KnowBe4
Human error. Conquered.

Cyber CSI: Learn How to Forensically Examine Phishing Emails to Better Protect Your Organization Today

Roger A. Grimes
Data-Driven Security 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/

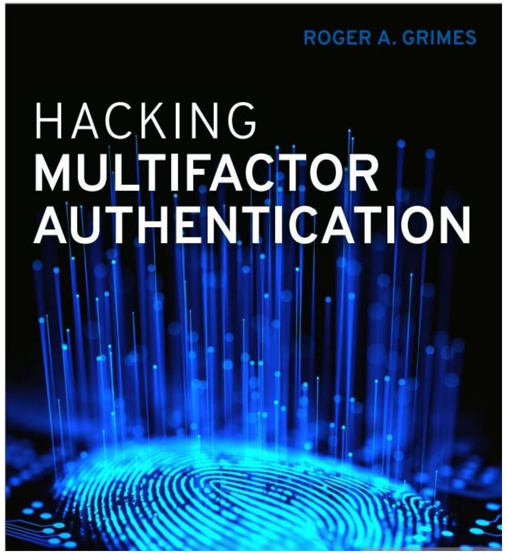
About Roger

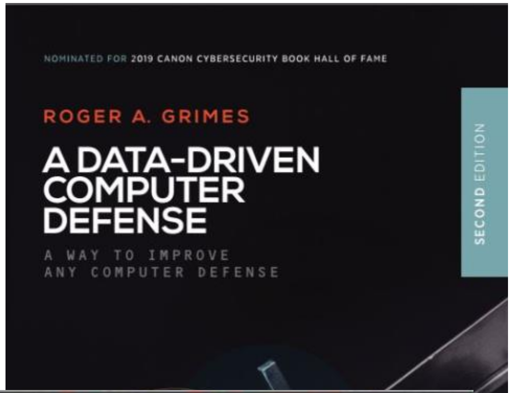
- 30 years plus in computer security, 20 years pen testing
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 13 books and over 1,200 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)

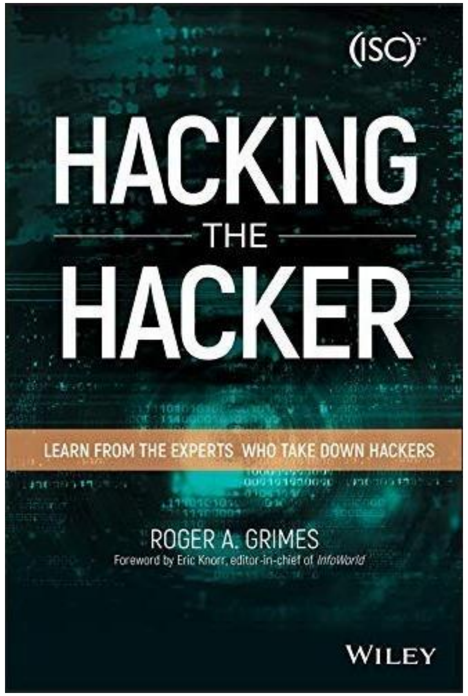
Certification exams passed include:

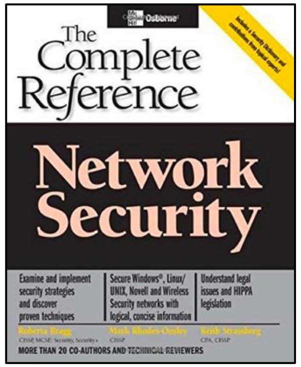
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

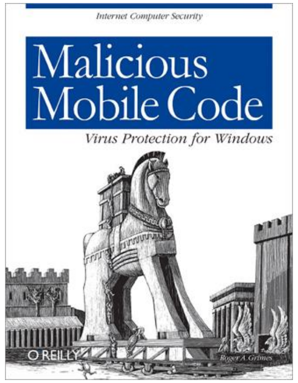
Roger’s Books

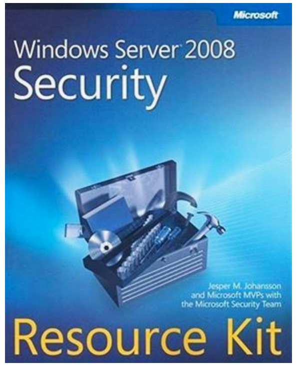


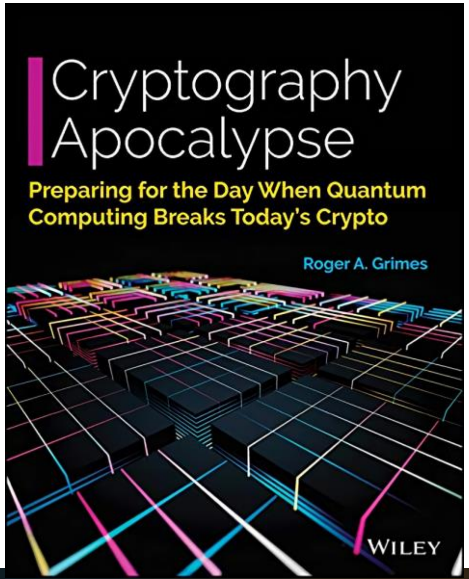

NOMINATED FOR 2019 CANON CYBERSECURITY BOOK HALL OF FAME
ROGER A. GRIMES
A DATA-DRIVEN COMPUTER DEFENSE
A WAY TO IMPROVE ANY COMPUTER DEFENSE
SECOND EDITION

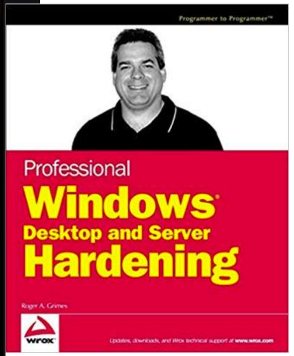

(ISC)²
HACKING THE HACKER
LEARN FROM THE EXPERTS WHO TAKE DOWN HACKERS
ROGER A. GRIMES
Foreword by Eric Knorr, editor-in-chief of InfoWorld
WILEY

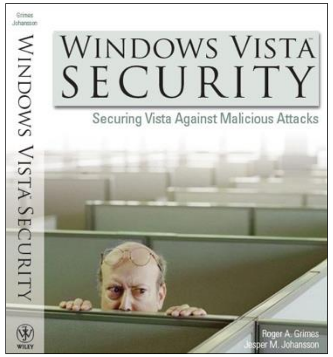


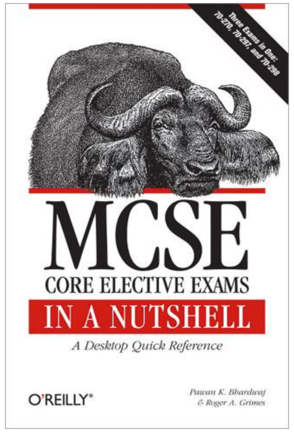


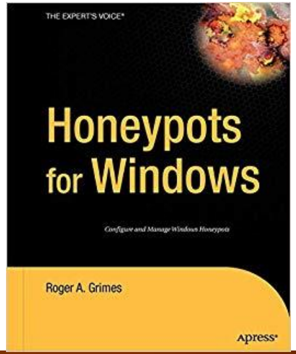

Microsoft
Windows Server 2008
Security
Jesper M. Johansson and Microsoft MVPs with the Microsoft Security Team
Resource Kit


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





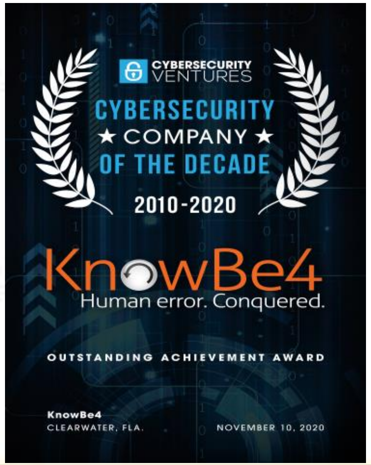

MCSE
CORE ELECTIVE EXAMS
IN A NUTSHELL
A Desktop Quick Reference
O'REILLY
Pawan K. Bhardwaj & Roger A. Grimes



TRAIN
PHISH
ANALYZE

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



Agenda

- How to Investigate
- Investigating Phishing
- Defenses

Agenda

- How to Investigate
- Investigating Phishing
- Defenses

How to Investigate

Main Methods

- Visual Inspection
- Research
- Forensic Analysis
- Tools

Be aware this can be a rabbit hole of a time consumption

How to Investigate

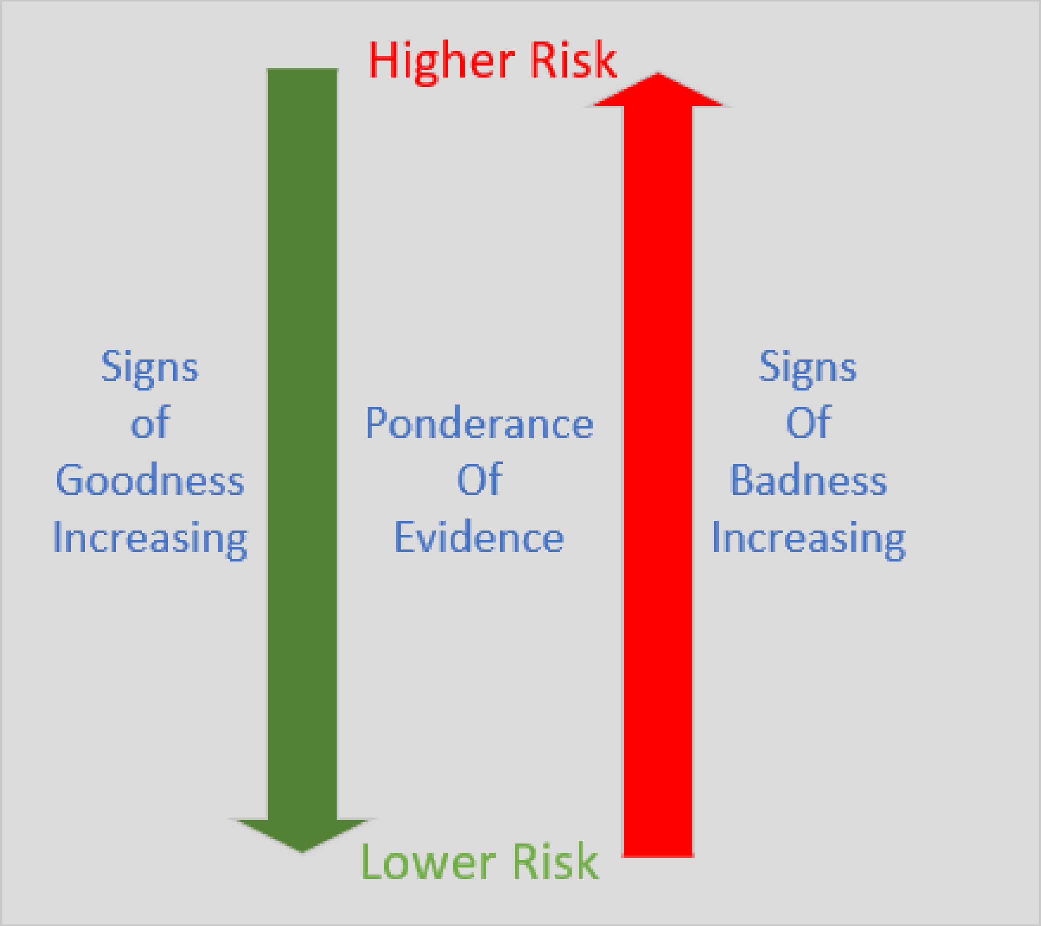
Note

- Anything beyond research, looking, or viewing text requires an isolated forensics “clean” system
- Preferably running an isolated virtual machine environment disconnected from the network having none of the same logon information as production environment

Evidence Collection

Ponderance of Evidence

- It’s rarely 100% clear
- If it was, stopping it would be easy
- It’s about Risk Analysis



Agenda

- How to Investigate
- Investigating Phishing
- Defenses

How to Investigate Email Phishes

How to Investigate Email Phishes

Email Structure

- Message Body
- Header

How to Investigate Email Phishes

Email Structure

- **Message Body**
  - Message
  - URLs
  - File Attachments
  - Embedded Images

How to Investigate Email Phishes

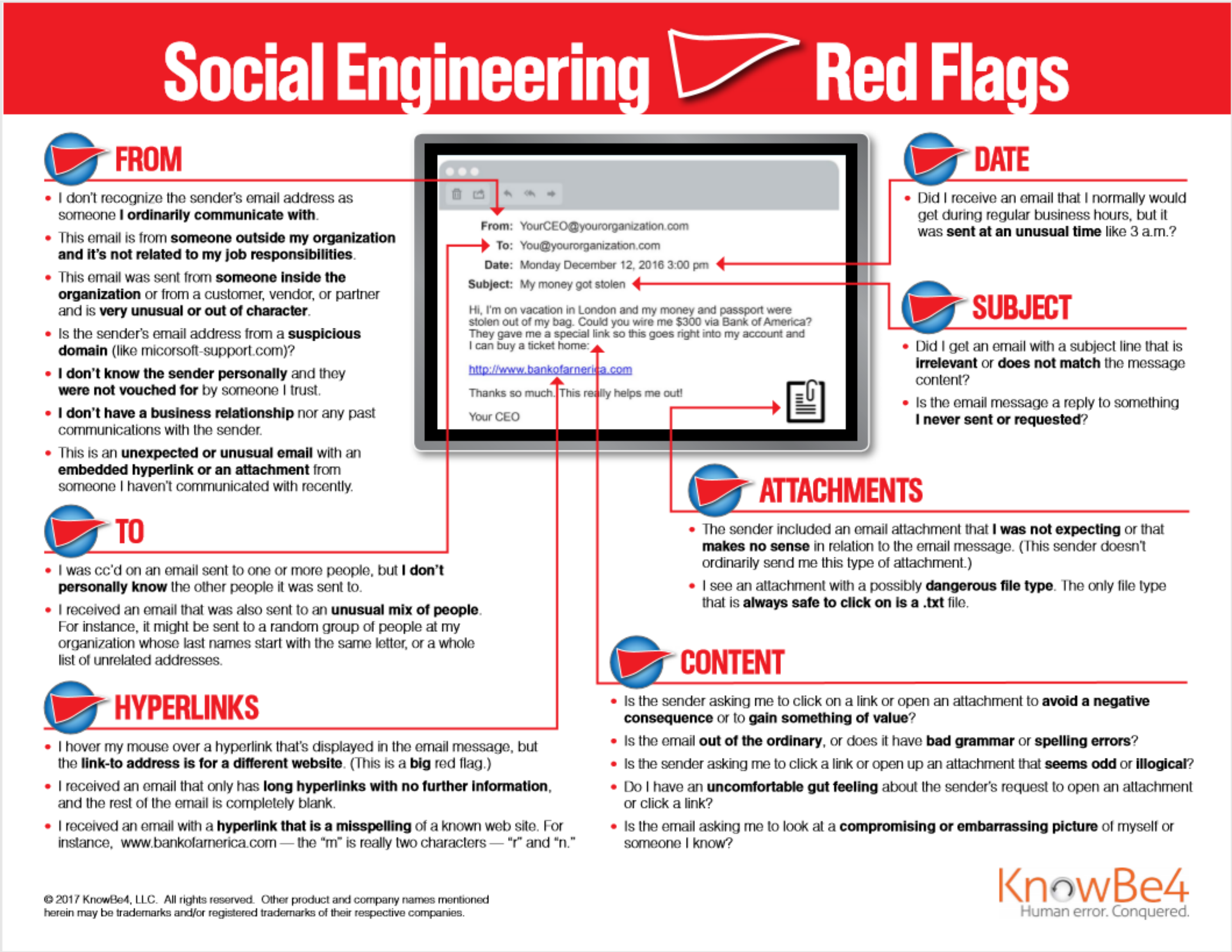
How to Spot Phishing

(each symptom adds risk)

- **Email/Message/Call Arrives Unexpectedly**
- **It's asking you to do something that person or company has never asked you to do before**
- **Requested action could be harmful**
- **Tries to create a sense of urgency ("stressor")**
- **Contains a link or file attachment**

- **Solution:** **When in doubt, call person on known legitimate phone number to confirm request or visit vender website using known legitimate link**

How to Investigate Email Phishes



Social Engineering Red Flags

From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2016 3:00 pm
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

KnowBe4
Human error. Conquered.

