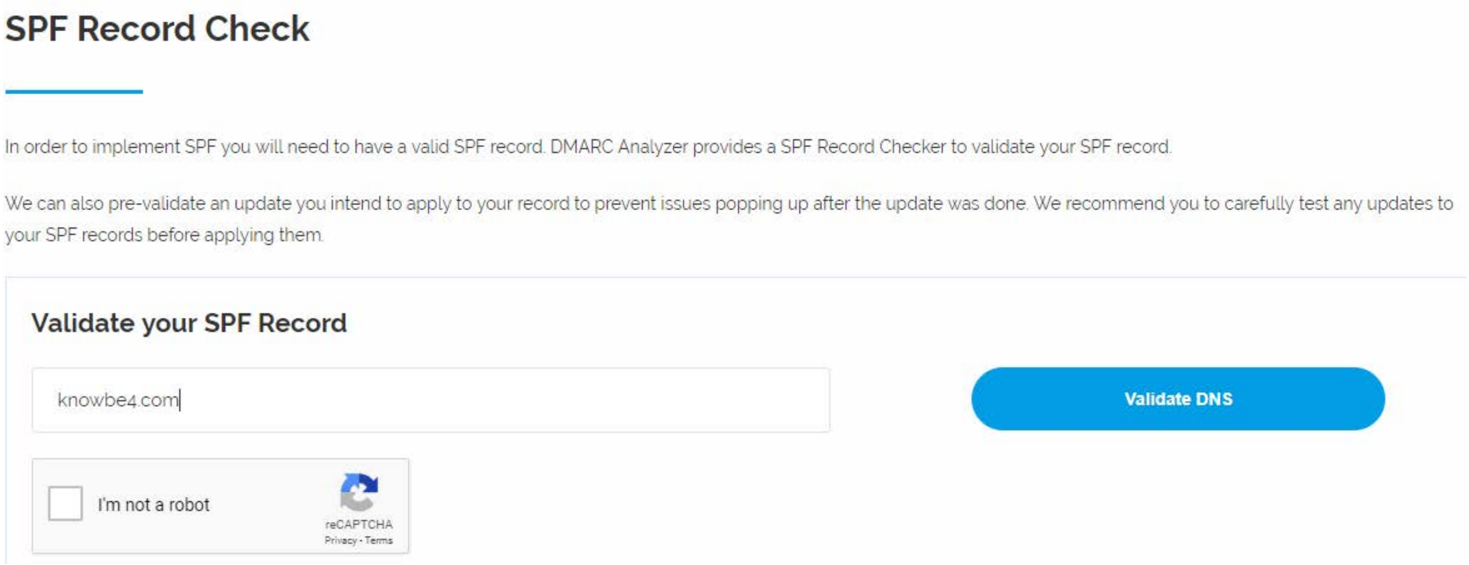


```
C:\>nslookup -type=txt knowbe4.com
Server:  UnKnown
Address:  10.0.0.4

Non-authoritative answer:
knowbe4.com     text =

        "MS=ms32168056"
knowbe4.com     text =

        "atlassian-domain-verification=ZhRqnN6RnH8AgFl3lYmodGh0L2aAKbEGfJETpJzak6O+lhMbMJ7WMiS392cSws63"
knowbe4.com     text =

        "google-site-verification=0aAUofkA6qAxk_uYttw0L4RjiIWAGL8-x-_pybvGhVo"
knowbe4.com     text =

        "v=spf1 include:mailsenders.netsuite.com include:_spf.google.com include:_phishspf.knowbe4.com"
        " ip4:168.235.226.71 ip4:168.235.226.72 ip4:168.235.226.73 ip4:168.235.226.74 ip4:168.235.233.211 ip4:168.235.23
3.212 ip4:168.235.233.213"
        " mx:spe.intercom.io include:mail.zendesk.com include:stspg-customer.com ip4:192.254.121.248 ip4:167.89.63.53 ex
ists:%{i}._spf.mta.salesforce.com ~all"

C:\>
```

SPF

Sender Policy Framework (SPF)

- Lots of DMARC/SPF verification sites, including https://www.kitterman.com/spf/validate.html, https://mxtoolbox.com/spf.aspx, https://www.dmarcanalyzer.com/spf/checker/



SPF Record Check

In order to implement SPF you will need to have a valid SPF record. DMARC Analyzer provides a SPF Record Checker to validate your SPF record.

We can also pre-validate an update you intend to apply to your record to prevent issues popping up after the update was done. We recommend you to carefully test any updates to your SPF records before applying them.

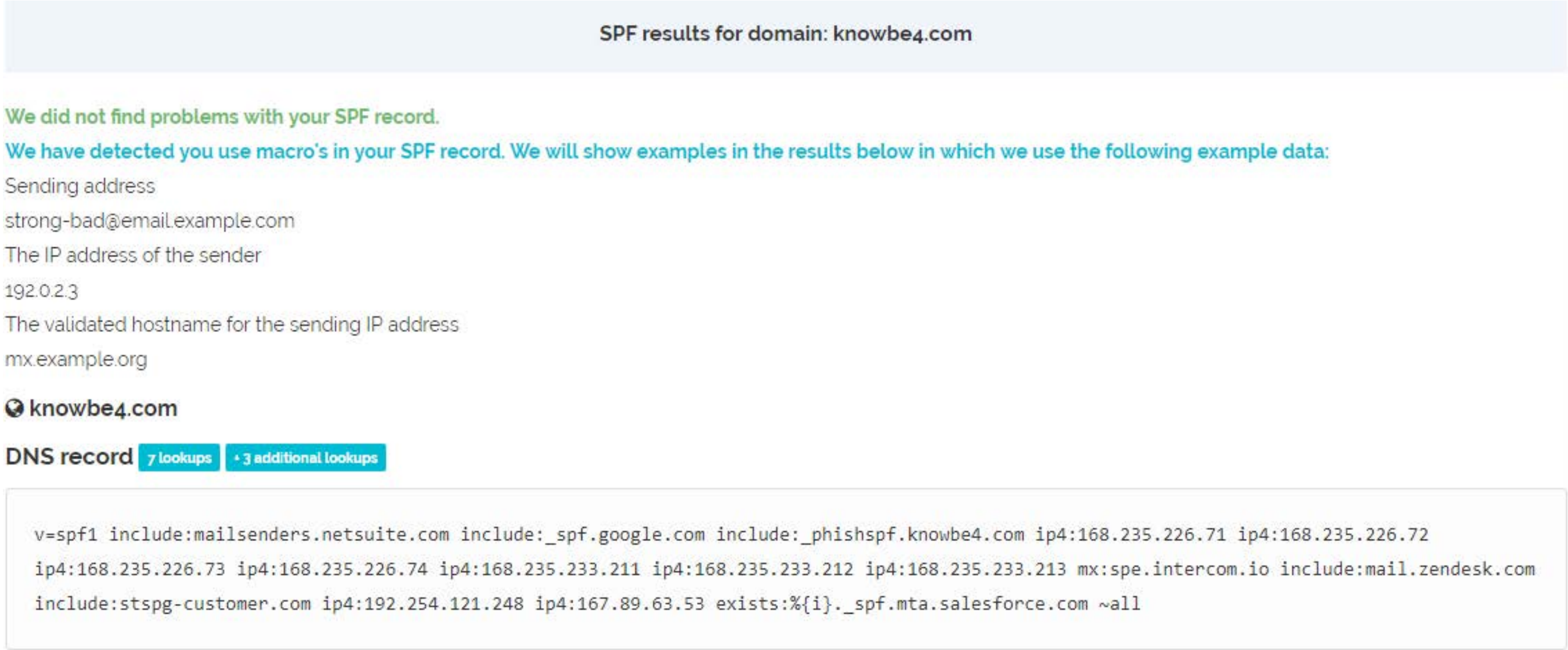
Validate your SPF Record

knowbe4.com

SPF

Sender Policy Framework (SPF)

- Lots of DMARC/SPF verification sites, including
- https://www.dmarcanalyzer.com/spf/checker/ results



SPF results for domain: knowbe4.com

We did not find problems with your SPF record.

We have detected you use macro's in your SPF record. We will show examples in the results below in which we use the following example data:

Sending address

strong-bad@email.example.com

The IP address of the sender

192.0.2.3

The validated hostname for the sending IP address

mx.example.org

knowbe4.com

DNS record 7 lookups + 3 additional lookups

```
v=spf1 include:mailsenders.netsuite.com include:_spf.google.com include:_phishspf.knowbe4.com ip4:168.235.226.71 ip4:168.235.226.72
ip4:168.235.226.73 ip4:168.235.226.74 ip4:168.235.233.211 ip4:168.235.233.212 ip4:168.235.233.213 mx:spe.intercom.io include:mail.zendesk.com
include:stspg-customer.com ip4:192.254.121.248 ip4:167.89.63.53 exists:%{i}._spf.mta.salesforce.com ~all
```

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.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:

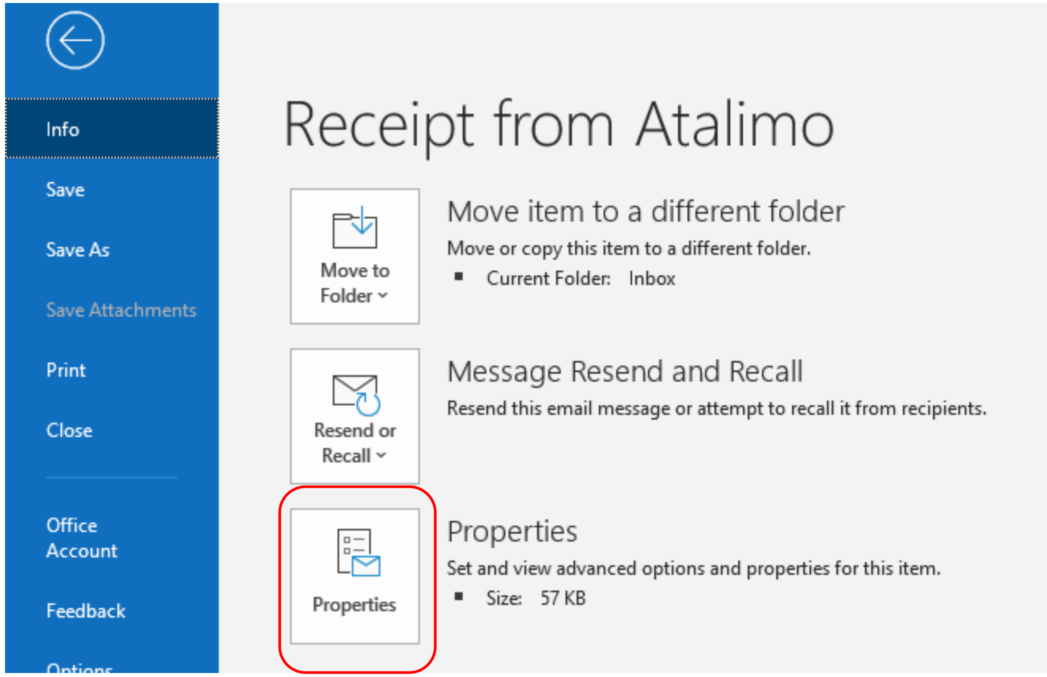
- Should automatically be enabled

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 $true** (SenderID not the same as SPF, but essentially the same)
- **Set-SenderIDConfig -SpoofedDomainAction Reject**

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**



Receipt from Atalimo

Move item to a different folder

Move or copy this item to a different folder.