How to Investigate Email Phishes

Email Body – Signs of Maliciousness

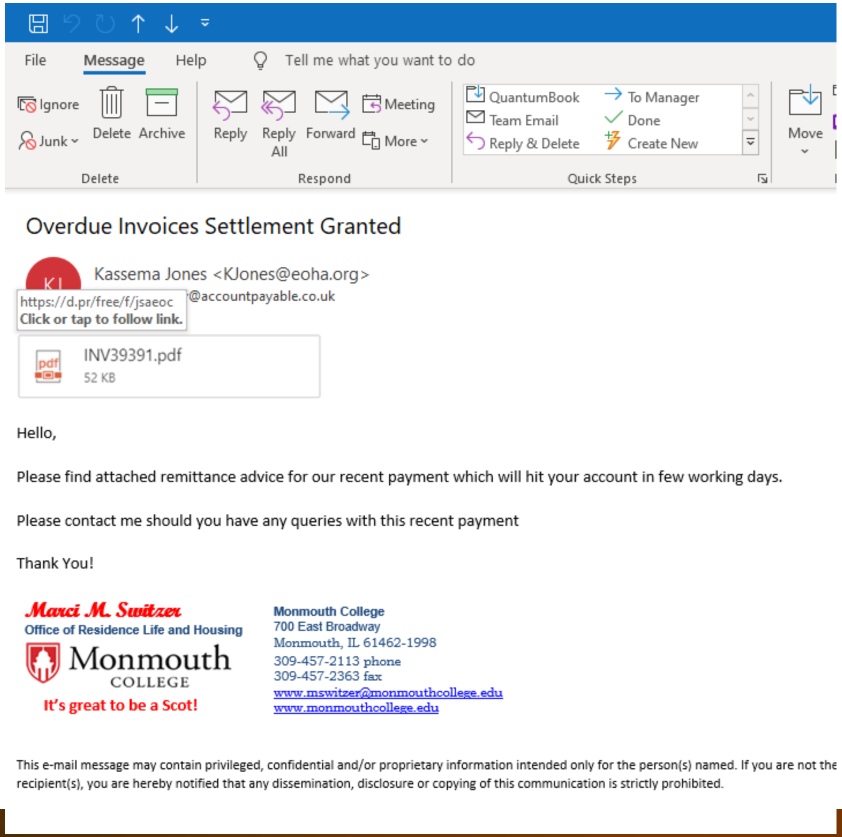
- File attachment image, not file attachment
- Image points to URL link

How to Investigate Email Phishes

Email Body – Signs of Maliciousness

- File attachment image, not file attachment
- Image points to URL link

Fake file attachments which are really images



Overdue Invoices Settlement Granted

Kassema Jones <KJones@eoha.org>
@accountpayable.co.uk

https://d.pr/free/f/jsaeoc
Click or tap to follow link.

INV39391.pdf
52 KB

Hello,

Please find attached remittance advice for our recent payment which will hit your account in few working days.

Please contact me should you have any queries with this recent payment

Thank You!

Marci M. Switzer
Office of Residence Life and Housing
Monmouth
COLLEGE
It's great to be a Scot!

Monmouth College
700 East Broadway
Monmouth, IL 61462-1998
309-457-2113 phone
309-457-2363 fax
www.mswitzer@monmouthcollege.edu
www.monmouthcollege.edu

This e-mail message may contain privileged, confidential and/or proprietary information intended only for the person(s) named. If you are not the recipient(s), you are hereby notified that any dissemination, disclosure or copying of this communication is strictly prohibited.

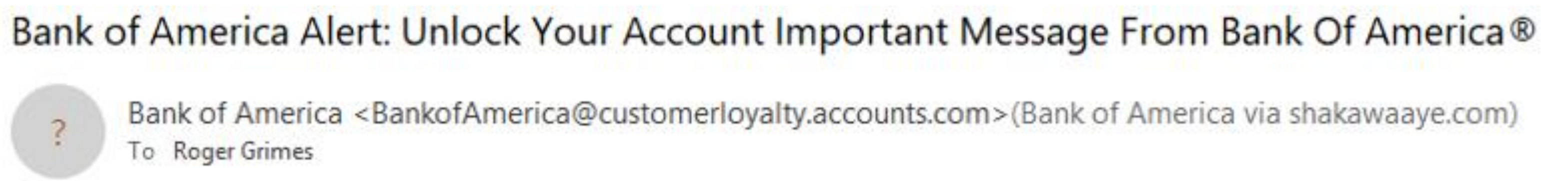
How to Investigate Email Phishes

Email Body – Signs of Maliciousness

- Disjointed “From/Received/Reply” email addresses
- Mis-Branded URLs
- Disconnected/bogus URLs
- Unexpected file attachments
- MIME-type mismatches

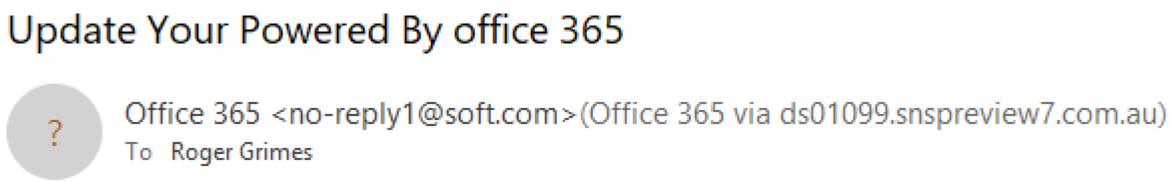
How to Investigate Email Phishes

Spotting Disconnected Email Addresses

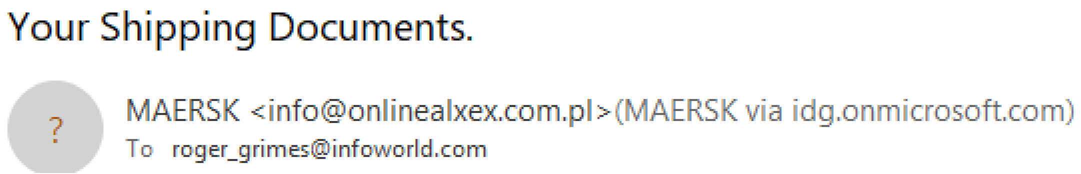

Bank of America Alert: Unlock Your Account Important Message From Bank Of America®

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

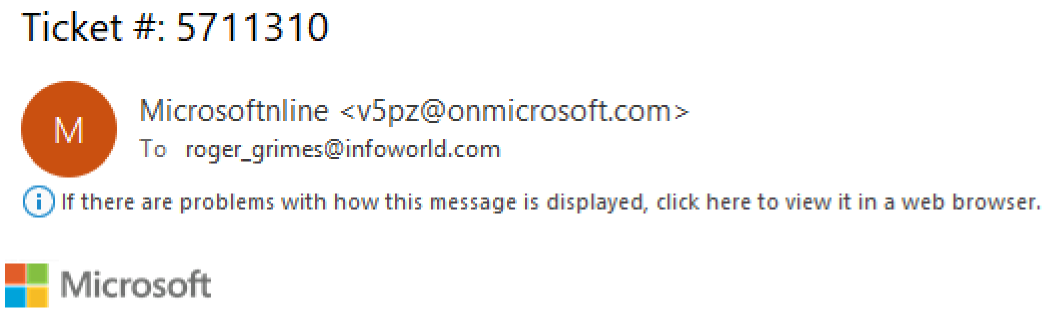
Brand/URL mismatches


Update Your Powered By office 365

Office 365 <no-reply1@soft.com>(Office 365 via ds01099.snspreview7.com.au)
To Roger Grimes


Your Shipping Documents.

MAERSK <info@onlinealxex.com.pl>(MAERSK via idg.onmicrosoft.com)
To roger_grimes@infoworld.com

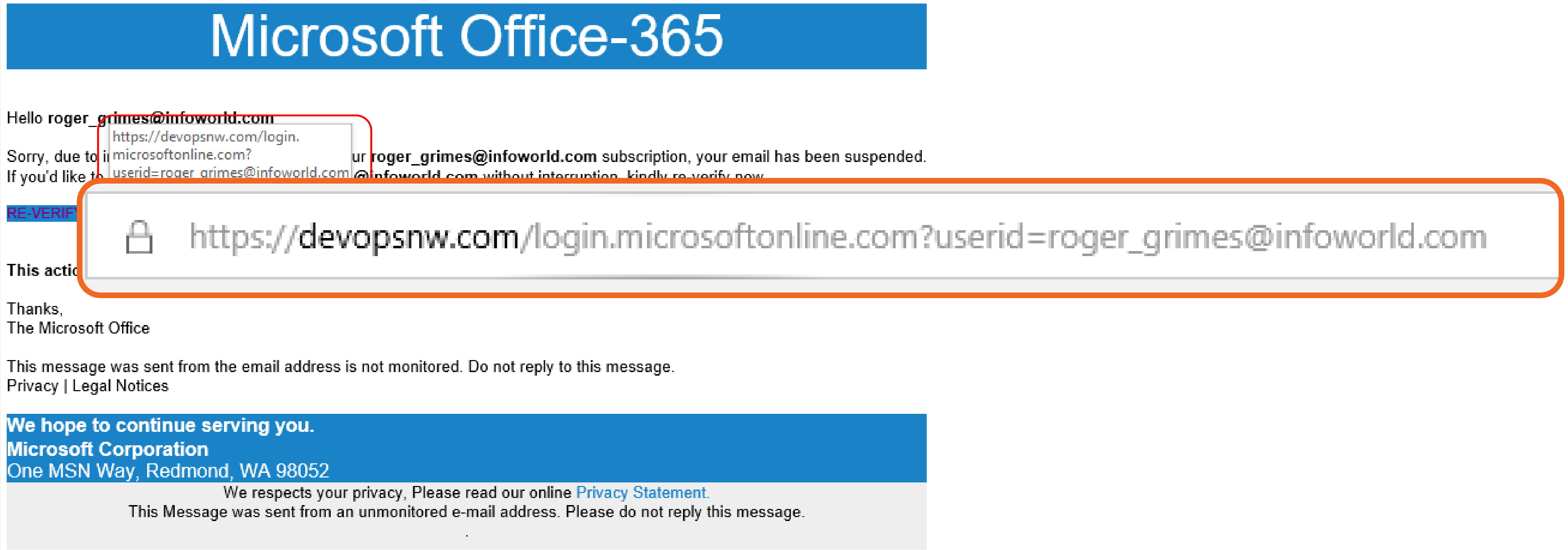

Ticket #: 5711310

Microsoftnline <v5pz@onmicrosoft.com>
To roger_grimes@infoworld.com

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

How to Investigate Email Phishes

Spotting Rogue URLs



Microsoft Office-365

Hello roger_grimes@infoworld.com

https://devopsnw.com/login.
microsoftonline.com?
userid=roger_grimes@infoworld.com

Sorry, due to i ur roger_grimes@infoworld.com subscription, your email has been suspended.
If you'd like to @infoworld.com without interruption, kindly re-verify now.

RE-VERIF

https://devopsnw.com/login.microsoftonline.com?userid=roger_grimes@infoworld.com

This actio

Thanks,
The Microsoft Office

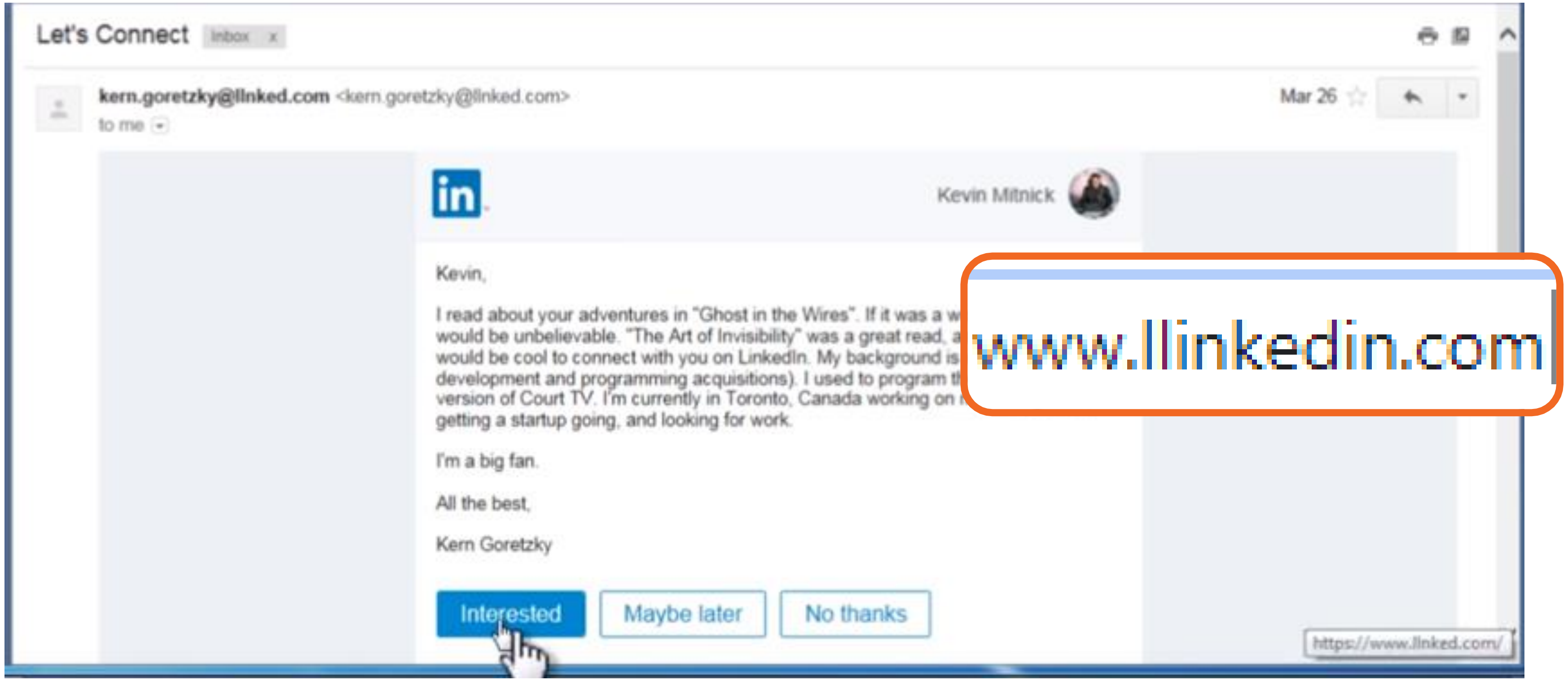
This message was sent from the email address is not monitored. Do not reply to this message.
Privacy | Legal Notices

We hope to continue serving you.
Microsoft Corporation
One MSN Way, Redmond, WA 98052

We respects your privacy, Please read our online Privacy Statement.
This Message was sent from an unmonitored e-mail address. Please do not reply this message.

How to Investigate Email Phishes

Spotting Rogue URLs



kern.goretzky@llnked.com <kern.goretzky@llnked.com>
to me

Mar 26

Kevin,

I read about your adventures in "Ghost in the Wires". If it was a w
would be unbelievable. "The Art of Invisibility" was a great read, a
would be cool to connect with you on LinkedIn. My background is
development and programming acquisitions). I used to program t
version of Court TV. I'm currently in Toronto, Canada working on
getting a startup going, and looking for work.

I'm a big fan.

All the best,

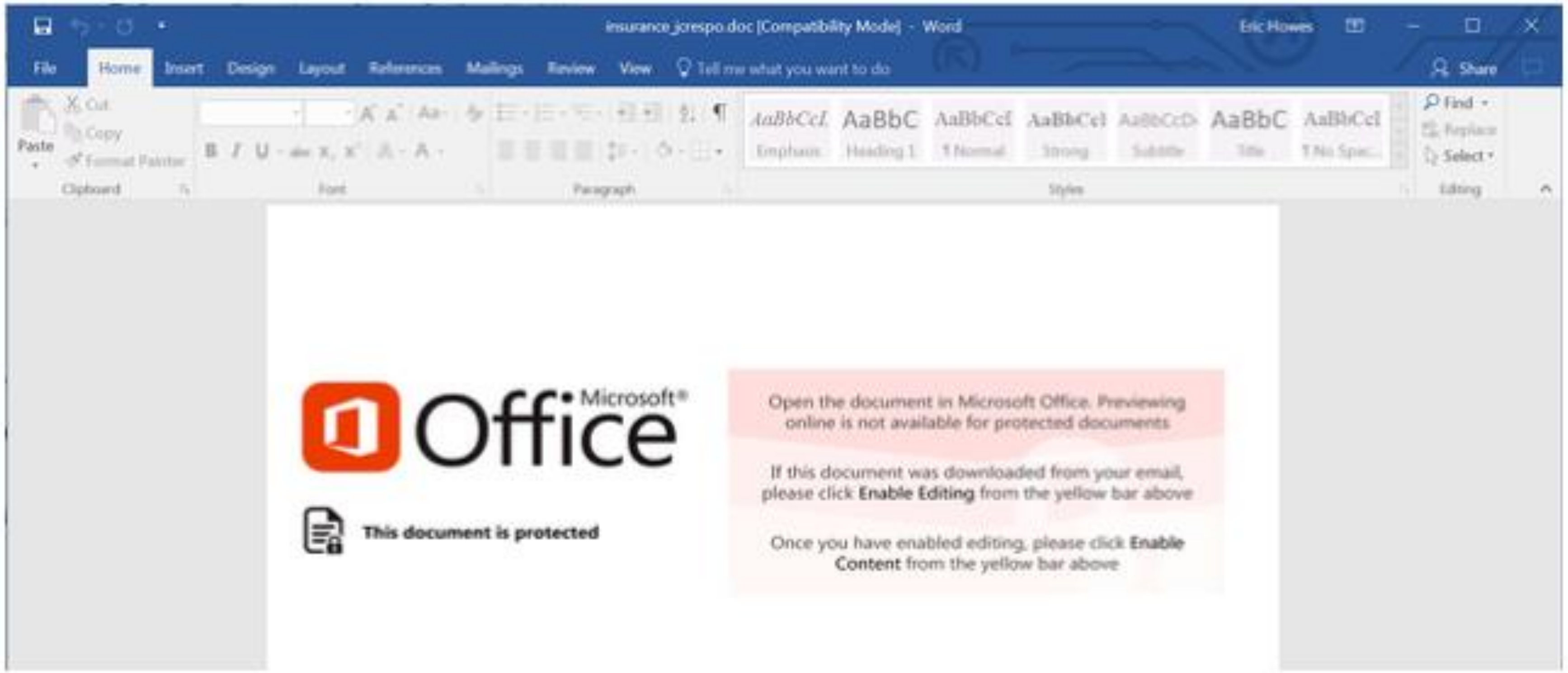
Kern Goretzky

https://www.llnked.com/

www.llinkedin.com

How to Investigate Email Phishes

Instructions to Ignore Warnings or Activate Content



This document is protected

Open the document in Microsoft Office. Previewing online is not available for protected documents

If this document was downloaded from your email, please click **Enable Editing** from the yellow bar above

Once you have enabled editing, please click **Enable Content** from the yellow bar above

"Helpful instructions" for opening document

How to Investigate Email Phishes

Email Body – Signs of Maliciousness

Keeping up-to-date on the various phishing trends

- **KnowBe4 blog** (https://blog.knowbe4.com)
  - Example: https://blog.knowbe4.com/double-the-phish-double-the-phun
- **KnowBe4 resources** https://blog.knowbe4.com/resources
- **Phish of the Week**
- **Quarterly Infographic**

How to Investigate Email Phishes

Email Structure

- **Header**
  - Required fields
  - Optional information
  - Lots of garbage that means something to somebody…maybe…

How to Investigate Email Phishes

Email Structure

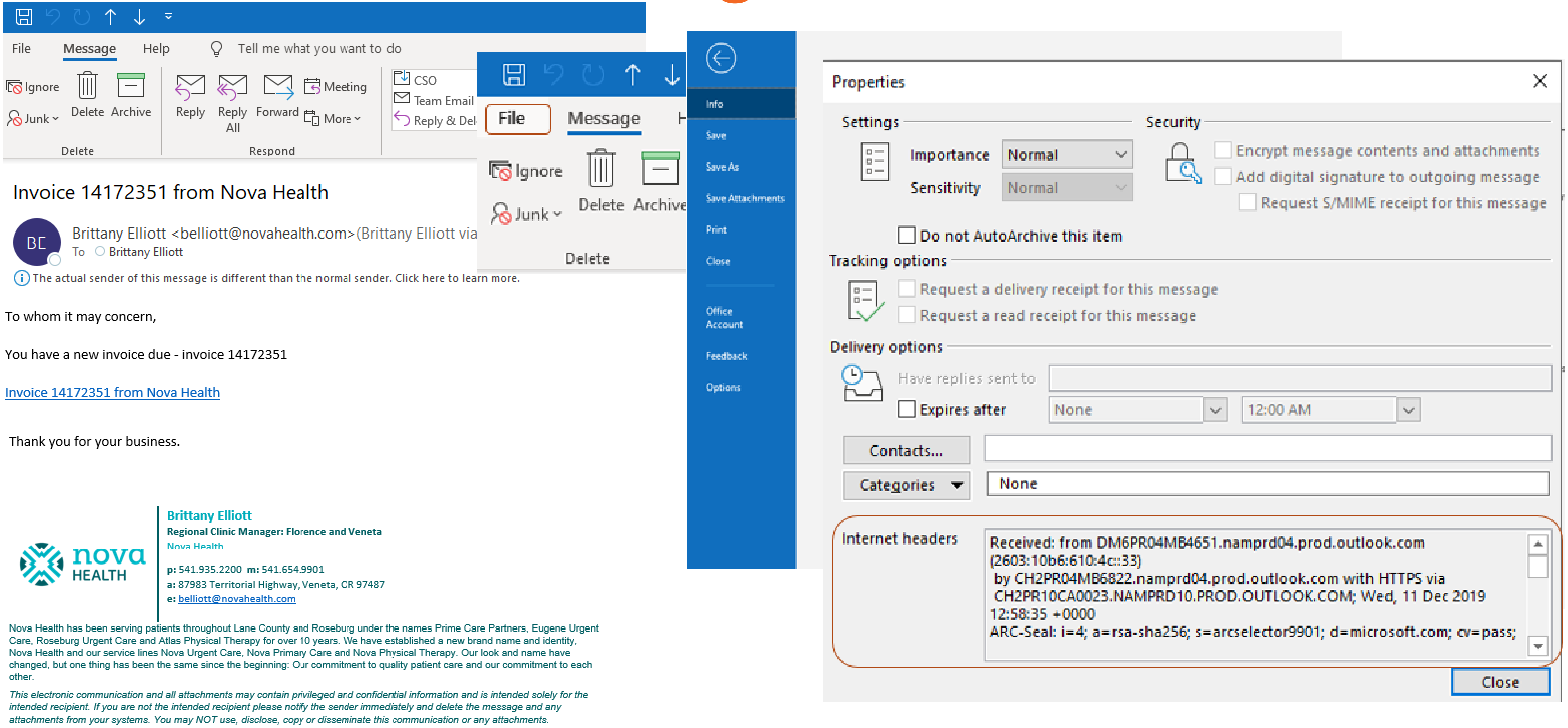
- Header
  - It is changed or added to each time it passes through an email server/gateway/inspection service, which is
    - Officially known as a Mail Transfer Agent (MTA)
  - You can use it to follow the email's path from source to destination (in reverse time order)
- Note: Sender or intermediate MTA can forge/change parts. Forwarding message deletes old header.

How to Investigate Email Phishes

Email Structure

- Viewing Email Headers
  - Different instructions per email client
  - **Outlook** – Open email, File, Properties, Internet Headers, Ctrl-A, Ctrl-C, paste into Notepad.exe

How to Investigate Email Phishes



Invoice 14172351 from Nova Health

Brittany Elliott <belliott@novahealth.com>(Brittany Elliott via

To ○ Brittany Elliott

ⓘ The actual sender of this message is different than the normal sender. Click here to learn more.

To whom it may concern,

You have a new invoice due - invoice 14172351

Invoice 14172351 from Nova Health

Thank you for your business.

nova HEALTH

Brittany Elliott
Regional Clinic Manager: Florence and Veneta
Nova Health

p: 541.935.2200 m: 541.654.9901
a: 87983 Territorial Highway, Veneta, OR 97487
e: belliott@novahealth.com

Nova Health has been serving patients throughout Lane County and Roseburg under the names Prime Care Partners, Eugene Urgent Care, Roseburg Urgent Care and Atlas Physical Therapy for over 10 years. We have established a new brand name and identity, Nova Health and our service lines Nova Urgent Care, Nova Primary Care and Nova Physical Therapy. Our look and name have changed, but one thing has been the same since the beginning: Our commitment to quality patient care and our commitment to each other.

This electronic communication and all attachments may contain privileged and confidential information and is intended solely for the intended recipient. If you are not the intended recipient please notify the sender immediately and delete the message and any attachments from your systems. You may NOT use, disclose, copy or disseminate this communication or any attachments.

Properties

Settings

Importance: Normal

Sensitivity: Normal

Security

□ Encrypt message contents and attachments

□ Add digital signature to outgoing message

□ Request S/MIME receipt for this message

□ Do not AutoArchive this item

Tracking options

□ Request a delivery receipt for this message

□ Request a read receipt for this message

Delivery options

Have replies sent to

□ Expires after None 12:00 AM

Contacts...

Categories: None

Internet headers

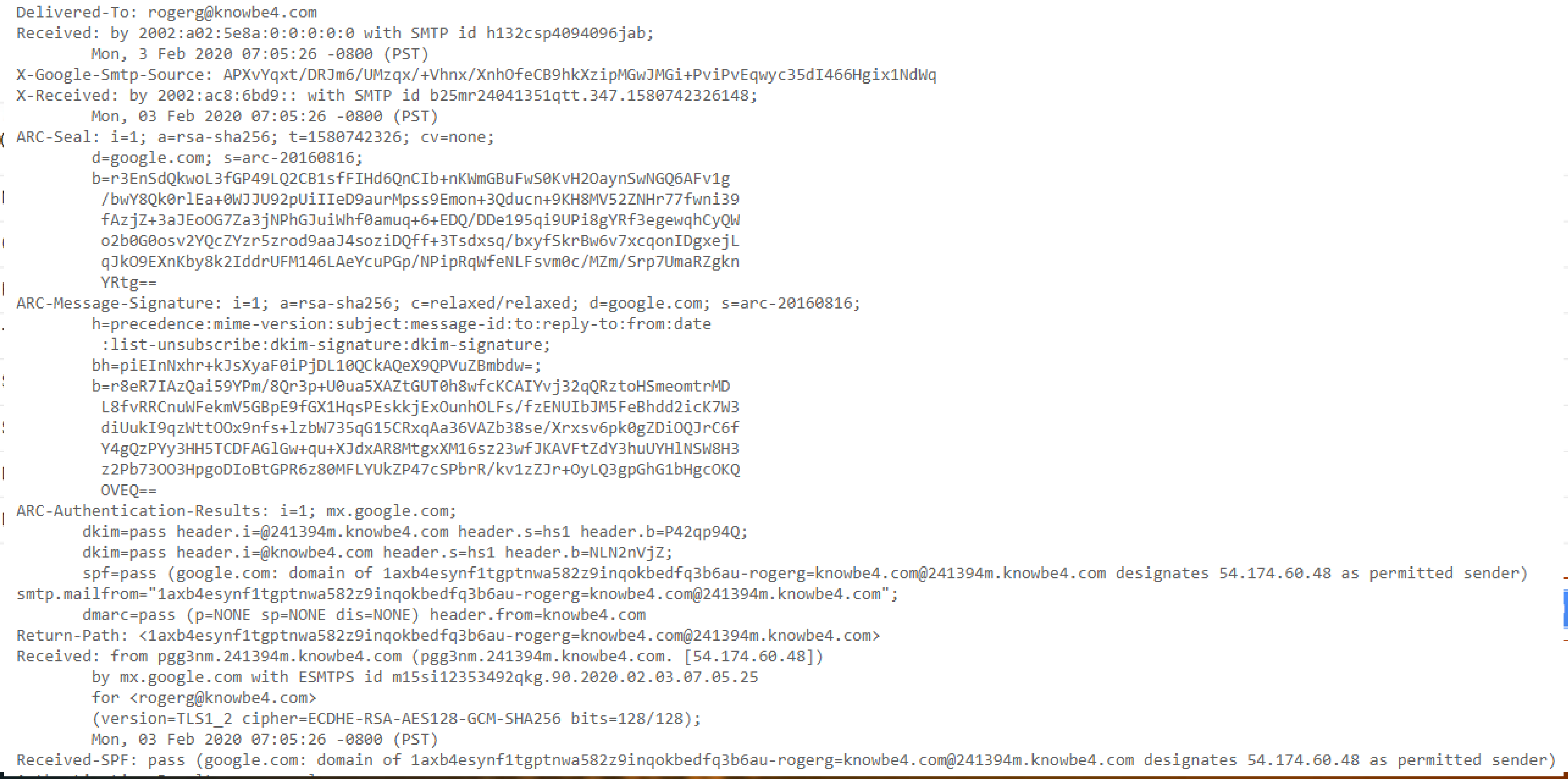
```
Received: from DM6PR04MB4651.namprd04.prod.outlook.com
(2603:10b6:610:4c::33)
 by CH2PR04MB6822.namprd04.prod.outlook.com with HTTPS via
 CH2PR10CA0023.NAMPRD10.PROD.OUTLOOK.COM; Wed, 11 Dec 2019
12:58:35 +0000
ARC-Seal: i=4; a=rsa-sha256; s=arcselector9901; d=microsoft.com; cv=pass;
```