- Current Folder: Inbox

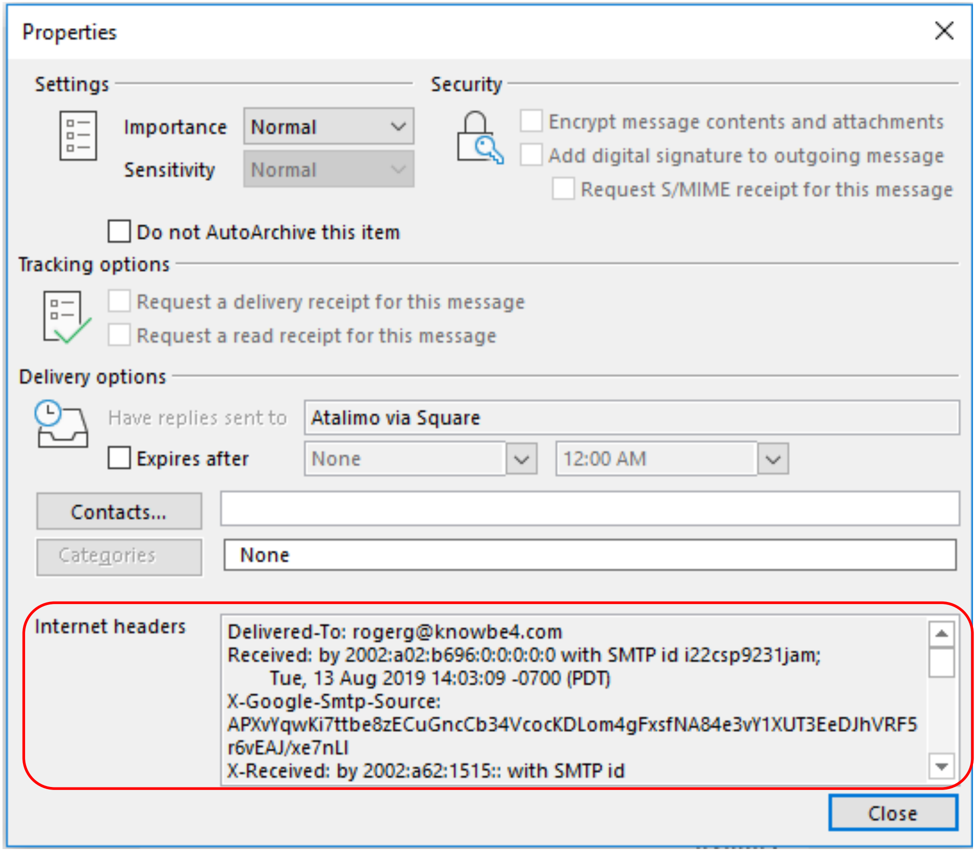
Message Resend and Recall

Resend this email message or attempt to recall it from recipients.

Properties

Set and view advanced options and properties for this item.

- Size: 57 KB



Importance: Normal

Sensitivity: Normal

□ Encrypt message contents and attachments

□ Add digital signature to outgoing message

□ Request S/MIME receipt for this message

□ Do not AutoArchive this item

□ Request a delivery receipt for this message

□ Request a read receipt for this message

Have replies sent to: Atalimo via Square

□ Expires after: None 12:00 AM

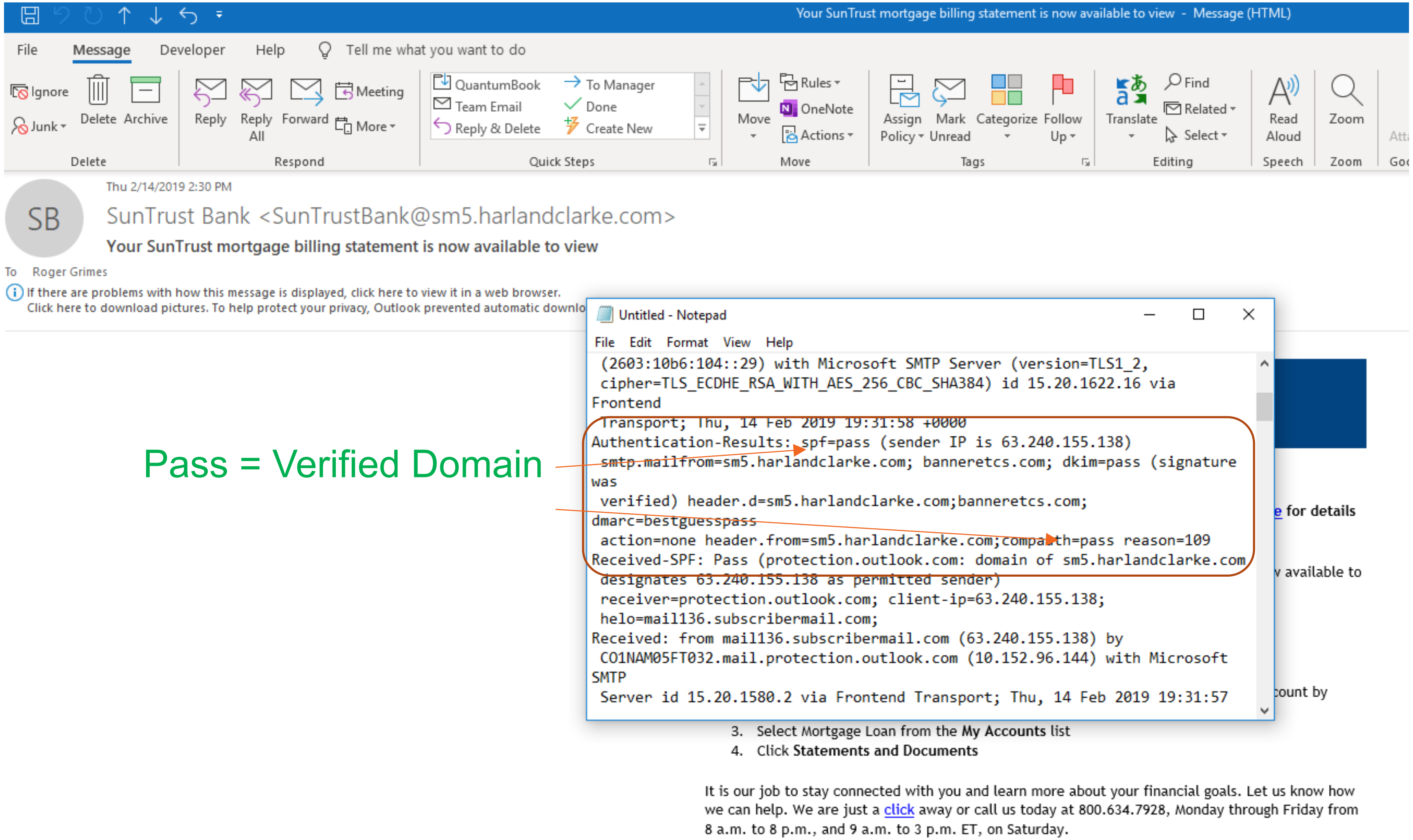
Categories: None

Internet headers

```
Delivered-To: rogerg@knowbe4.com
Received: by 2002:a02:b696:0:0:0:0:0 with SMTP id i22csp9231jam;
      Tue, 13 Aug 2019 14:03:09 -0700 (PDT)
X-Google-Smtp-Source:
APXvYqwKi7ttbe8zECuGncCb34VcocKDLom4gFxsfNA84e3vY1XUT3EeDJhVRF5
r6vEAJ/xe7nLI
X-Received: by 2002:a62:1515:: with SMTP id
```

KnowBe4
Human error. Conquered.

SPF Passes



Thu 2/14/2019 2:30 PM

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

```
 (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

e for details

v available to

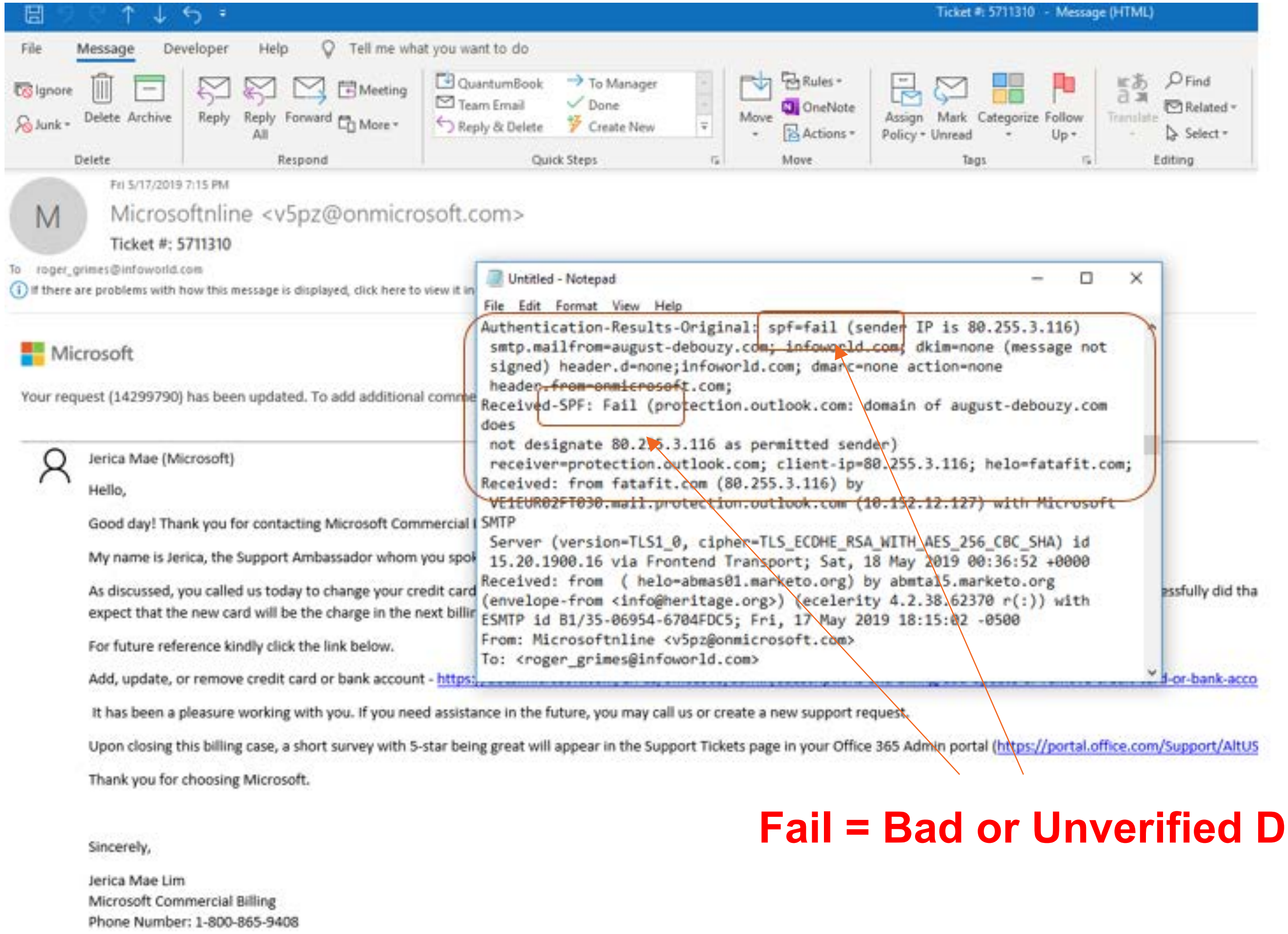
count by

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.

KnowBe4
Human error. Conquered.

SPF Fails



Fri 5/17/2019 7:15 PM

Microsoftnline <v5pz@onmicrosoft.com>

Ticket #: 5711310

To roger_grimes@infoworld.com

If there are problems with how this message is displayed, click here to view it in

Microsoft

Your request (14299790) has been updated. To add additional comme

Jerica Mae (Microsoft)

Hello,

Good day! Thank you for contacting Microsoft Commercial I

My name is Jerica, the Support Ambassador whom you spok

As discussed, you called us today to change your credit card ssfully did tha
expect that the new card will be the charge in the next billir

For future reference kindly click the link below.

Add, update, or remove credit card or bank account - https: d-or-bank-acco

It has been a pleasure working with you. If you need assistance in the future, you may call us or create a new support request.

Upon closing this billing case, a short survey with 5-star being great will appear in the Support Tickets page in your Office 365 Admin portal (https://portal.office.com/Support/AltUS

Thank you for choosing Microsoft.

Sincerely,

Jerica Mae Lim
Microsoft Commercial Billing
Phone Number: 1-800-865-9408