How to Investigate Email Phishes

Email Structure

- Viewing Email Headers
  - Different per email client
  - **Gmail** – Open email, click on three dots on right, click on **Show original**, **Copy to clipboard**

How to Investigate Email Phishes



```
Delivered-To: rogerg@knowbe4.com
Received: by 2002:a02:5e8a:0:0:0:0:0 with SMTP id h132csp4094096jab;
        Mon, 3 Feb 2020 07:05:26 -0800 (PST)
X-Google-Smtp-Source: APXvYqxt/DRJm6/UMzqx/+Vhnx/XnhOfeCB9hkXzipMGwJMGi+PviPvEqwyc35dI466Hgix1NdWq
X-Received: by 2002:ac8:6bd9:: with SMTP id b25mr24041351qtt.347.1580742326148;
        Mon, 03 Feb 2020 07:05:26 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1580742326; cv=none;
        d=google.com; s=arc-20160816;
        b=r3EnSdQkwoL3fGP49LQ2CB1sfFIHd6QnCIb+nKWmGBuFwS0KvH2OaynSwNGQ6AFv1g
         /bwY8Qk0rlEa+0WJJU92pUiIIeD9aurMpss9Emon+3Qducn+9KH8MV52ZNHr77fwni39
         fAzjZ+3aJEoOG7Za3jNPhGJuiWhf0amuq+6+EDQ/DDe195qi9UPi8gYRf3egewqhCyQW
         o2b0G0osv2YQcZYzr5zrod9aaJ4soziDQff+3Tsdxsq/bxyfSkrBw6v7xcqonIDgxejL
         qJkO9EXnKby8k2IddrUFM146LAeYcuPGp/NPipRqWfeNLFsvm0c/MZm/Srp7UmaRZgkn
         YRtg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=precedence:mime-version:subject:message-id:to:reply-to:from:date
         :list-unsubscribe:dkim-signature:dkim-signature;
        bh=piEInNxhr+kJsXyaF0iPjDL10QCkAQeX9QPVuZBmbdw=;
        b=r8eR7IAzQai59YPm/8Qr3p+U0ua5XAZtGUT0h8wfcKCAIYvj32qQRztoHSmeomtrMD
         L8fvRRCnuWFekmV5GBpE9fGX1HqsPEskkjExOunhOLFs/fzENUIbJM5FeBhdd2icK7W3
         diUukI9qzWttOOx9nfs+lzbW735qG15CRxqAa36VAZb38se/Xrxsv6pk0gZDiOQJrC6f
         Y4gQzPYy3HH5TCDFAGlGw+qu+XJdxAR8MtgxXM16sz23wfJKAVFtZdY3huUYHlNSW8H3
         z2Pb73OO3HpgoDIoBtGPR6z80MFLYUkZP47cSPbrR/kv1zZJr+OyLQ3gpGhG1bHgcOKQ
         OVEQ==
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@241394m.knowbe4.com header.s=hs1 header.b=P42qp94Q;
       dkim=pass header.i=@knowbe4.com header.s=hs1 header.b=NLN2nVjZ;
       spf=pass (google.com: domain of 1axb4esynf1tgptnwa582z9inqokbedfq3b6au-rogerg=knowbe4.com@241394m.knowbe4.com designates 54.174.60.48 as permitted sender) smtp.mailfrom="1axb4esynf1tgptnwa582z9inqokbedfq3b6au-rogerg=knowbe4.com@241394m.knowbe4.com";
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=knowbe4.com
Return-Path: <1axb4esynf1tgptnwa582z9inqokbedfq3b6au-rogerg=knowbe4.com@241394m.knowbe4.com>
Received: from pgg3nm.241394m.knowbe4.com (pgg3nm.241394m.knowbe4.com. [54.174.60.48])
        by mx.google.com with ESMTPS id m15si12353492qkg.90.2020.02.03.07.05.25
        for <rogerg@knowbe4.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Mon, 03 Feb 2020 07:05:26 -0800 (PST)
Received-SPF: pass (google.com: domain of 1axb4esynf1tgptnwa582z9inqokbedfq3b6au-rogerg=knowbe4.com@241394m.knowbe4.com designates 54.174.60.48 as permitted sender)
```

How to Investigate Email Phishes

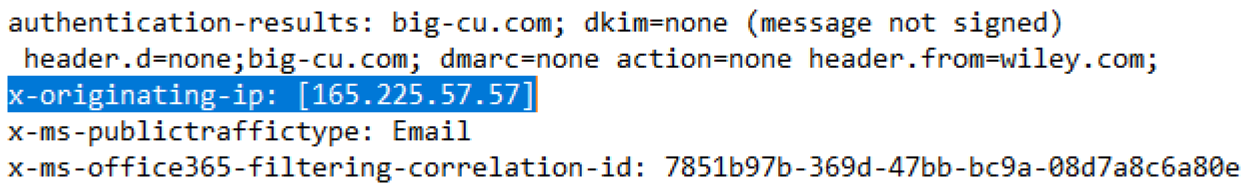
Email Structure

- Finding Original Sender

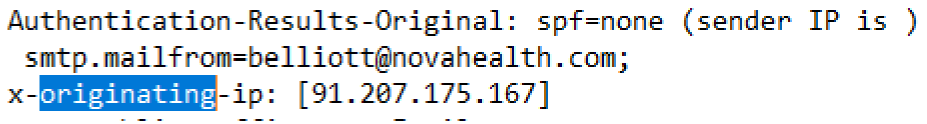
How to Investigate Email Phishes

Email Structure

- Header – Notable Fields
  - **x-originating-ip** – public IP address of original sender
    - Unfortunately, optional



```
authentication-results: big-cu.com; dkim=none (message not signed)
 header.d=none;big-cu.com; dmarc=none action=none header.from=wiley.com;
x-originating-ip: [165.225.57.57]
x-ms-publictraffictype: Email
x-ms-office365-filtering-correlation-id: 7851b97b-369d-47bb-bc9a-08d7a8c6a80e
```



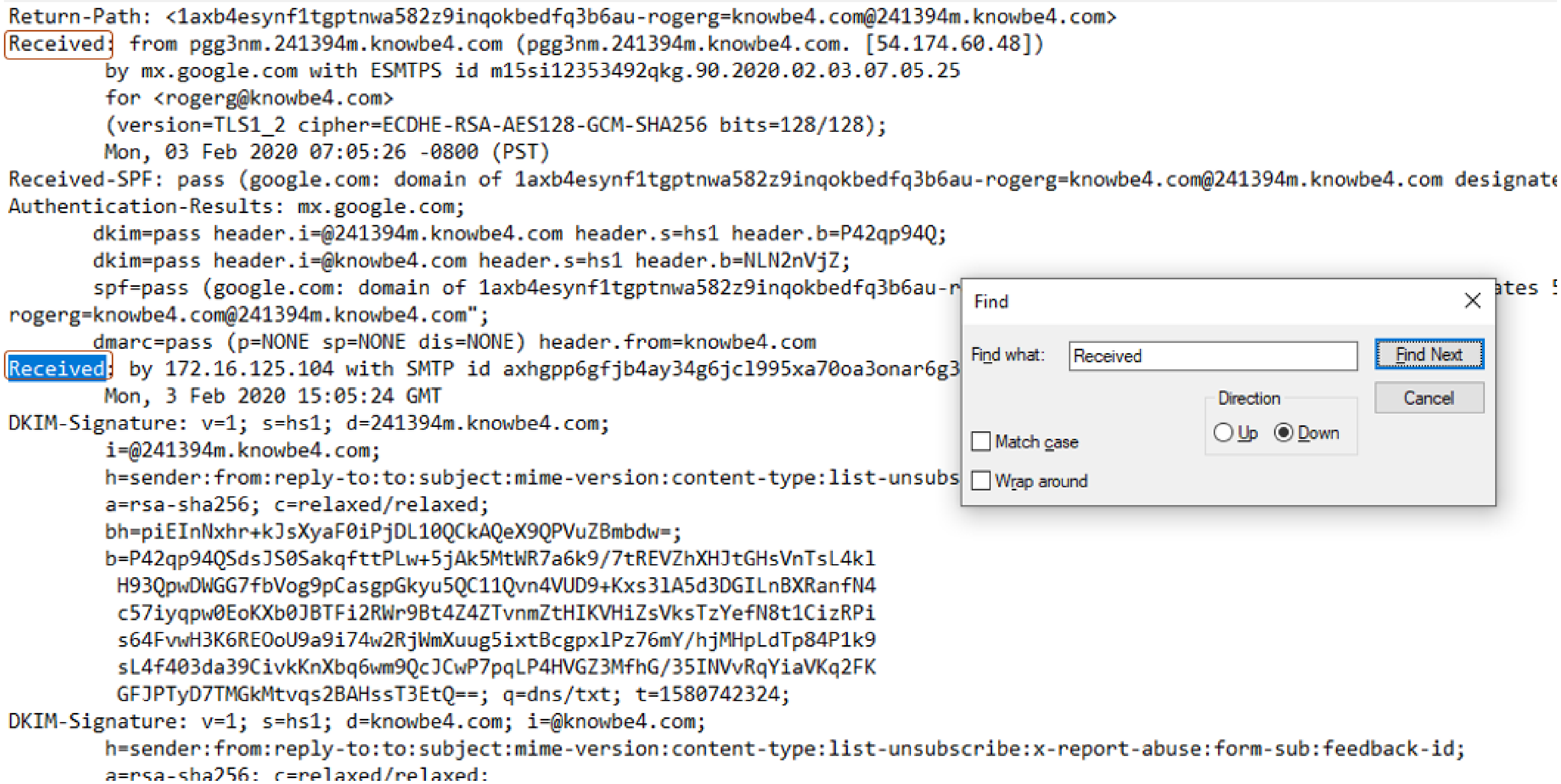
```
Authentication-Results-Original: spf=none (sender IP is )
 smtp.mailfrom=belliott@novahealth.com;
x-originating-ip: [91.207.175.167]
```

How to Investigate Email Phishes

Email Structure

- Header – Notable Fields
  - **Received** – public IP address or domain name of original sender and intermediate MTAs
    - Required field
    - Find the first one (at bottom to find the original sender
    - Different “style” per MTA
    - Remember, previous record can be modified or spoofed by intermediate MFA

How to Investigate Email Phishes



```
Return-Path: <1axb4esynf1tgptnwa582z9inqokbedfq3b6au-rogerg=knowbe4.com@241394m.knowbe4.com>
Received: from pgg3nm.241394m.knowbe4.com (pgg3nm.241394m.knowbe4.com. [54.174.60.48])
        by mx.google.com with ESMTPS id m15si12353492qkg.90.2020.02.03.07.05.25
        for <rogerg@knowbe4.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Mon, 03 Feb 2020 07:05:26 -0800 (PST)
Received-SPF: pass (google.com: domain of 1axb4esynf1tgptnwa582z9inqokbedfq3b6au-rogerg=knowbe4.com@241394m.knowbe4.com designate
Authentication-Results: mx.google.com;
       dkim=pass header.i=@241394m.knowbe4.com header.s=hs1 header.b=P42qp94Q;
       dkim=pass header.i=@knowbe4.com header.s=hs1 header.b=NLN2nVjZ;
       spf=pass (google.com: domain of 1axb4esynf1tgptnwa582z9inqokbedfq3b6au-r                                           ates 
rogerg=knowbe4.com@241394m.knowbe4.com";
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=knowbe4.com
Received: by 172.16.125.104 with SMTP id axhgpp6gfjb4ay34g6jcl995xa70oa3onar6g3
        Mon, 3 Feb 2020 15:05:24 GMT
DKIM-Signature: v=1; s=hs1; d=241394m.knowbe4.com;
        i=@241394m.knowbe4.com;
        h=sender:from:reply-to:to:subject:mime-version:content-type:list-unsubs
        a=rsa-sha256; c=relaxed/relaxed;
        bh=piEInNxhr+kJsXyaF0iPjDL10QCkAQeX9QPVuZBmbdw=;
        b=P42qp94QSdsJS0SakqfttPLw+5jAk5MtWR7a6k9/7tREVZhXHJtGHsVnTsL4kl
         H93QpwDWGG7fbVog9pCasgpGkyu5QC11Qvn4VUD9+Kxs31A5d3DGILnBXRanfN4
         c57iyqpw0EoKXb0JBTFi2RWr9Bt4Z4ZTvnmZtHIKVHiZsVksTzYefN8t1CizRPi
         s64FvwH3K6REOoU9a9i74w2RjWmXuug5ixtBcgpxlPz76mY/hjMHpLdTp84P1k9
         sL4f403da39CivkKnXbq6wm9QcJCwP7pqLP4HVGZ3MfhG/35INVvRqYiaVKq2FK
         GFJPTyD7TMGkMtvqs2BAHssT3EtQ==; q=dns/txt; t=1580742324;
DKIM-Signature: v=1; s=hs1; d=knowbe4.com; i=@knowbe4.com;
        h=sender:from:reply-to:to:subject:mime-version:content-type:list-unsubscribe:x-report-abuse:form-sub:feedback-id;
        a=rsa-sha256; c=relaxed/relaxed;
```

Find

Find what: Received

Direction ○ Up ● Down

☐ Match case

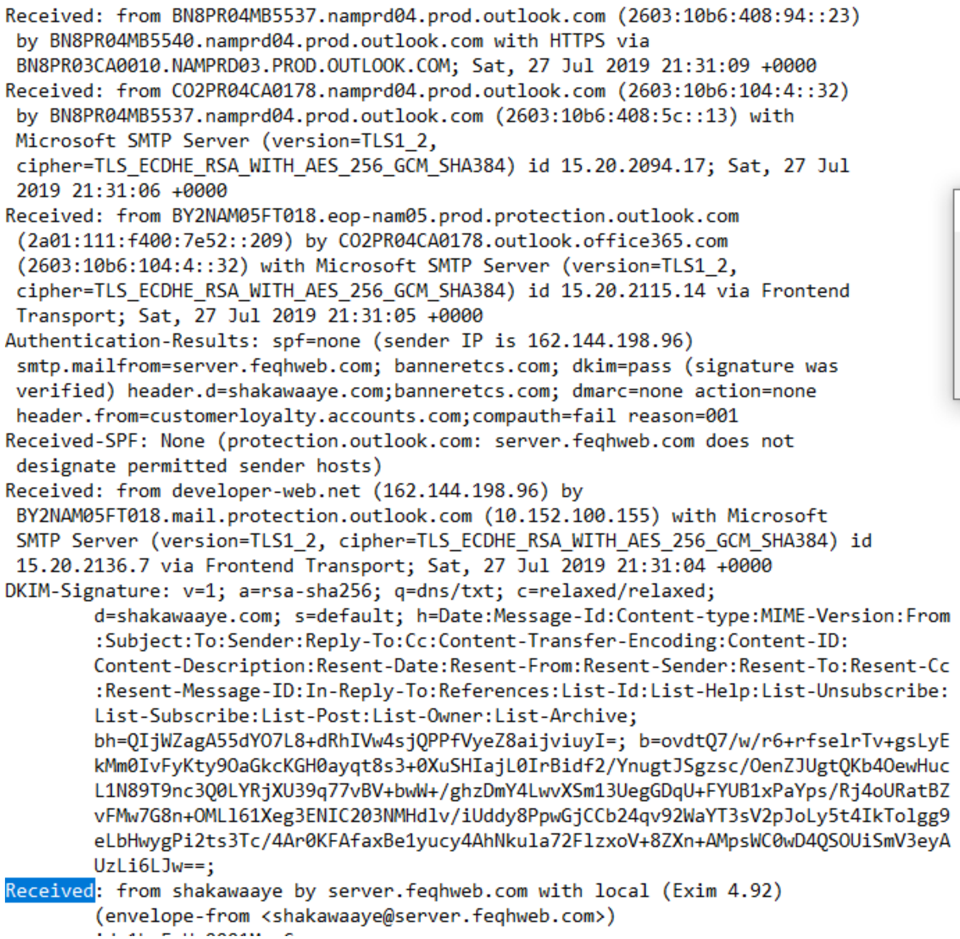
☐ Wrap around

How to Investigate Email Phishes

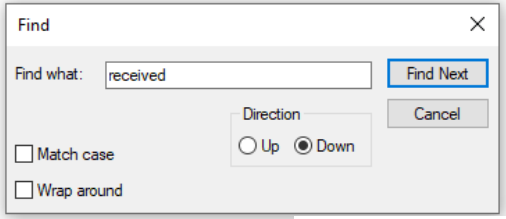
Email Structure

- Header – Notable Fields
  - **Received** – public IP address or domain name of original sender and intermediate MTAs
    - Sometimes only shows domain name and you have to use nslookup to find IP address

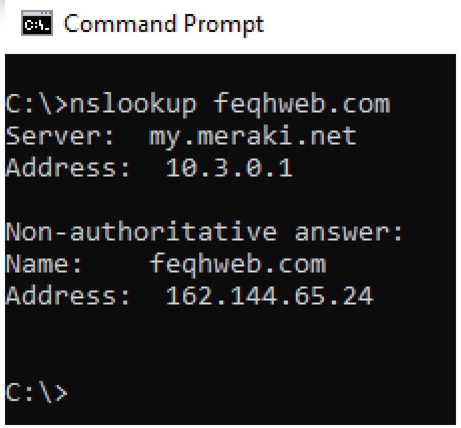
How to Investigate Email Phishes



```
Received: from BN8PR04MB5537.namprd04.prod.outlook.com (2603:10b6:408:94::23)
 by BN8PR04MB5540.namprd04.prod.outlook.com with HTTPS via
 BN8PR03CA0010.NAMPRD03.PROD.OUTLOOK.COM; Sat, 27 Jul 2019 21:31:09 +0000
Received: from CO2PR04CA0178.namprd04.prod.outlook.com (2603:10b6:104:4::32)
 by BN8PR04MB5537.namprd04.prod.outlook.com (2603:10b6:408:5c::13) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.2094.17; Sat, 27 Jul
 2019 21:31:06 +0000
Received: from BY2NAM05FT018.eop-nam05.prod.protection.outlook.com
 (2a01:111:f400:7e52::209) by CO2PR04CA0178.outlook.office365.com
 (2603:10b6:104:4::32) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.2115.14 via Frontend
 Transport; Sat, 27 Jul 2019 21:31:05 +0000
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
 designate permitted sender hosts)
Received: from developer-web.net (162.144.198.96) by
 BY2NAM05FT018.mail.protection.outlook.com (10.152.100.155) with Microsoft
 SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.2136.7 via Frontend Transport; Sat, 27 Jul 2019 21:31:04 +0000
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;
        d=shakawaaye.com; s=default; h=Date:Message-Id:Content-type:MIME-Version:From
        :Subject:To:Sender:Reply-To:Cc:Content-Transfer-Encoding:Content-ID:
        Content-Description:Resent-Date:Resent-From:Resent-Sender:Resent-To:Resent-Cc
        :Resent-Message-ID:In-Reply-To:References:List-Id:List-Help:List-Unsubscribe:
        List-Subscribe:List-Post:List-Owner:List-Archive;
        bh=QIjWZagA55dYO7L8+dRhIVw4sjQPPfVyeZ8aijviuyI=; b=ovdtQ7/w/r6+rfselrTv+gsLyE
        kMm0IvFyKty9OaGkcKGH0ayqt8s3+0XuSHIajL0IrBidf2/YnugtJSgzsc/OenZJUgtQKb4OewHuc
        L1N89T9nc3Q0LYRjXU39q77vBV+bwW+/ghzDmY4LwvXSm13UegGDqU+FYUB1xPaYps/Rj4oURatBZ
        vFMw7G8n+OMLl61Xeg3ENIC203NMHdlv/iUddy8PpwGjCCb24qv92WaYT3sV2pJoLy5t4IkTolgg9
        eLbHwygPi2ts3Tc/4Ar0KFAfaxBe1yucy4AhNkula72FlzxoV+8ZXn+AMpsWC0wD4QSOUiSmV3eyA
        UzLi6LJw==;
Received: from shakawaaye by server.feqhweb.com with local (Exim 4.92)
        (envelope-from <shakawaaye@server.feqhweb.com>)
```



Find what: received



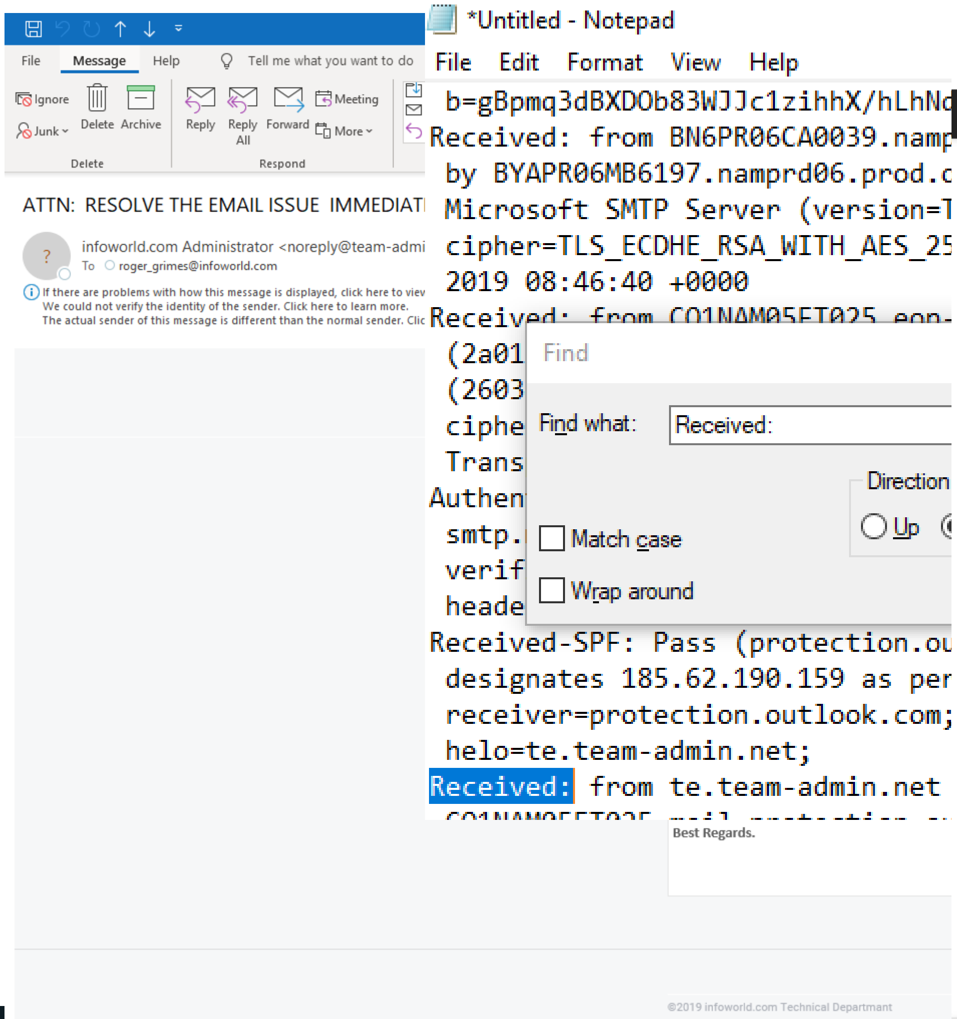
```
C:\>nslookup feqhweb.com
Server:  my.meraki.net
Address:  10.3.0.1

Non-authoritative answer:
Name:    feqhweb.com
Address:  162.144.65.24


C:\>
```

How to Investigate Email Phishes

Email Header

- Where does IP address originate from and belong to?

How to Investigate Email Phishes



ATTN: RESOLVE THE EMAIL ISSUE IMMEDIAT

infoworld.com Administrator <noreply@team-admi

To ○ roger_grimes@infoworld.com

If there are problems with how this message is displayed, click here to view
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. Clic

Best Regards.

©2019 infoworld.com Technical Department

*Untitled - Notepad

```
 b=gBpmq3dBXDOb83WJJc1zihhX/hLhNd
Received: from BN6PR06CA0039.namp
 by BYAPR06MB6197.namprd06.prod.c
 Microsoft SMTP Server (version=T
 cipher=TLS_ECDHE_RSA_WITH_AES_25
 2019 08:46:40 +0000
Received: from CO1NAM05FT025.eop-
 (2a01
 (2603
 ciphe
 Trans
Authen
 smtp.
 verif
 heade
Received-SPF: Pass (protection.ou
 designates 185.62.190.159 as per
 receiver=protection.outlook.com;
 helo=te.team-admin.net;
Received: from te.team-admin.net
```

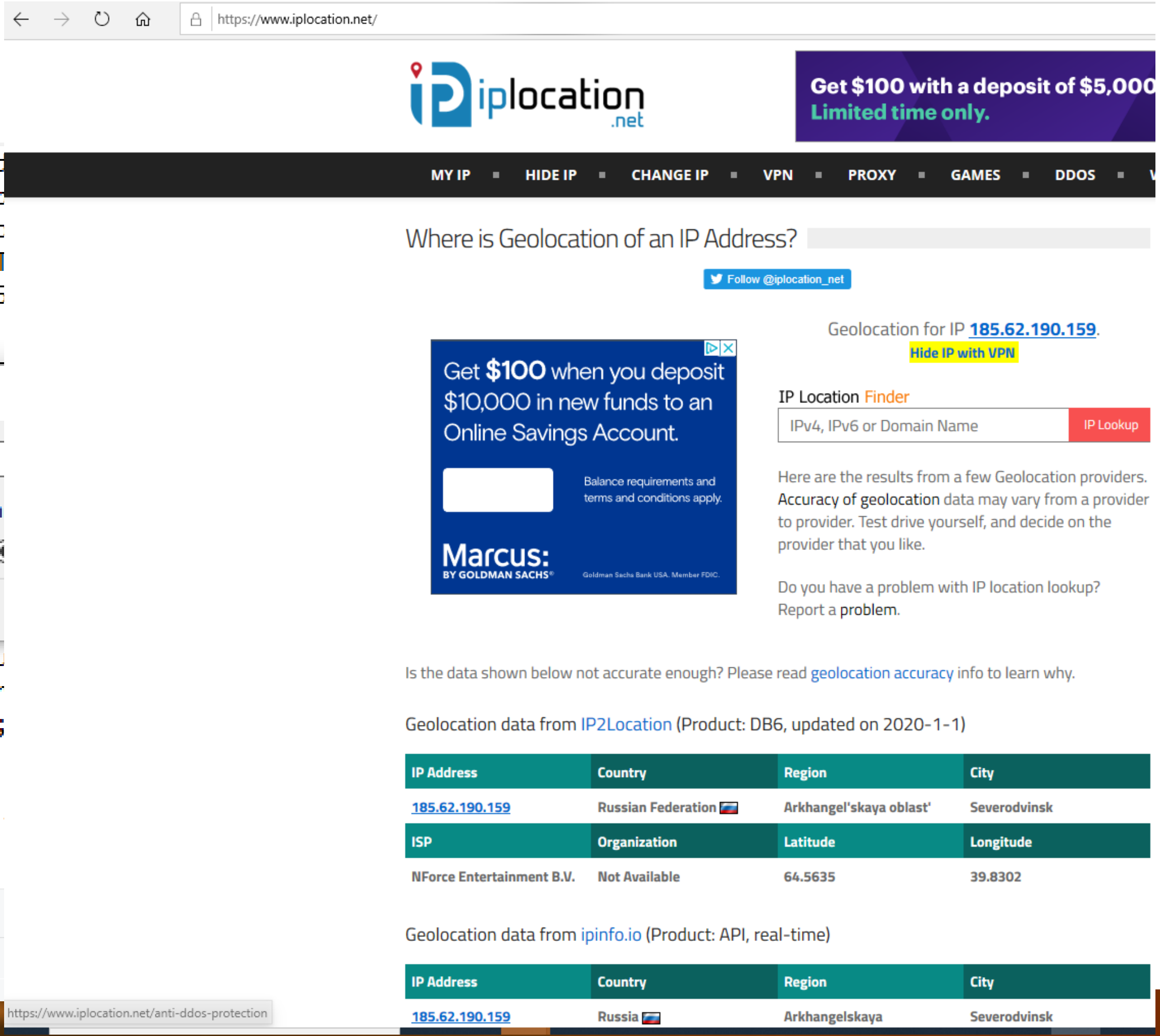
Find

Find what: Received:

Direction
○ Up ●

☐ Match case

☐ Wrap around



Where is Geolocation of an IP Address?

Geolocation for IP 185.62.190.159.

Hide IP with VPN

IP Location Finder

IPv4, IPv6 or Domain Name

Here are the results from a few Geolocation providers. Accuracy of geolocation data may vary from a provider to provider. Test drive yourself, and decide on the provider that you like.

Do you have a problem with IP location lookup? Report a problem.

Is the data shown below not accurate enough? Please read geolocation accuracy info to learn why.

Geolocation data from IP2Location (Product: DB6, updated on 2020-1-1)

IP Address	Country	Region	City
185.62.190.159	Russian Federation	Arkhangel'skaya oblast'	Severodvinsk
ISP	**Organization**	**Latitude**	**Longitude**
NForce Entertainment B.V.	Not Available	64.5635	39.8302

Geolocation data from ipinfo.io (Product: API, real-time)

IP Address	Country	Region	City
185.62.190.159	Russia	Arkhangelskaya	Severodvinsk

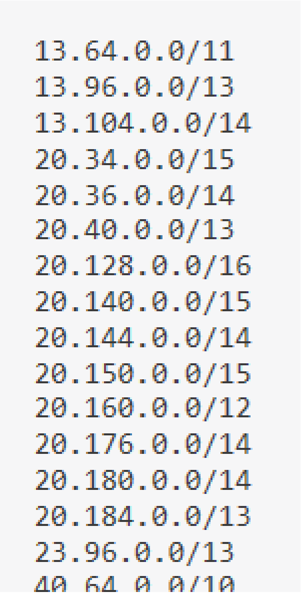
KnowBe4
Human error. Conquered.

How to Investigate Email Phishes

Email Header

Does IP address of MTA belong to service it claims to be from?