```
Authentication-Results-Original: spf=fail (sender IP is 80.255.3.116)
 smtp.mailfrom=august-debouzy.com; infoworld.com; dkim=none (message not
 signed) header.d=none;infoworld.com; dmarc=none action=none
 header.from=onmicrosoft.com;
Received-SPF: Fail (protection.outlook.com: domain of august-debouzy.com
does
 not designate 80.255.3.116 as permitted sender)
 receiver=protection.outlook.com; client-ip=80.255.3.116; helo=fatafit.com;
Received: from fatafit.com (80.255.3.116) by
 VE1EUR02FT030.mail.protection.outlook.com (10.152.12.127) with Microsoft
SMTP
 Server (version=TLS1_0, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA) id
 15.20.1900.16 via Frontend Transport; Sat, 18 May 2019 00:36:52 +0000
Received: from  ( helo=abmas01.marketo.org) by abmta15.marketo.org
(envelope-from <info@heritage.org>) (ecelerity 4.2.38.62370 r(:)) with
ESMTP id B1/35-06954-6704FDC5; Fri, 17 May 2019 18:15:02 -0500
From: Microsoftnline <v5pz@onmicrosoft.com>
To: <roger_grimes@infoworld.com>
```

Fail = Bad or Unverified Domain

DKIM

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 in 5322 Display Name field
- RFC 5585 (http://www.dkim.org/specs/rfc5585.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

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

<u>Example:</u>

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

DKIM

Setting up – Sender 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. Create **CNAME** DNS records (you'll need at least two per domain)

Host name: selector1._domainkey

Points to address or value: selector1-<domainGUID>._domainkey.<initialDomain>

TTL: 3600

Host name: selector2._domainkey

Points to address or value: selector2-<domainGUID>._domainkey.<initialDomain>

TTL: 3600

DKIM

Setting up – 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. Create 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 – 0365/Microsoft Exchange Online

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

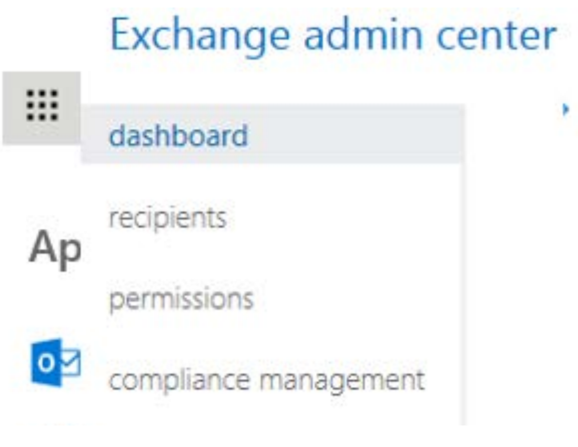
3. Sign into Office 365 with your work or school account
4. Select the app launcher icon in the upper-left and choose Admin
5. In Microsoft 365 admin center, click on Expand or Show all
6. Click on Exchange icon
7. Takes you to Exchange admin center
8. Choose **protection**
9. Choose **dkim**
10. Choose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

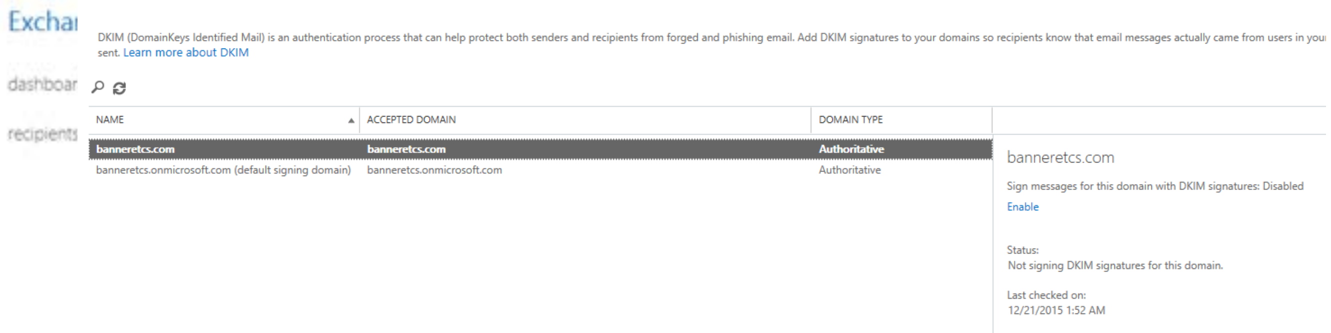
DKIM

Setting up – 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 (DomainKeys Identified Mail) is an authentication process that can help protect both senders and recipients from forged and phishing email. Add DKIM signatures to your domains so recipients know that email messages actually came from users in you sent. Learn more about DKIM

NAME	ACCEPTED DOMAIN	DOMAIN TYPE
banneretcs.com	**banneretcs.com**	**Authoritative**
banneretcs.onmicrosoft.com (default signing domain)	banneretcs.onmicrosoft.com	Authoritative

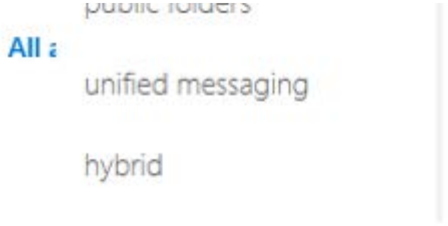
banneretcs.com

Sign messages for this domain with DKIM signatures: Disabled

Enable

Status:
Not signing DKIM signatures for this domain.

Last checked on:
12/21/2015 1:52 AM



DKIM

Domain Keys Identified Mail (DKIM)

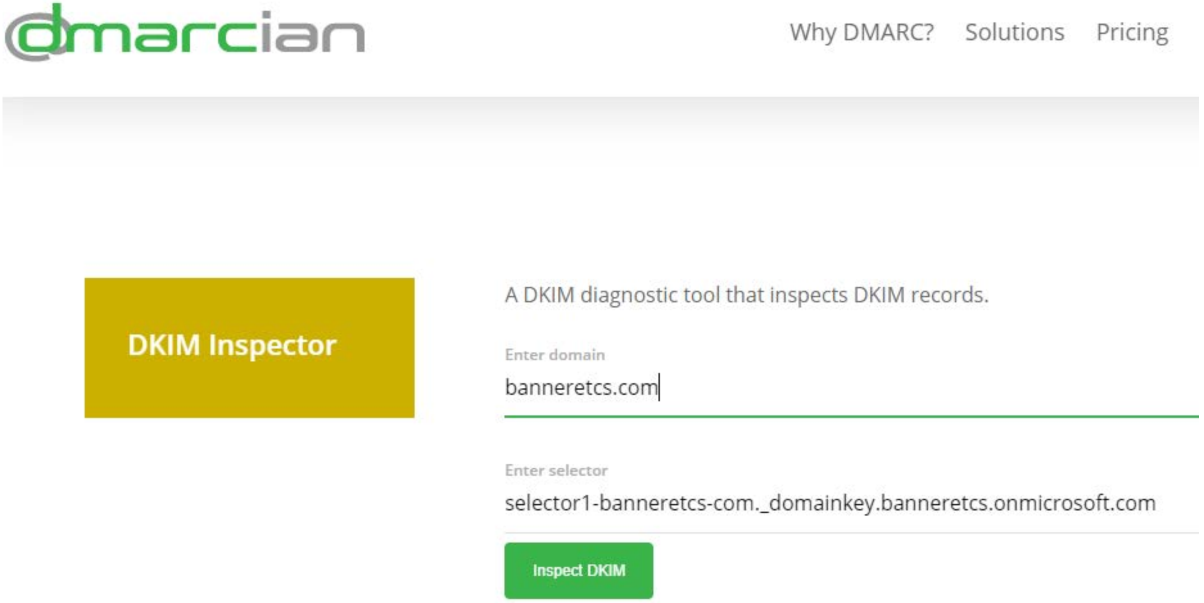
Setting up – On-Premise Microsoft Exchange

- 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

DKIM

Domain Keys Identified Mail (DKIM)

Verify DKIM is Setup Correctly – Lots of verification sites



A DKIM diagnostic tool that inspects DKIM records.

Enter domain
banneretcs.com

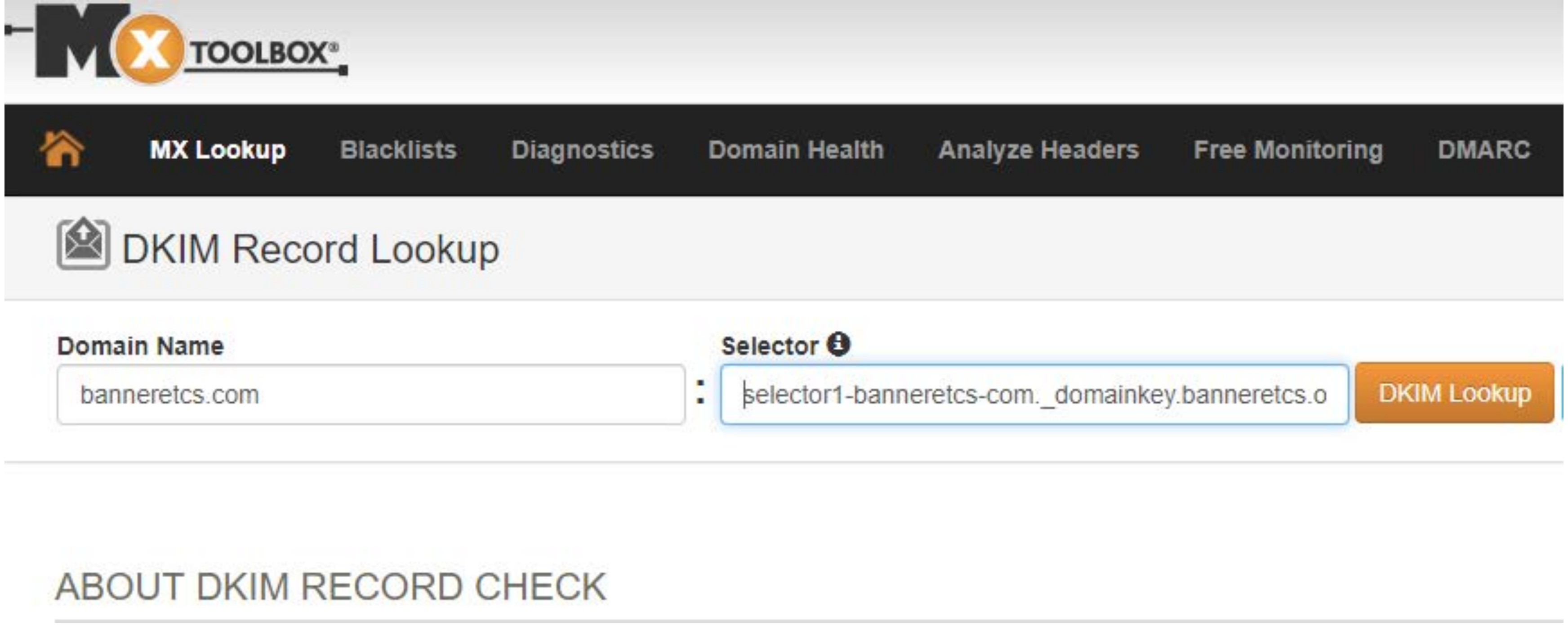
Enter selector
selector1-banneretcs-com._domainkey.banneretcs.onmicrosoft.com

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

DKIM

Domain Keys Identified Mail (DKIM)

Verify DKIM is Setup Correctly – Lots of verification sites



DKIM Record Lookup

Domain Name: banneretcs.com

Selector: selector1-banneretcs-com._domainkey.banneretcs.o

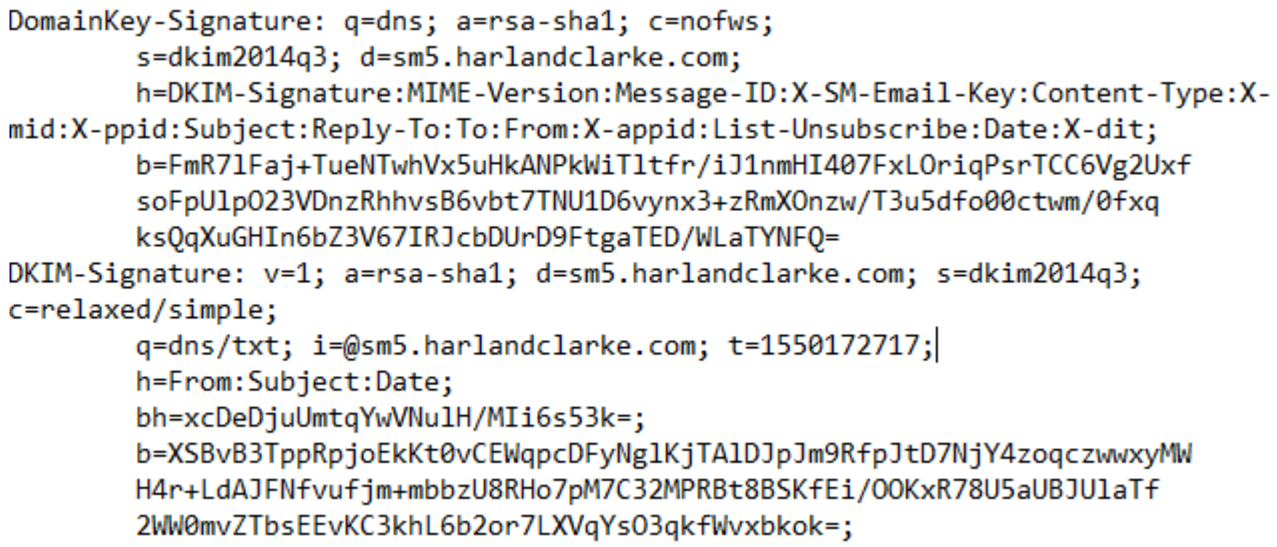
ABOUT DKIM RECORD CHECK

https://mxtoolbox.com/dkim.aspx

DKIM

Domain Keys Identified Mail (DKIM)

Example DKIM Signature in Email Header

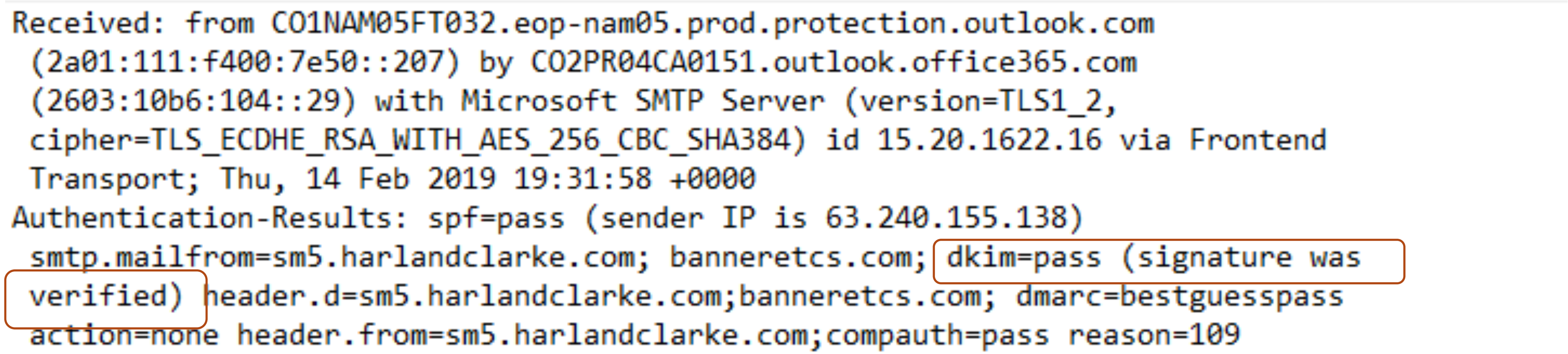