- For example:
- Microsoft public IP addresses for email
  - https://www.microsoft.com/en-us/download/details.aspx?id=53602



```
13.64.0.0/11
13.96.0.0/13
13.104.0.0/14
20.34.0.0/15
20.36.0.0/14
20.40.0.0/13
20.128.0.0/16
20.140.0.0/15
20.144.0.0/14
20.150.0.0/15
20.160.0.0/12
20.176.0.0/14
20.180.0.0/14
20.184.0.0/13
23.96.0.0/13
40.64.0.0/10
```

Partial list

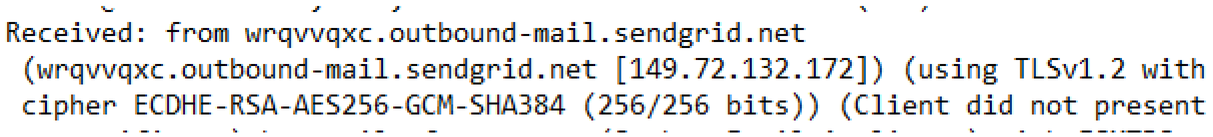
How to Investigate Email Phishes

Origination IP Address

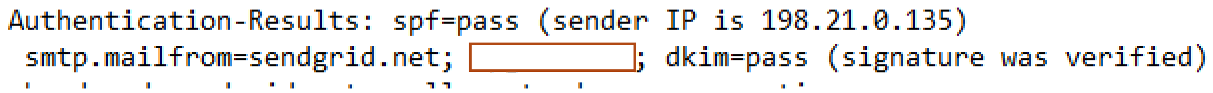
Possibly malicious phish if MTA is a public SMTP SAS service from supposedly big brand name company

Examples

- Smtp.com
- Sendgrid.net
- Constantcontact.com
- Gmail
- 0365



```
Received: from wrqvvqxc.outbound-mail.sendgrid.net
 (wrqvvqxc.outbound-mail.sendgrid.net [149.72.132.172]) (using TLSv1.2 with
 cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)) (Client did not present
```



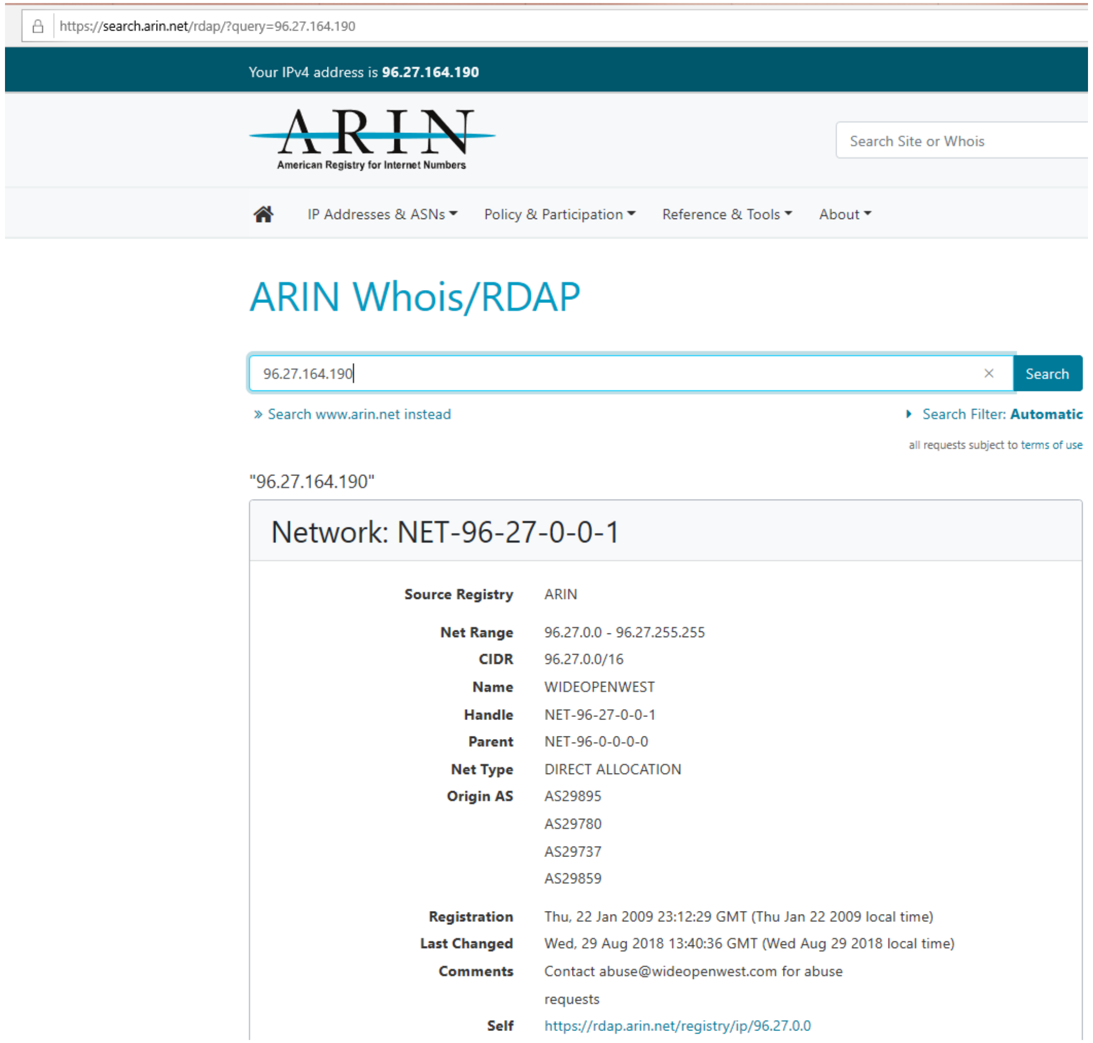
```
Authentication-Results: spf=pass (sender IP is 198.21.0.135)
 smtp.mailfrom=sendgrid.net; [redacted]; dkim=pass (signature was verified)
```

How to Investigate Email Phishes

Research

- Where does IP address originate from and belong to?

How to Investigate Email Phishes



https://search.arin.net/rdap/?query=96.27.164.190
Your IPv4 address is 96.27.164.190
ARIN
American Registry for Internet Numbers
Search Site or Whois
IP Addresses & ASNs
Policy & Participation
Reference & Tools
About

ARIN Whois/RDAP

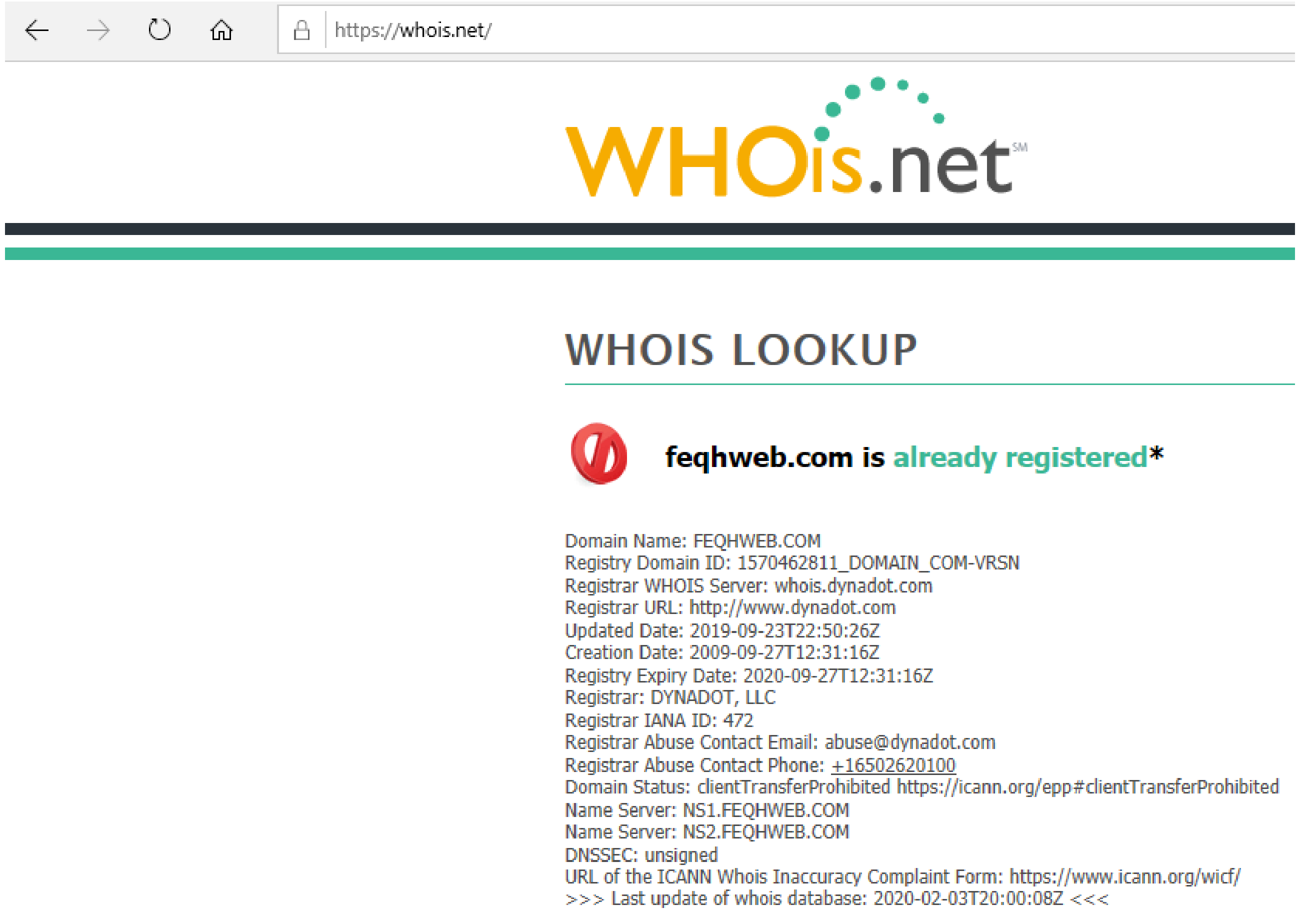
96.27.164.190
Search
» Search www.arin.net instead
Search Filter: Automatic
all requests subject to terms of use

"96.27.164.190"

Network: NET-96-27-0-0-1

Source Registry	ARIN
Net Range	96.27.0.0 - 96.27.255.255
CIDR	96.27.0.0/16
Name	WIDEOPENWEST
Handle	NET-96-27-0-0-1
Parent	NET-96-0-0-0-0
Net Type	DIRECT ALLOCATION
Origin AS	AS29895 AS29780 AS29737 AS29859
Registration	Thu, 22 Jan 2009 23:12:29 GMT (Thu Jan 22 2009 local time)
Last Changed	Wed, 29 Aug 2018 13:40:36 GMT (Wed Aug 29 2018 local time)
Comments	Contact abuse@wideopenwest.com for abuse requests
Self	https://rdap.arin.net/registry/ip/96.27.0.0

How to Investigate Email Phishes



WHOIS LOOKUP

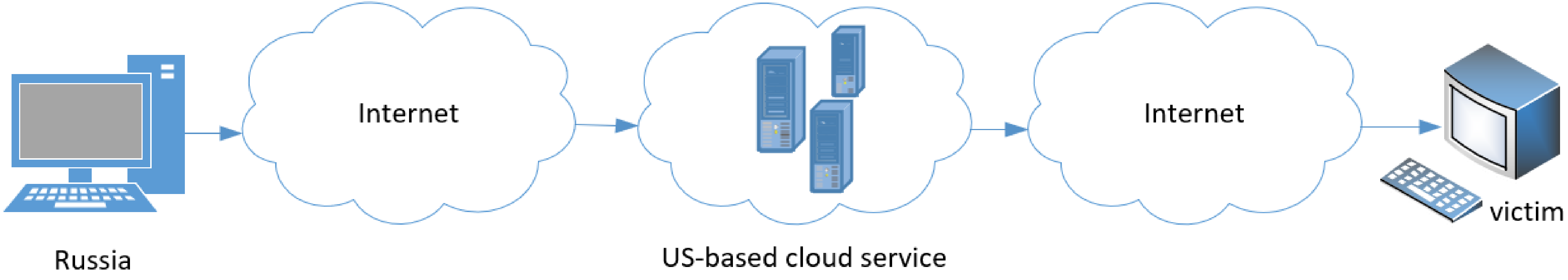
feqhweb.com is already registered*

```
Domain Name: FEQHWEB.COM
Registry Domain ID: 1570462811_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.dynadot.com
Registrar URL: http://www.dynadot.com
Updated Date: 2019-09-23T22:50:26Z
Creation Date: 2009-09-27T12:31:16Z
Registry Expiry Date: 2020-09-27T12:31:16Z
Registrar: DYNADOT, LLC
Registrar IANA ID: 472
Registrar Abuse Contact Email: abuse@dynadot.com
Registrar Abuse Contact Phone: +16502620100
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS1.FEQHWEB.COM
Name Server: NS2.FEQHWEB.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-02-03T20:00:08Z <<<
```