```
DomainKey-Signature: q=dns; a=rsa-sha1; c=nofws;
        s=dkim2014q3; d=sm5.harlandclarke.com;
        h=DKIM-Signature:MIME-Version:Message-ID:X-SM-Email-Key:Content-Type:X-
mid:X-ppid:Subject:Reply-To:To:From:X-appid:List-Unsubscribe:Date:X-dit;
        b=FmR71Faj+TueNTwhVx5uHkANPkWiTltfr/iJ1nmHI407FxLOriqPsrTCC6Vg2Uxf
        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

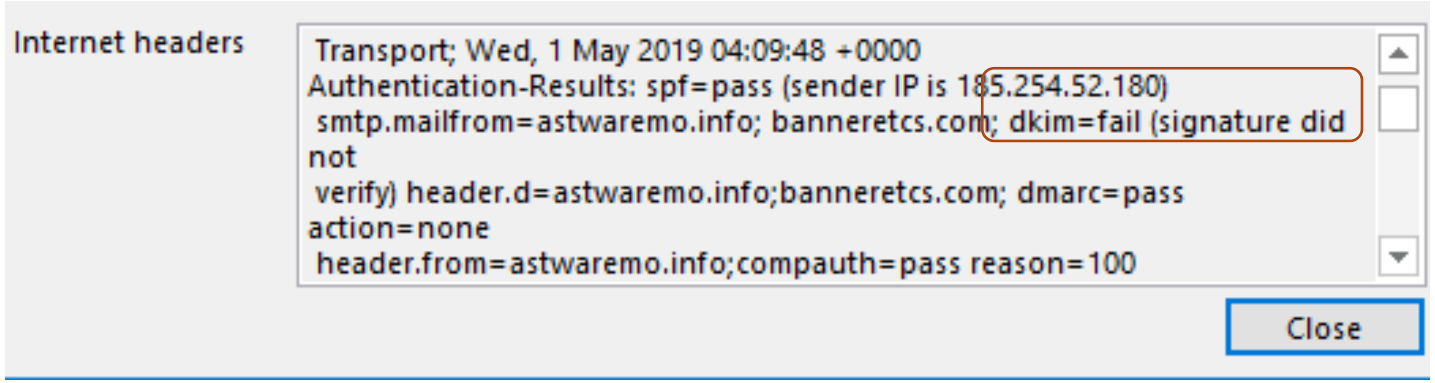


```
Received: from CO1NAM05FT032.eop-nam05.prod.protection.outlook.com
 (2a01:111:f400:7e50::207) by CO2PR04CA0151.outlook.office365.com
 (2603:10b6:104::29) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id 15.20.1622.16 via Frontend
 Transport; Thu, 14 Feb 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