How to Investigate Email Phishes

Origination IP Address

- Keep **location attribution redirection** tactics in mind



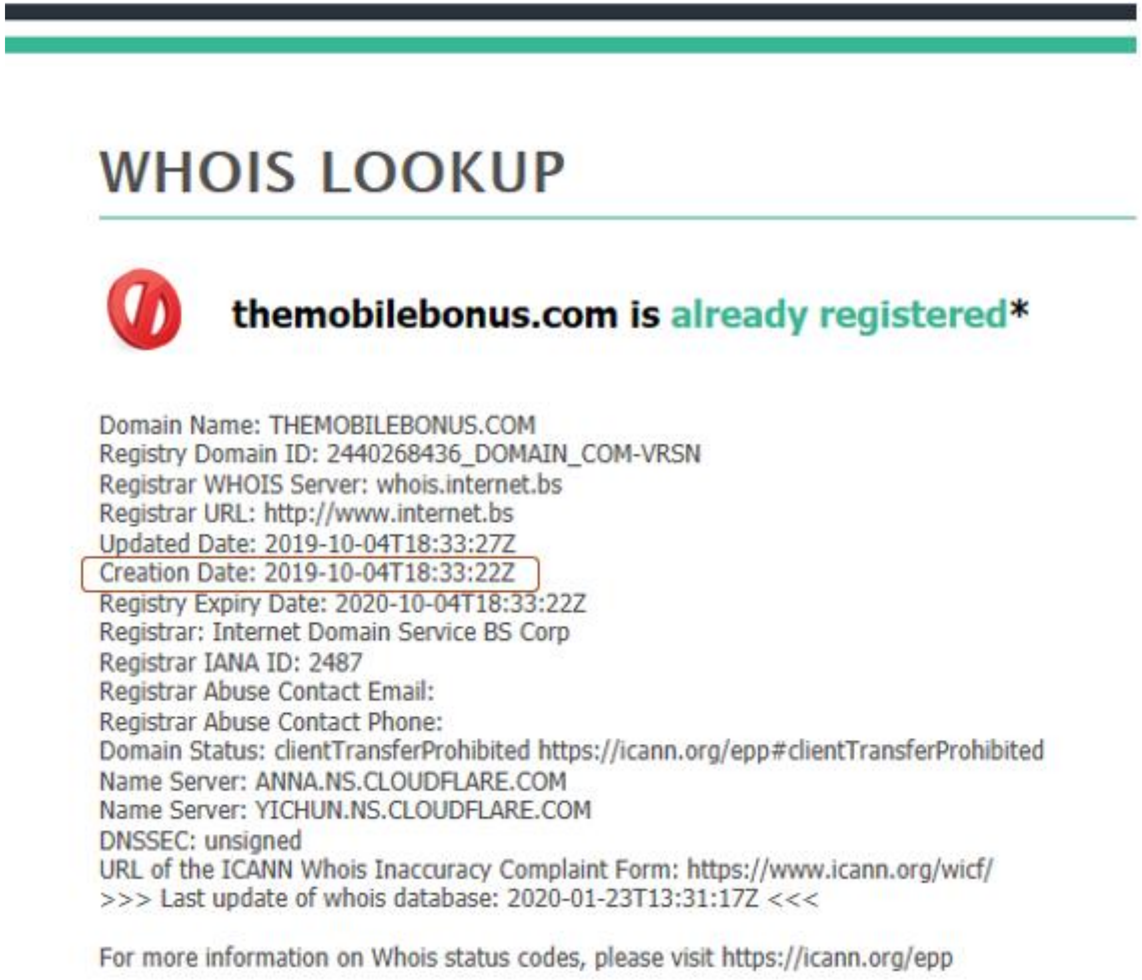
Originating IP would be US-based

How to Investigate Email Phishes

Research

- How old is domain registration creation?
- Younger is more risky

How to Investigate Email Phishes



WHOIS LOOKUP

themobilebonus.com is already registered*

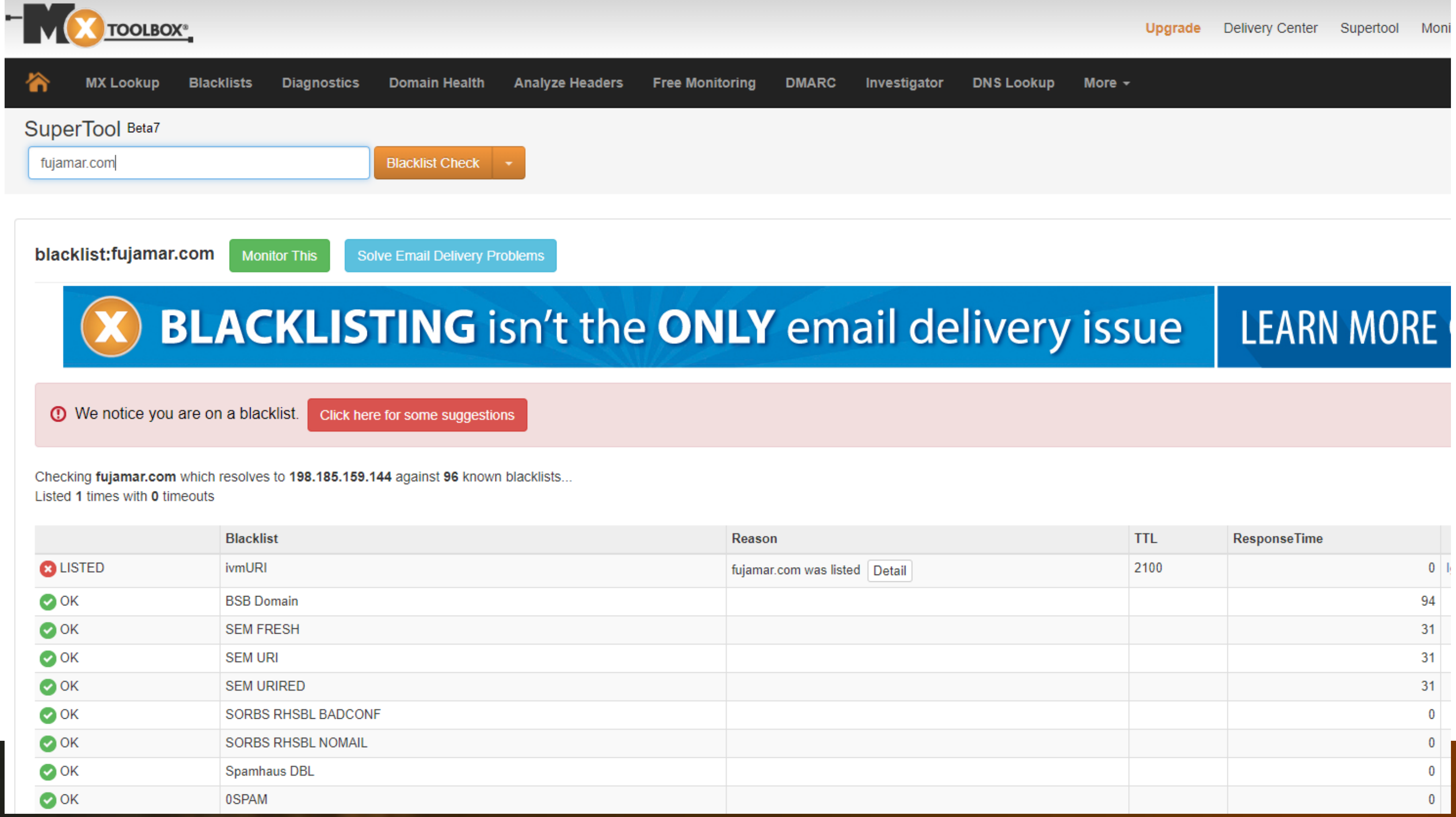
```
Domain Name: THEMOBILEBONUS.COM
Registry Domain ID: 2440268436_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.internet.bs
Registrar URL: http://www.internet.bs
Updated Date: 2019-10-04T18:33:27Z
Creation Date: 2019-10-04T18:33:22Z
Registry Expiry Date: 2020-10-04T18:33:22Z
Registrar: Internet Domain Service BS Corp
Registrar IANA ID: 2487
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: ANNA.NS.CLOUDFLARE.COM
Name Server: YICHUN.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-01-23T13:31:17Z <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

Example was less than 4 months old at time of looked up and referred to pestware domain

How to Investigate Email Phishes

Research

- Is domain on a blacklist?



blacklist:fujamar.com

We notice you are on a blacklist.

Checking **fujamar.com** which resolves to **198.185.159.144** against **96** known blacklists...
Listed **1** times with **0** timeouts

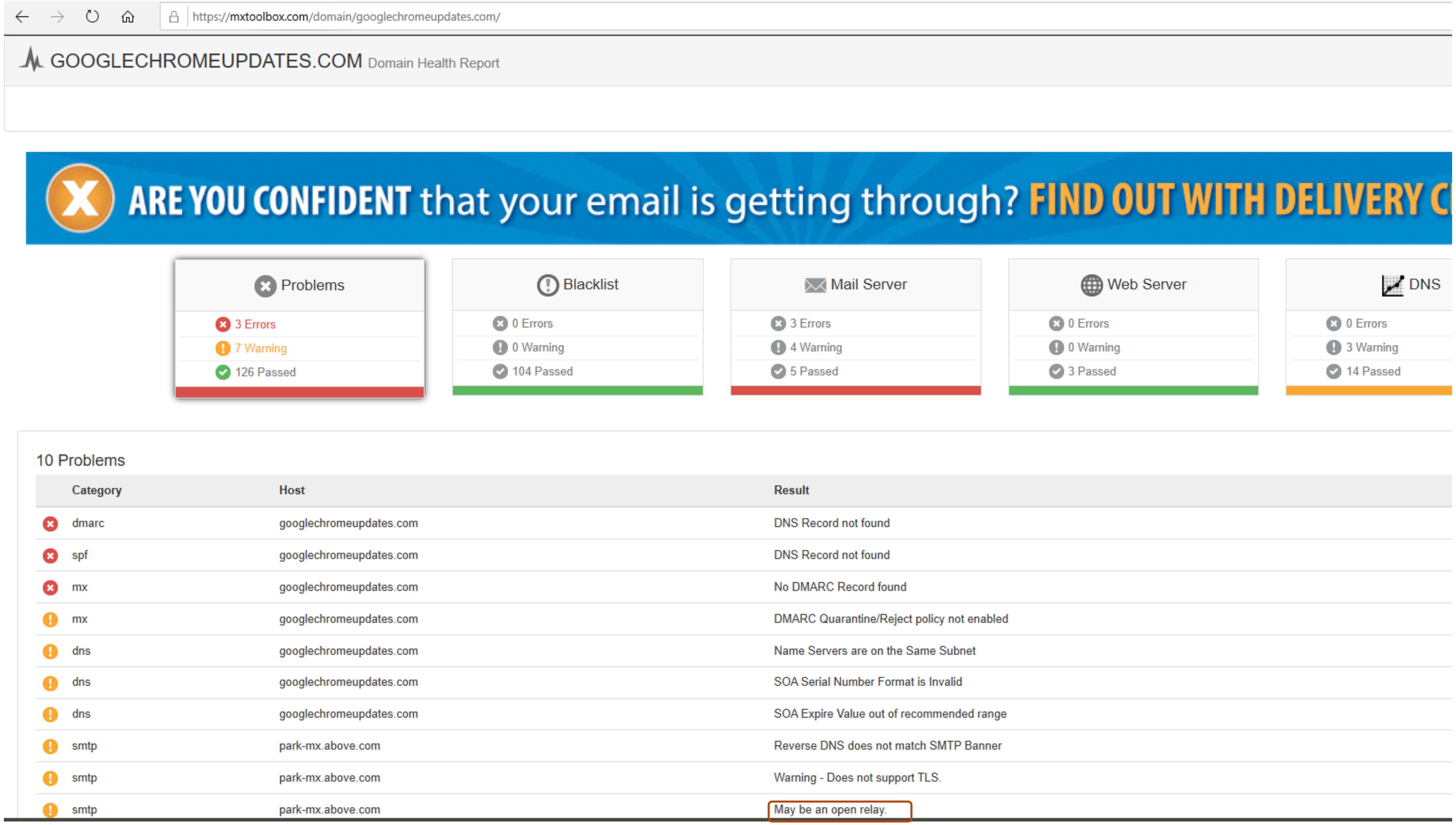
	Blacklist	Reason	TTL	ResponseTime
LISTED	ivmURI	fujamar.com was listed Detail	2100	0
OK	BSB Domain			94
OK	SEM FRESH			31
OK	SEM URI			31
OK	SEM URIRED			31
OK	SORBS RHSBL BADCONF			0
OK	SORBS RHSBL NOMAIL			0
OK	Spamhaus DBL			0
OK	0SPAM			0

How to Investigate Email Phishes

Research

- Is domain healthy?

How to Investigate Email Phishes



https://mxtoolbox.com/domain/googlechromeupdates.com/

GOOGLECHROMEUPDATES.COM Domain Health Report

ARE YOU CONFIDENT that your email is getting through? FIND OUT WITH DELIVERY C

Problems	Blacklist	Mail Server	Web Server	DNS
✗ 3 Errors	✗ 0 Errors	✗ 3 Errors	✗ 0 Errors	✗ 0 Errors
! 7 Warning	! 0 Warning	! 4 Warning	! 0 Warning	! 3 Warning
✓ 126 Passed	✓ 104 Passed	✓ 5 Passed	✓ 3 Passed	✓ 14 Passed

10 Problems

	Category	Host	Result
✗	dmarc	googlechromeupdates.com	DNS Record not found
✗	spf	googlechromeupdates.com	DNS Record not found
✗	mx	googlechromeupdates.com	No DMARC Record found
!	mx	googlechromeupdates.com	DMARC Quarantine/Reject policy not enabled
!	dns	googlechromeupdates.com	Name Servers are on the Same Subnet
!	dns	googlechromeupdates.com	SOA Serial Number Format is Invalid
!	dns	googlechromeupdates.com	SOA Expire Value out of recommended range
!	smtp	park-mx.above.com	Reverse DNS does not match SMTP Banner
!	smtp	park-mx.above.com	Warning - Does not support TLS.
!	smtp	park-mx.above.com	May be an open relay.

How to Investigate Email Phishes

Research

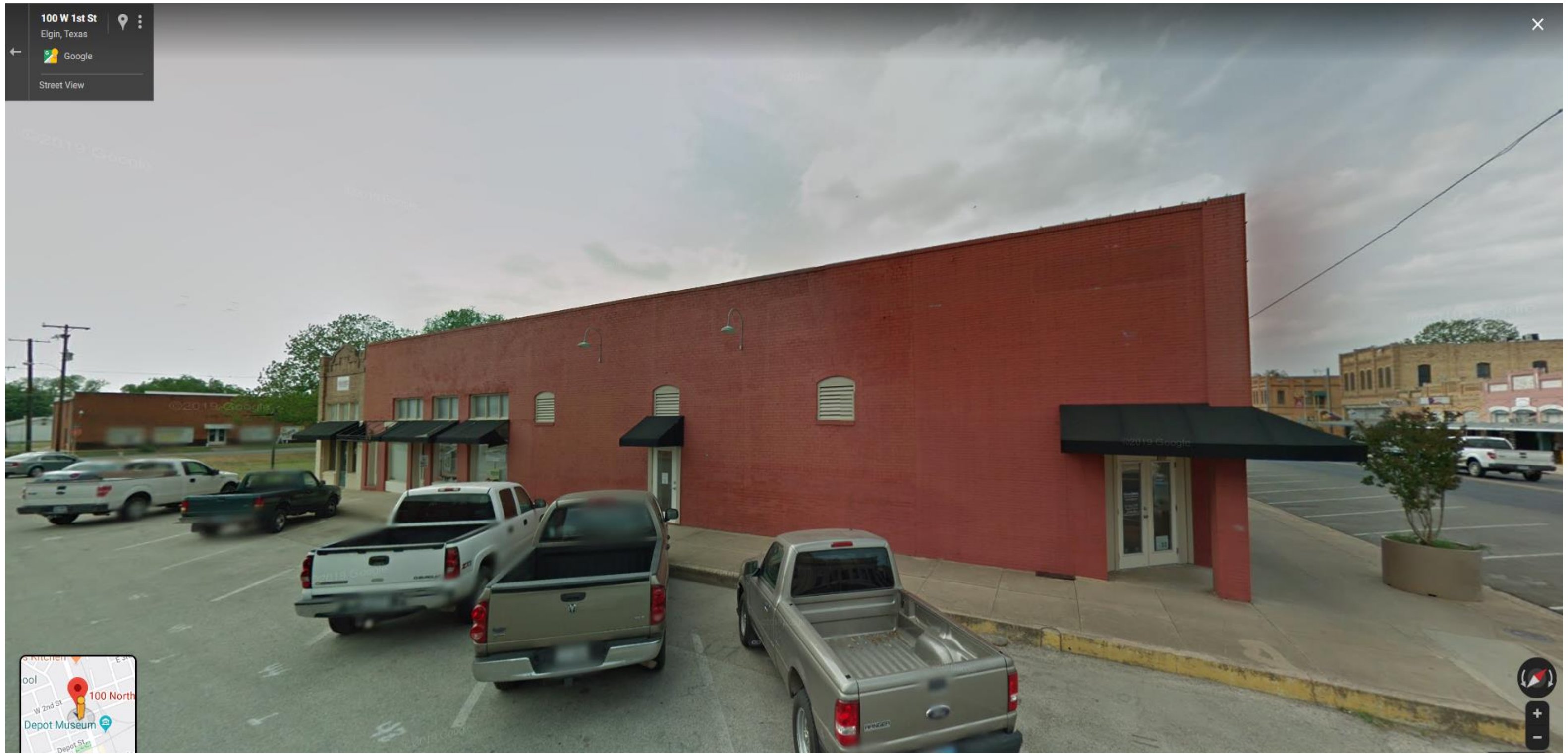
Physical location of domain business?

- Use Google Maps street view
- Does it look like the right business location for the claimed business
- Do you see signs of the same business at the physical location?

How to Investigate Email Phishes

Research

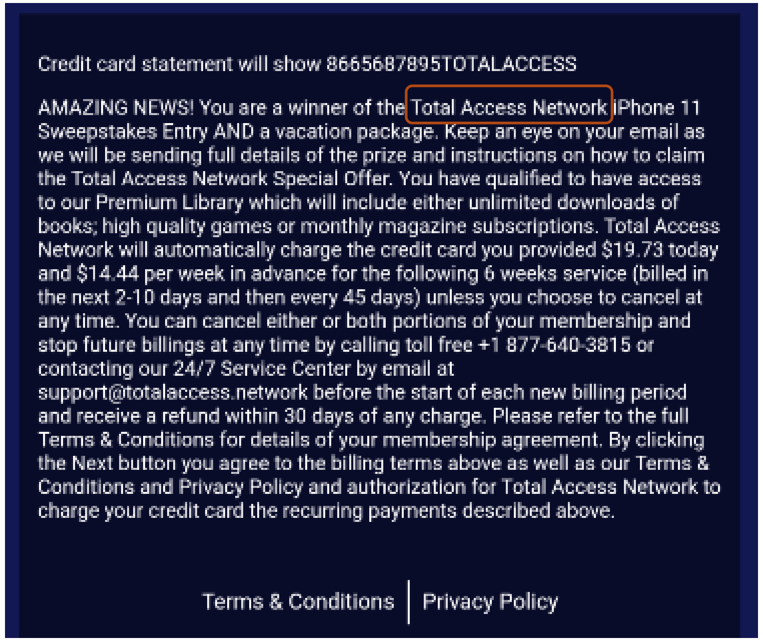
Physical location of domain business?



How to Investigate Email Phishes

Research

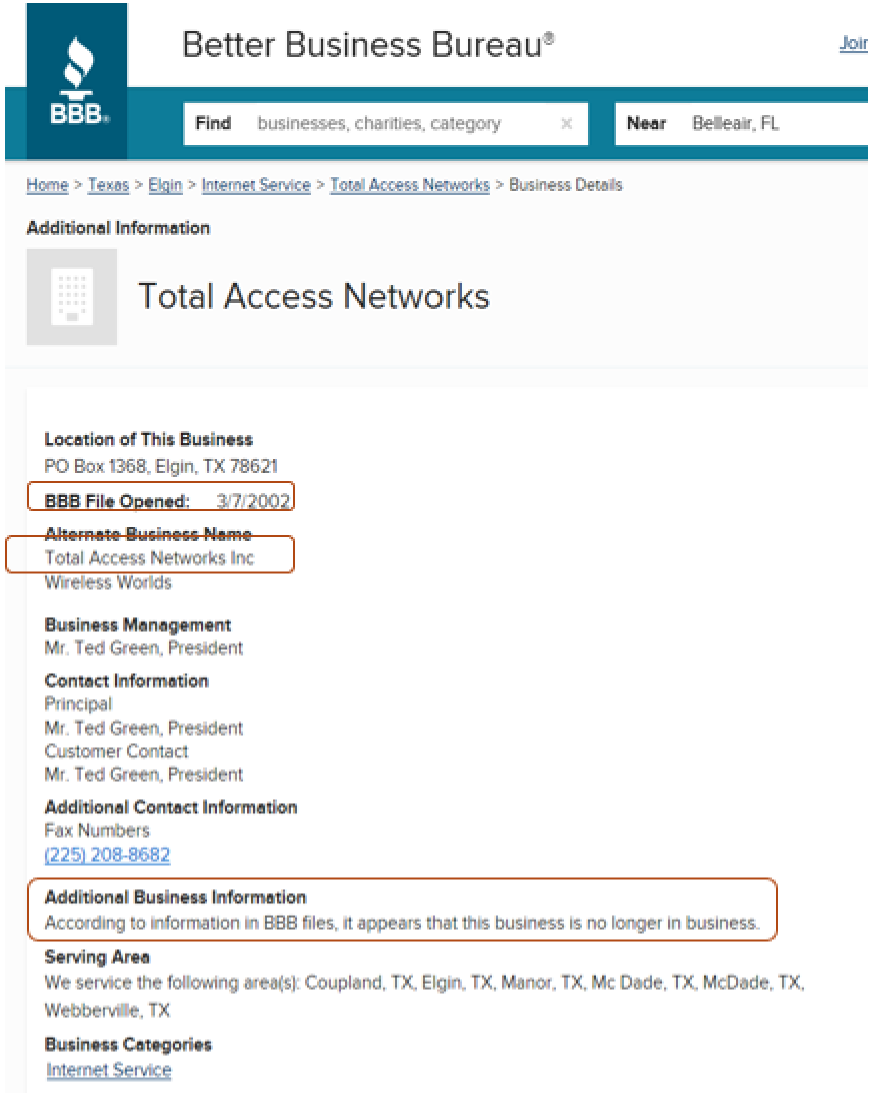
- Better Business Bureau



Credit card statement will show 8665687895TOTALACCESS

AMAZING NEWS! You are a winner of the Total Access Network iPhone 11 Sweepstakes Entry AND a vacation package. Keep an eye on your email as we will be sending full details of the prize and instructions on how to claim the Total Access Network Special Offer. You have qualified to have access to our Premium Library which will include either unlimited downloads of books; high quality games or monthly magazine subscriptions. Total Access Network will automatically charge the credit card you provided $19.73 today and $14.44 per week in advance for the following 6 weeks service (billed in the next 2-10 days and then every 45 days) unless you choose to cancel at any time. You can cancel either or both portions of your membership and stop future billings at any time by calling toll free +1 877-640-3815 or contacting our 24/7 Service Center by email at support@totalaccess.network before the start of each new billing period and receive a refund within 30 days of any charge. Please refer to the full Terms & Conditions for details of your membership agreement. By clicking the Next button you agree to the billing terms above as well as our Terms & Conditions and Privacy Policy and authorization for Total Access Network to charge your credit card the recurring payments described above.

Terms & Conditions | Privacy Policy



BBB
Better Business Bureau®
Joir
Find businesses, charities, category
Near Belleair, FL

Home > Texas > Elgin > Internet Service > Total Access Networks > Business Details

Additional Information

Total Access Networks

Location of This Business
PO Box 1368, Elgin, TX 78621

BBB File Opened: 3/7/2002

Alternate Business Name
Total Access Networks Inc
Wireless Worlds

Business Management
Mr. Ted Green, President

Contact Information
Principal
Mr. Ted Green, President
Customer Contact
Mr. Ted Green, President

Additional Contact Information
Fax Numbers
(225) 208-8682

Additional Business Information
According to information in BBB files, it appears that this business is no longer in business.

Serving Area
We service the following area(s): Coupland, TX, Elgin, TX, Manor, TX, Mc Dade, TX, McDade, TX, Webberville, TX

Business Categories
Internet Service

How to Investigate Email Phishes

Is it from the domain it says it is from?

How to Investigate Email Phishes

Global Phishing Protection Standards

- **Sender Policy Framework (SPF)**
- **Domain Keys Identified Mail (DKIM)**
- SPF and DKIM 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

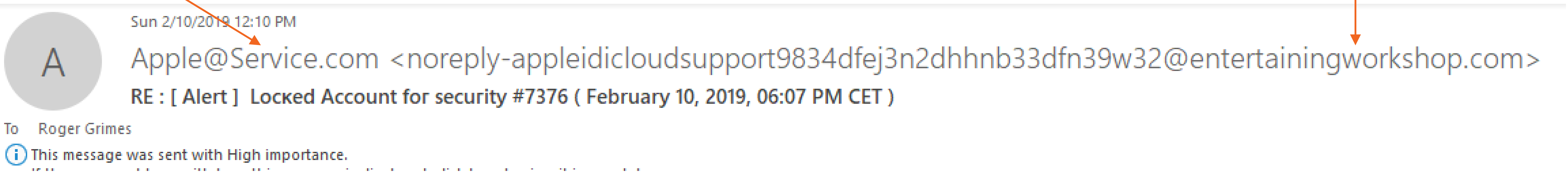
How to Investigate Email Phishes

SPF

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

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

5322.DISPLAY
FROM domain



Sun 2/10/2019 12:10 PM

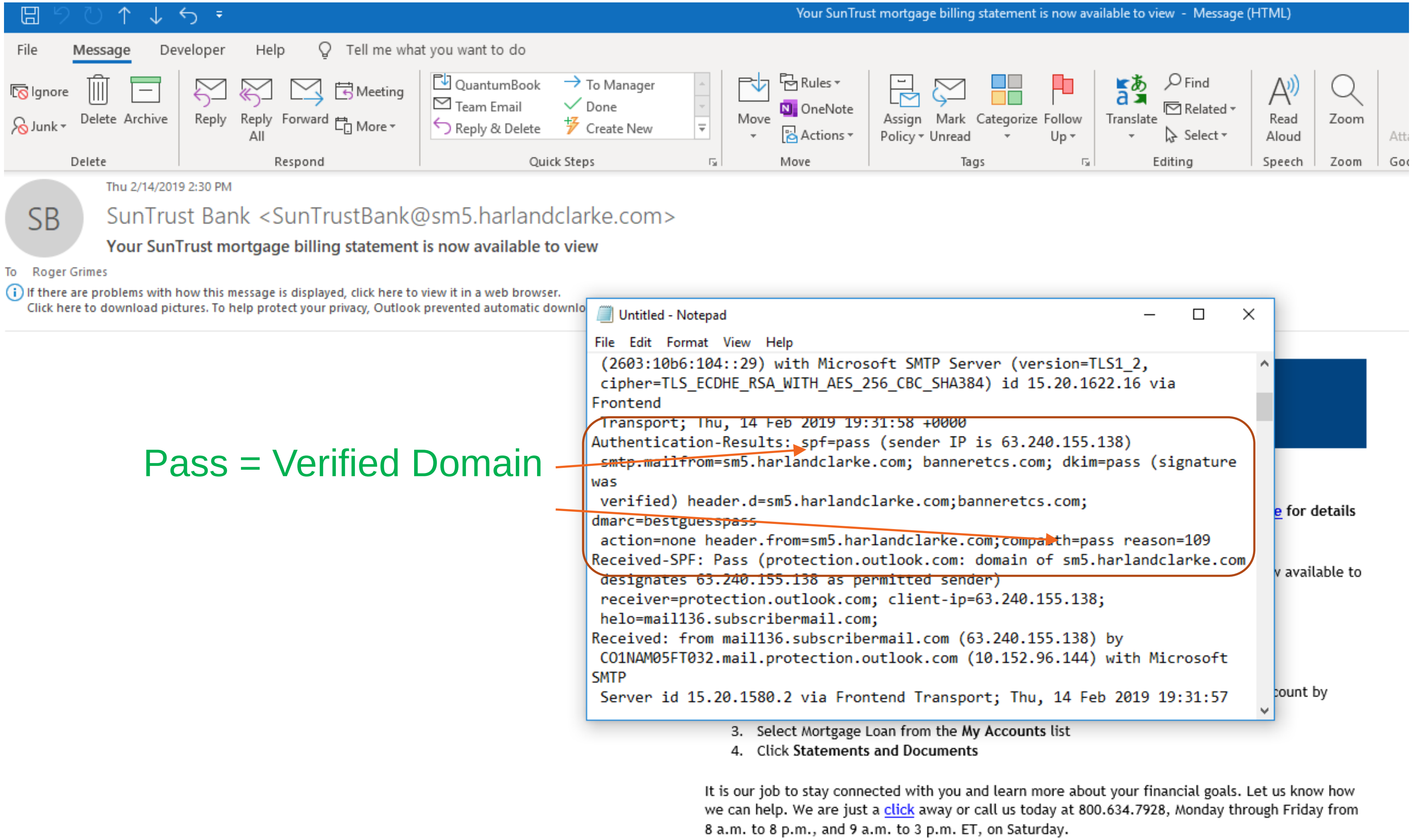
Apple@Service.com <noreply-appleidicloudsupport9834dfej3n2dhhnb33dfn39w32@entertainingworkshop.com>

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 Passes



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