```
 Transport; Wed, 1 May 2019 04:09:48 +0000
Authentication-Results: spf=pass (sender IP is 185.254.52.180)
 smtp.mailfrom=astwaremo.info; banneretcs.com; dkim=fail (signature did
not
 verify) header.d=astwaremo.info;banneretcs.com; dmarc=pass
action=none
 header.from=astwaremo.info;compauth=pass reason=100
```

DMARC

DMARC

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;"

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 – 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.
- 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.
- fo: Dictates what type of authentication and/or alignment vulnerabilities are reported back

There are four values to the latter fo: tag:

- 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

DMARC

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

Other Resources

- https://dmarc.org/overview/
- 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

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

DMARC Reports

DMARC Aggregate Reports

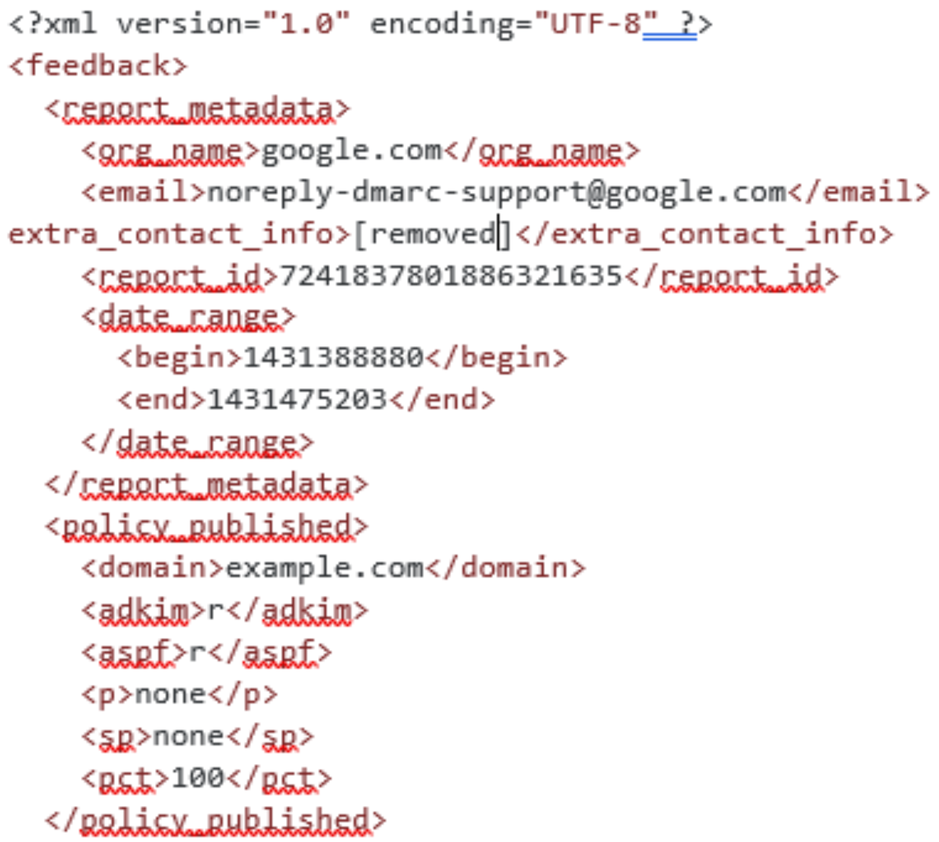
- Sent daily about daily cumulative results relating to your DMARC’d domains from participating DMARC receivers who get emails claiming to be from your domains

Includes:

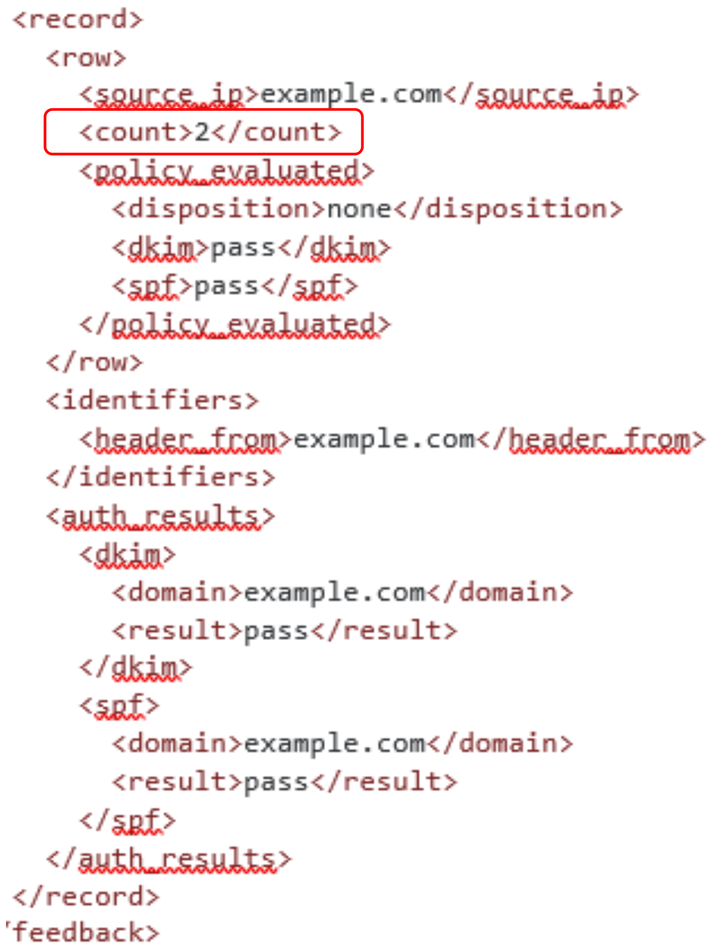
- How many emails they received claiming to be from your domain
- How many failed DMARC checking
- How many passed DMARC checking

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 Forensic Reports

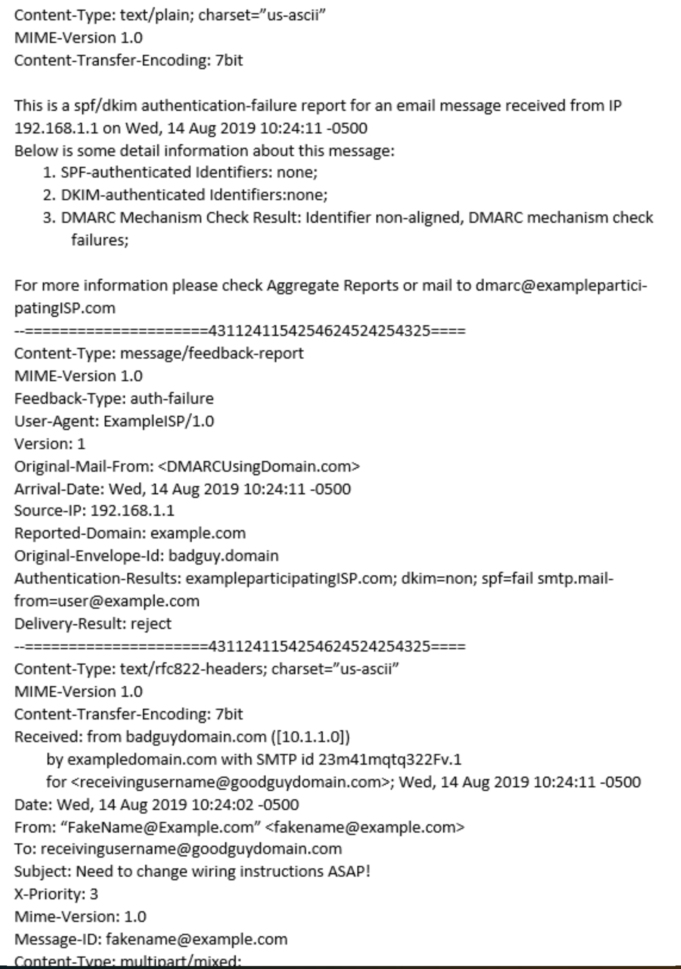
- Diagnostic info sent for each failed email, text-based in an email

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

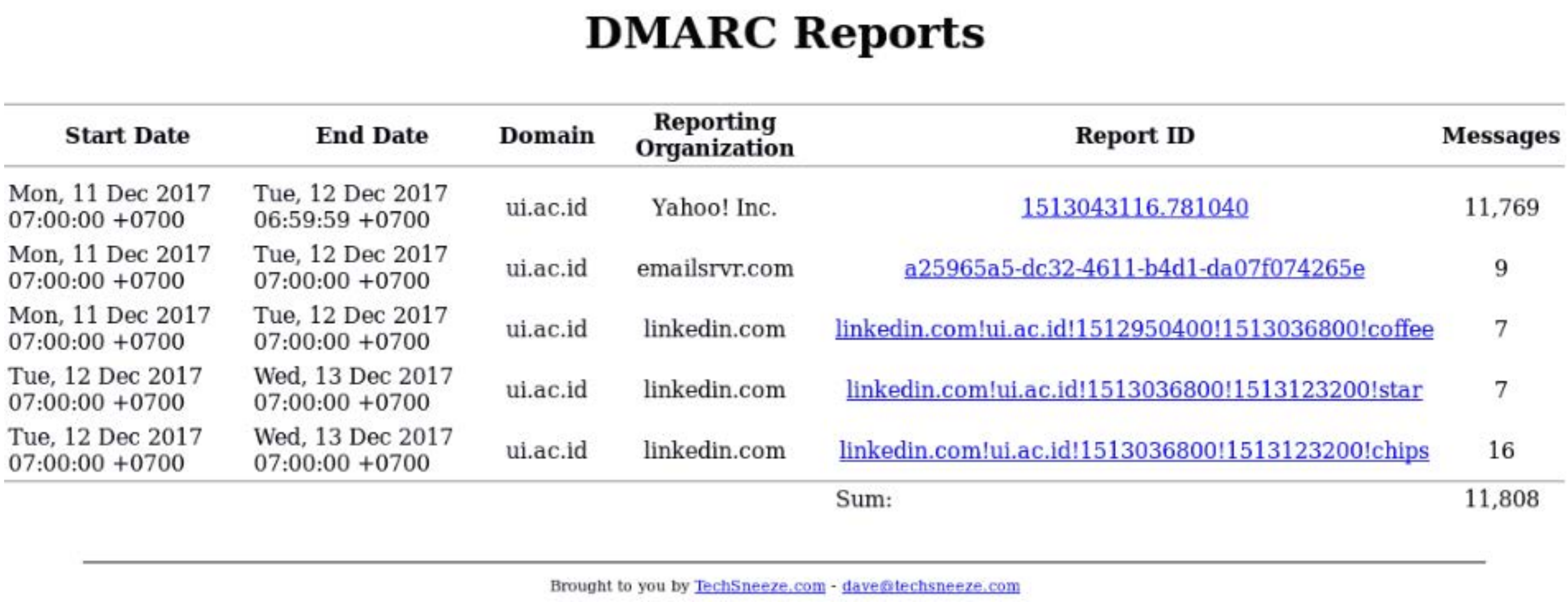
DMARC Forensic Report Example



```
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@examplepartici-
patingISP.com
--====================4311241154254624524254325====
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
--====================4311241154254624524254325====
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



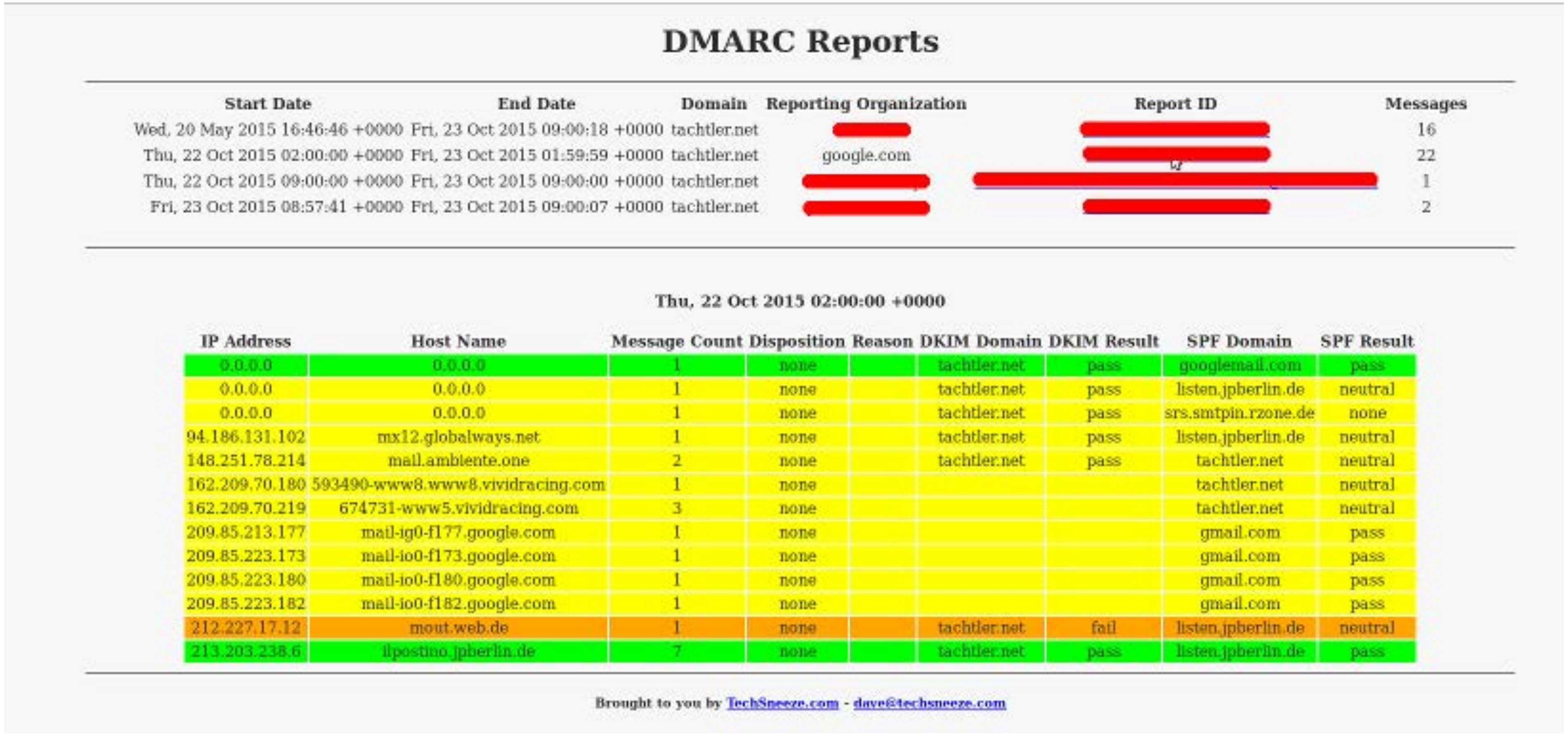
DMARC Reports

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

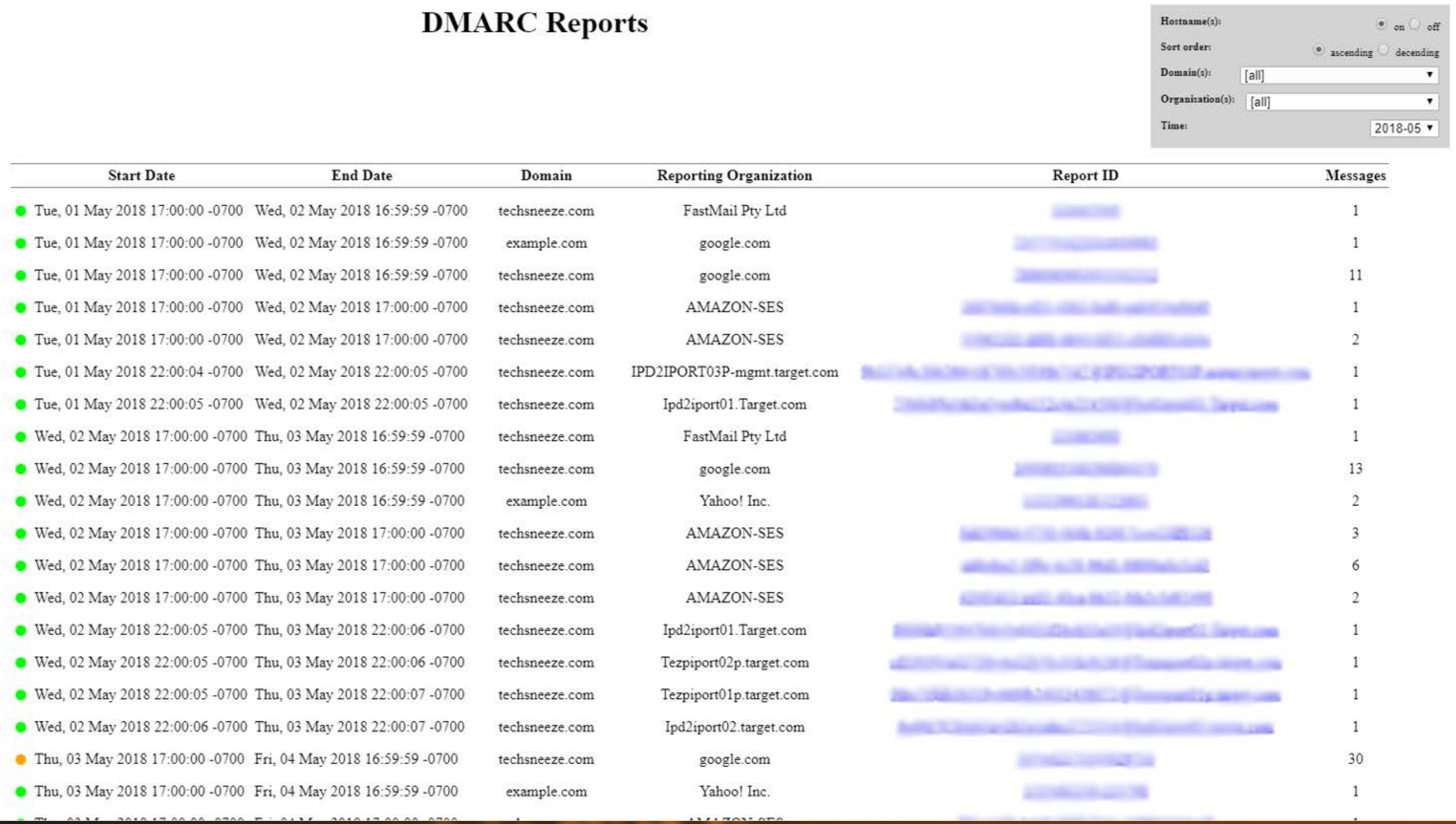
Thu, 22 Oct 2015 02:00:00 +0000

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] ▾

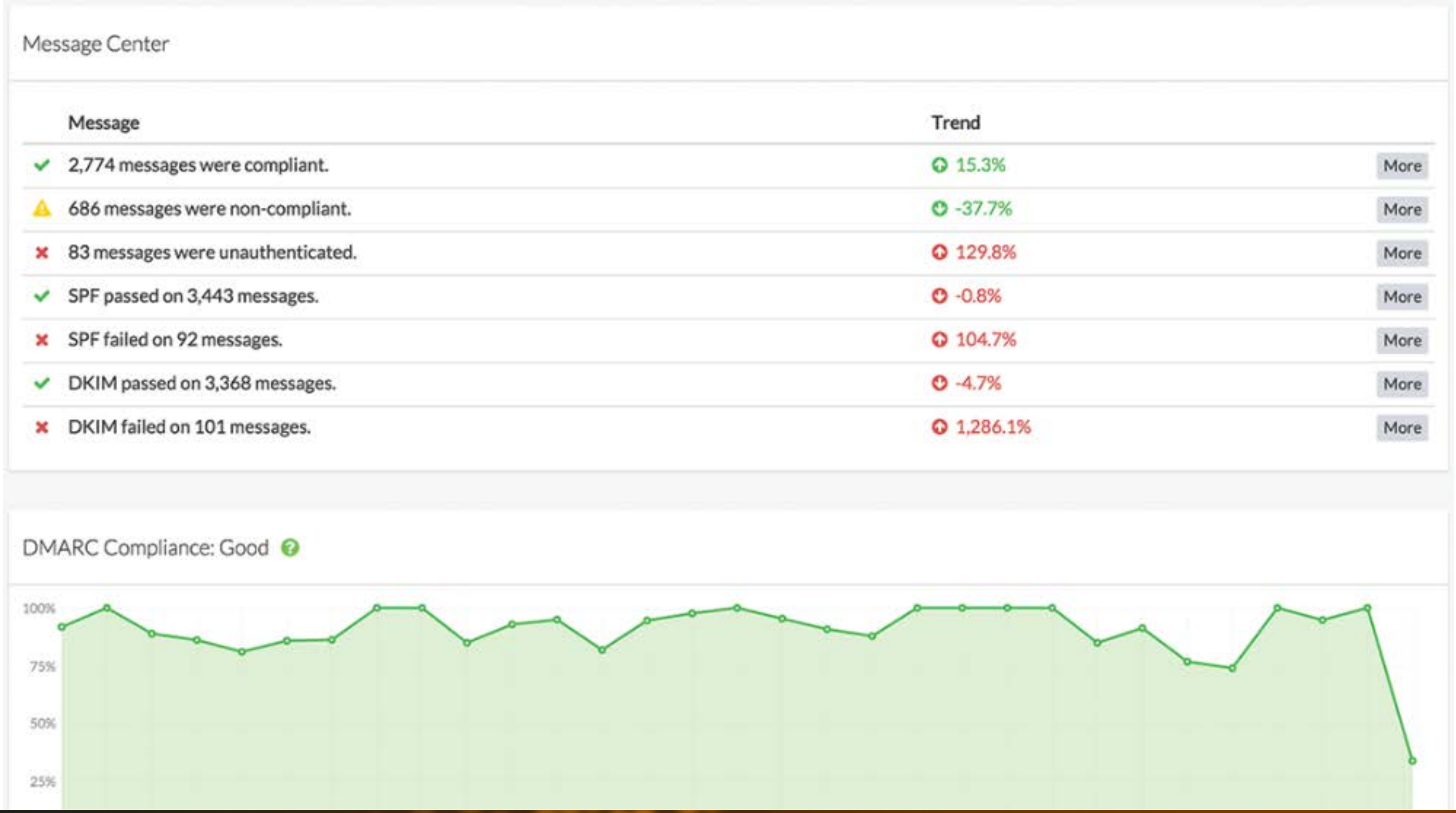
Organisation(s): [all] ▾

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



Message Center

	Message	Trend	
✓	2,774 messages were compliant.	15.3%	More
⚠	686 messages were non-compliant.	-37.7%	More
✗	83 messages were unauthenticated.	129.8%	More
✓	SPF passed on 3,443 messages.	-0.8%	More
✗	SPF failed on 92 messages.	104.7%	More
✓	DKIM passed on 3,368 messages.	-4.7%	More
✗	DKIM failed on 101 messages.	1,286.1%	More

DMARC Compliance: Good

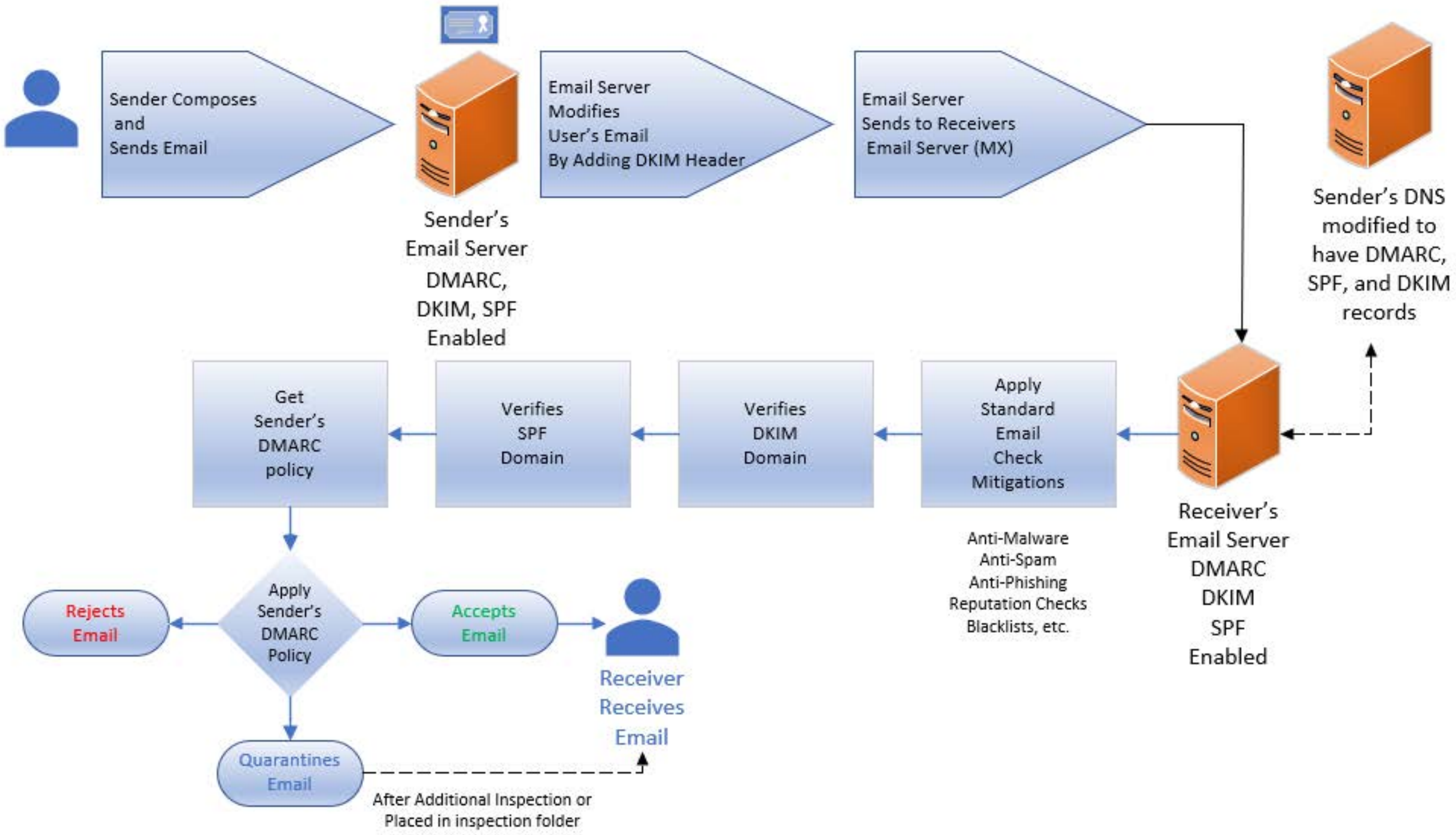
DMARC Reports

DMARC Reports – Caveats

- Some ISPs and big email providers, like Microsoft, do not send reports
- Be aware that if you use email proxies that per the DMARC RFC, the proxies will get your reports

SPF, DKIM, and DMARC

Putting it all together



Sender Composes and Sends Email

Sender's Email Server DMARC, DKIM, SPF Enabled

Email Server Modifies User's Email By Adding DKIM Header

Email Server Sends to Receivers Email Server (MX)

Sender's DNS modified to have DMARC, SPF, and DKIM records

Receiver's Email Server DMARC DKIM SPF Enabled

Apply Standard Email Check Mitigations

Anti-Malware
Anti-Spam
Anti-Phishing
Reputation Checks
Blacklists, etc.

Verifies DKIM Domain

Verifies SPF Domain

Get Sender's DMARC policy

Apply Sender's DMARC Policy

Rejects Email

Accepts Email

Receiver Receives Email

Quarantines Email

After Additional Inspection or Placed in inspection folder

Agenda

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

DMARC

Best Practices

- Set DMARC to None 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, 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

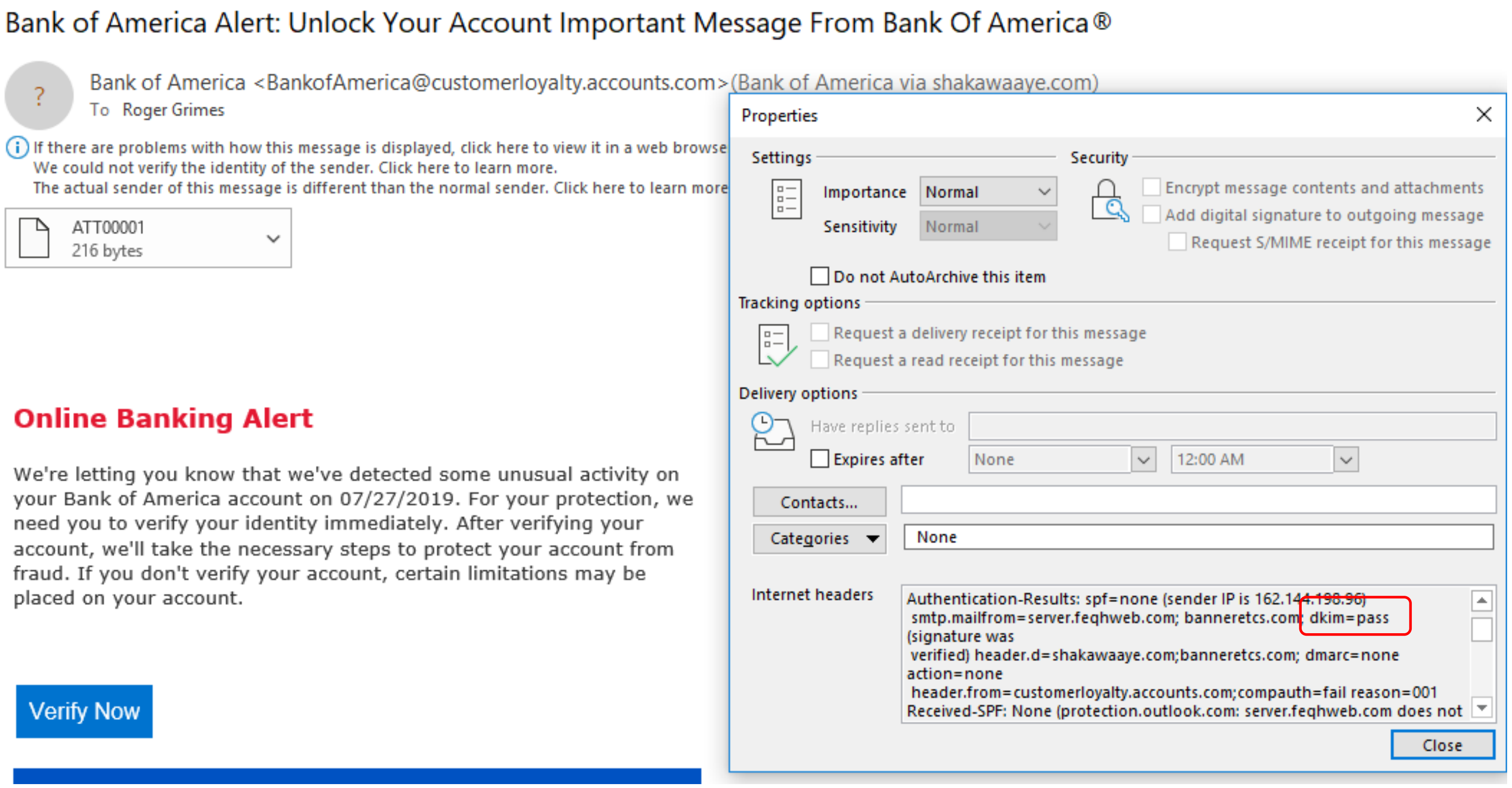
Summary

- 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



Bank of America Alert: Unlock Your Account Important Message From Bank Of America®

Bank of America <BankofAmerica@customerloyalty.accounts.com> (Bank of America via shakawaaye.com)
To Roger Grimes

If there are problems with how this message is displayed, click here to view it in a web browse
We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here to learn more

ATT00001
216 bytes

Online Banking Alert

We're letting you know that we've detected some unusual activity on your Bank of America account on 07/27/2019. For your protection, we need you to verify your identity immediately. After verifying your account, we'll take the necessary steps to protect your account from fraud. If you don't verify your account, certain limitations may be placed on your account.

Verify Now

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

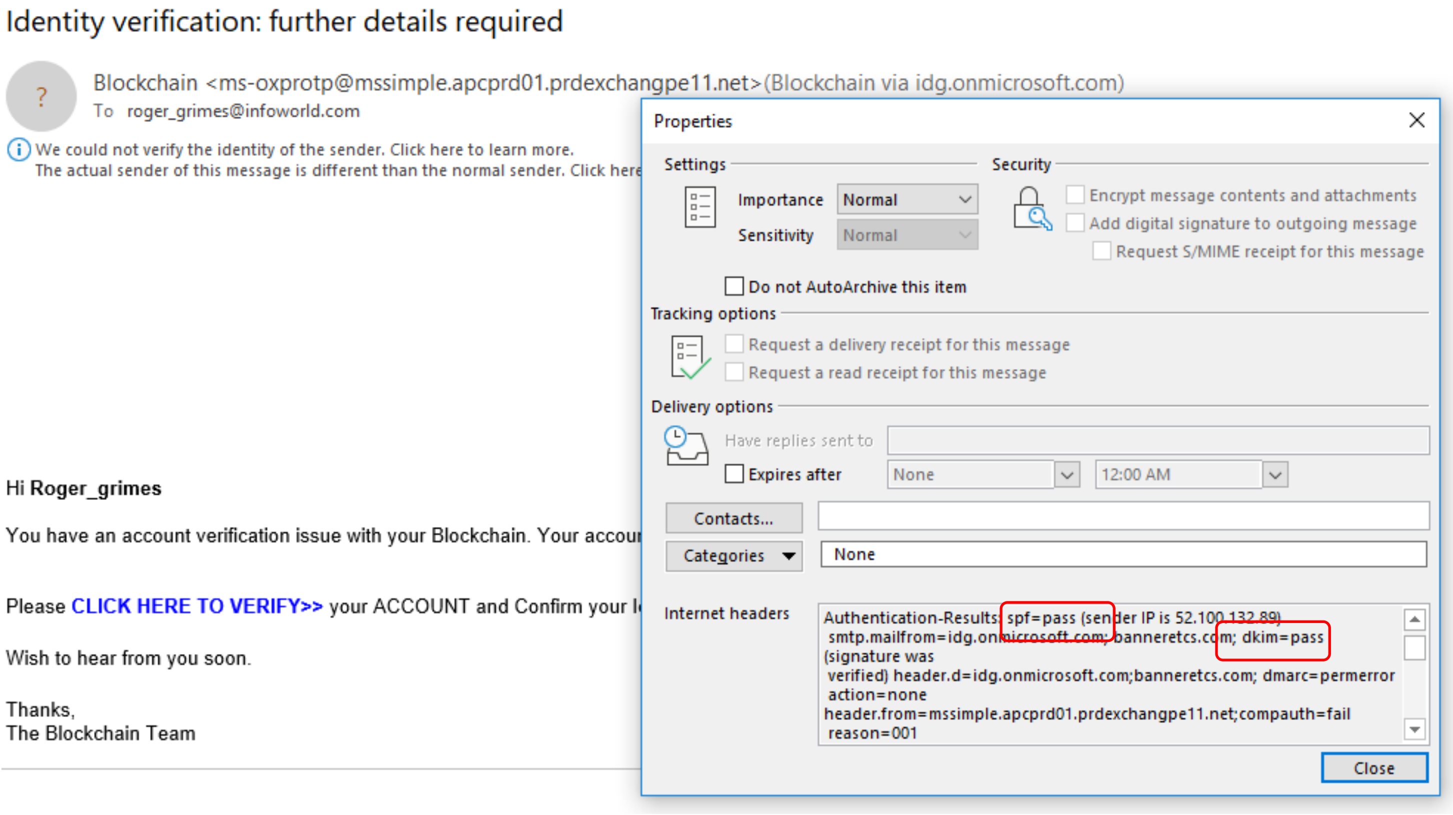
Internet headers

```
Authentication-Results: spf=none (sender IP is 162.144.198.96)
 smtp.mailfrom=server.feqhweb.com; banneretcs.com; dkim=pass
(signature was
 verified) header.d=shakawaaye.com;banneretcs.com; dmarc=none
action=none
 header.from=customerloyalty.accounts.com;compauth=fail reason=001
Received-SPF: None (protection.outlook.com: server.feqhweb.com does not
```

How Phishes Get By

Phishers Use SPF, DKIM, and DMARC

- Examples



Identity verification: further details required

Blockchain <ms-oxprotp@mssimple.apcprd01.prdexchangpe11.net>(Blockchain via idg.onmicrosoft.com)
To roger_grimes@infoworld.com

We could not verify the identity of the sender. Click here to learn more.
The actual sender of this message is different than the normal sender. Click here

Hi **Roger_grimes**

You have an account verification issue with your Blockchain. Your accou

Please CLICK HERE TO VERIFY>> your ACCOUNT and Confirm your l

Wish to hear from you soon.

Thanks,
The Blockchain Team

Properties

Settings
Importance: Normal
Sensitivity: Normal
□ Do not AutoArchive this item

Security
□ Encrypt message contents and attachments
□ Add digital signature to outgoing message
□ Request S/MIME receipt for this message

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

Categories: None

Internet headers

```
Authentication-Results: spf=pass (sender IP is 52.100.132.89)
 smtp.mailfrom=idg.onmicrosoft.com; banneretcs.com; dkim=pass
(signature was
 verified) header.d=idg.onmicrosoft.com;banneretcs.com; dmarc=permerror
 action=none
header.from=mssimple.apcprd01.prdexchangpe11.net;compauth=fail
 reason=001
```

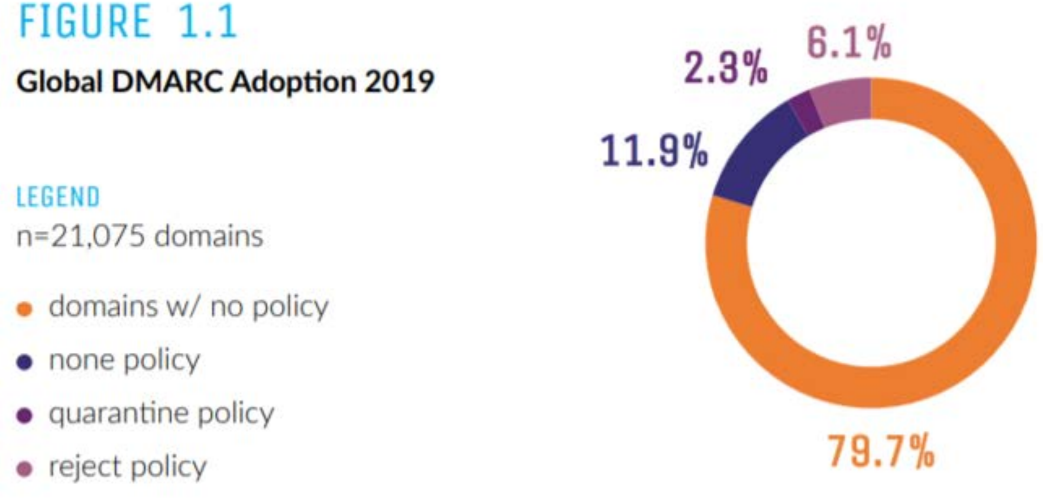
How Phishes Get By

Phishers Use DMARC and Many Senders Don’t

- 80% of legitimate companies don’t

FIGURE 1.1

Global DMARC Adoption 2019



https://250ok.com/email-deliverability/how-has-dmarc-adoption-evolved-since-2018-its-complicated/

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 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

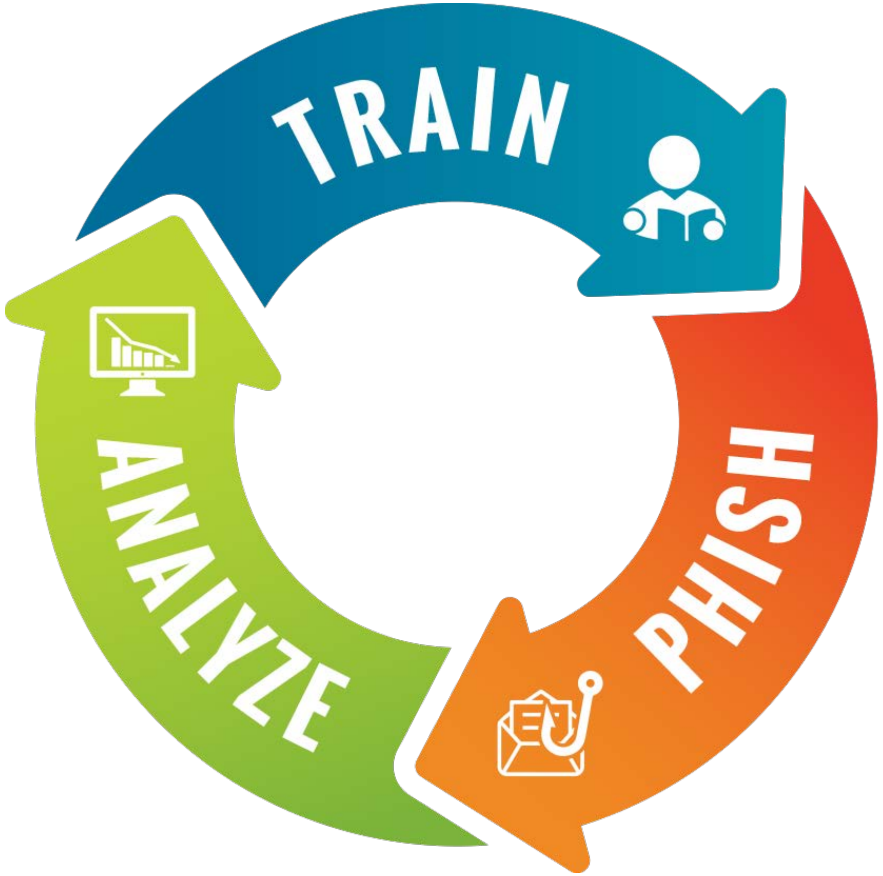
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users

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

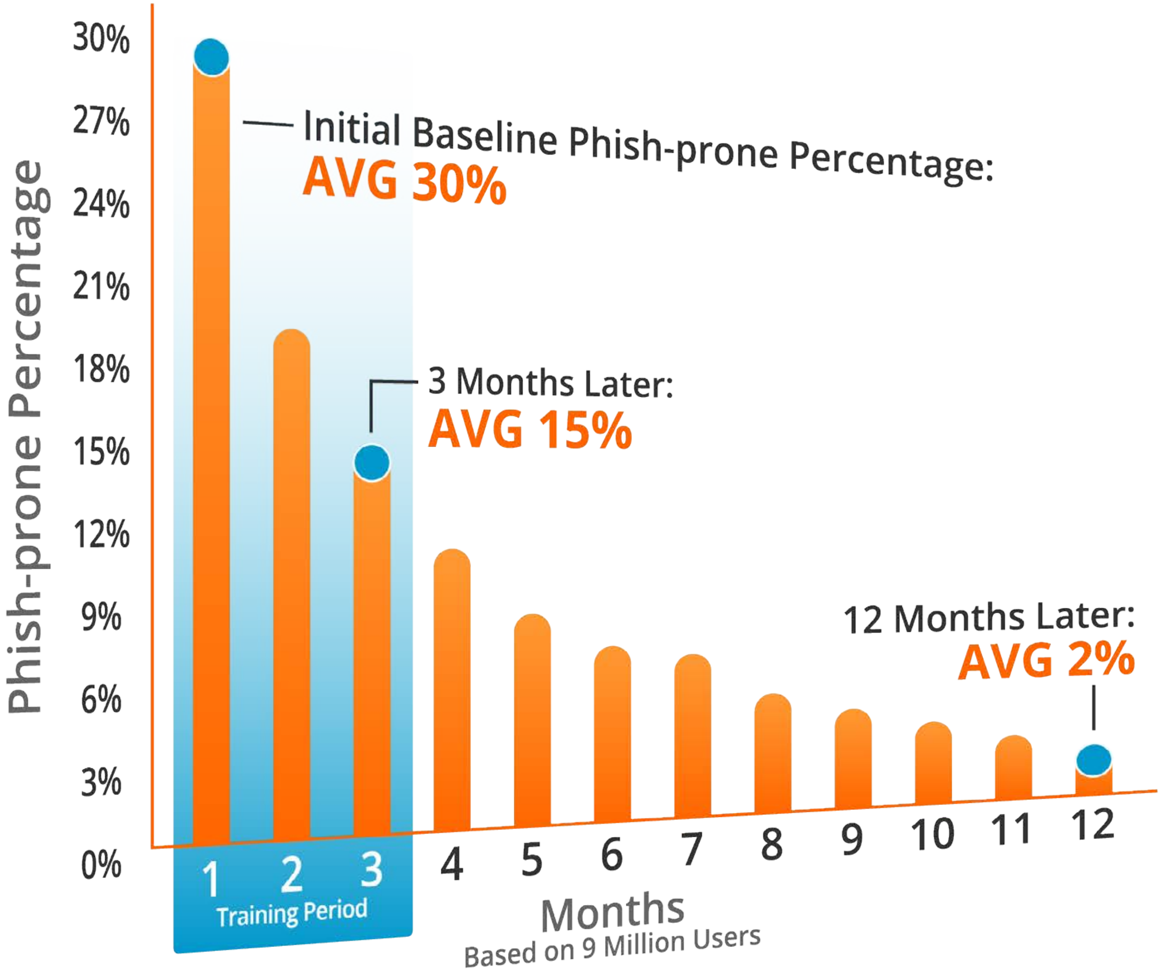
See the Results

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



Security Awareness Training Program That Works

- Drawn from a data set of **over six million users**
- Across **nearly 11K organizations**
- Segmented **by industry type** and **organization size**
- **241,762** Phishing Security Tests (PSTs)

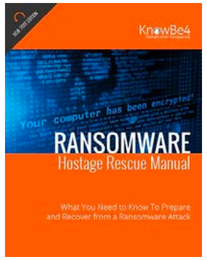


Resources

Free IT Security Tools

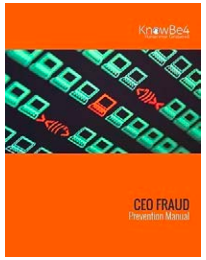
- Domain Doppelgänger
- Awareness Program Builder
- Domain Spoof Tool
- Mailserver Security Assessment
- Phish Alert
- Ransomware Simulator
- Weak Password Test
- Phishing Security Test
- Second Chance
- Email Exposure Check Pro
- Training Preview
- Breached Password Test

Whitepapers



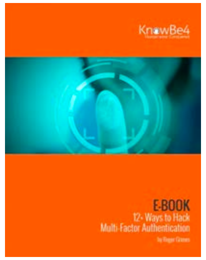
Ransomware Hostage Rescue Manual

Get the most complete Ransomware Manual packed with actionable info that you need to have to prevent infections, and what to do when you are hit with ransomware.



CEO Fraud Prevention Manual

CEO fraud is responsible for over $3 billion in losses. Don't be next. The CEO Fraud Prevention Manual provides a thorough overview of how executives are compromised, how to prevent such an attack and what to do if you become a victim.



12+ Ways to Hack Two-Factor Authentication

All multi-factor authentication (MFA) mechanisms can be compromised, and in some cases, it's as simple as sending a traditional phishing email. Want to know how to defend against MFA hacks? This whitepaper covers over a dozen different ways to hack various types of MFA and how to defend against those attacks.

» Learn More at www.KnowBe4.com/Resources «

Questions?

Roger A. Grimes

Data-Driven Defense Evangelist, KnowBe4

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