```
 (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

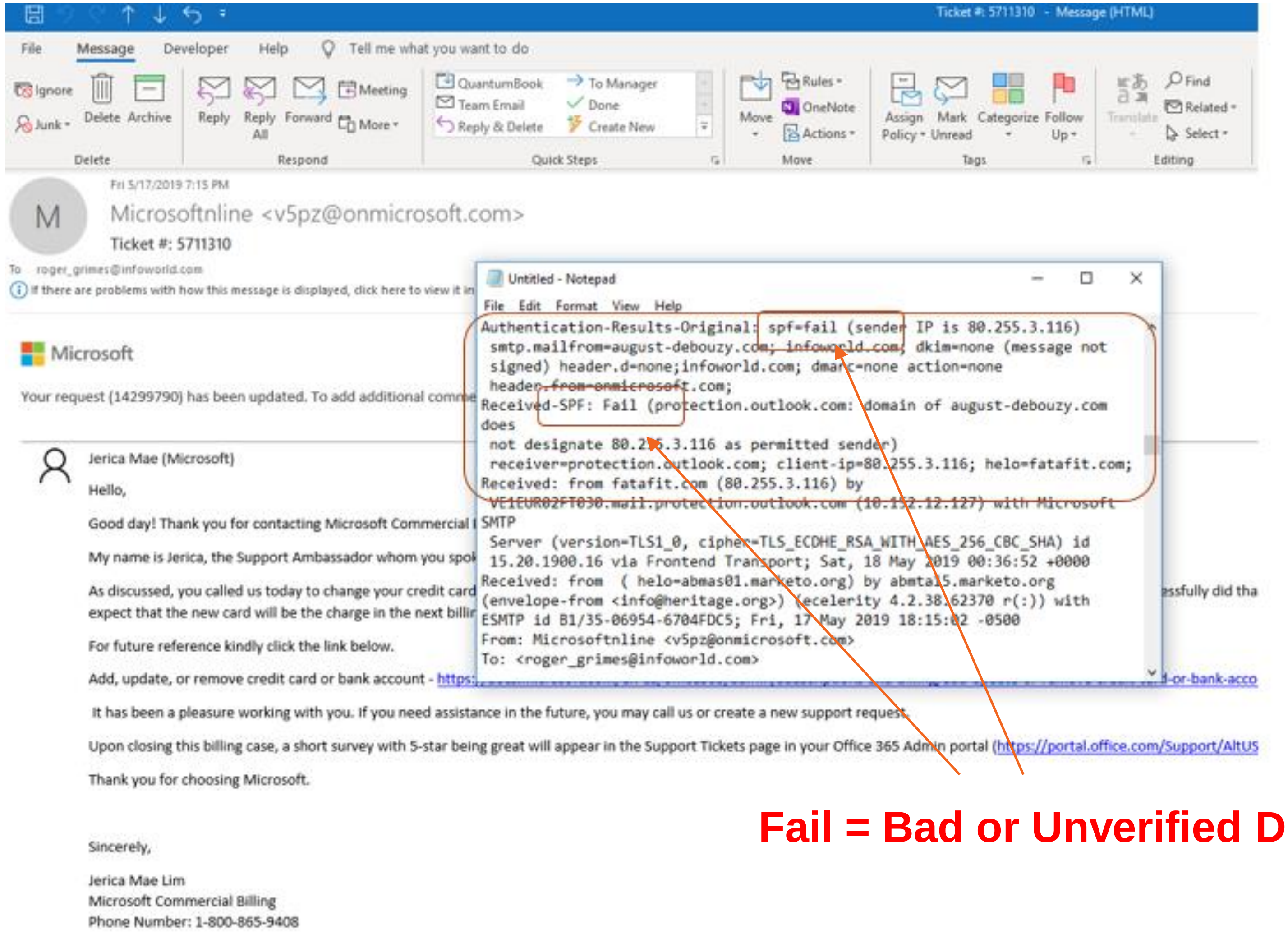
v available to

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.

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

My name is Jerica, the Support Ambassador whom you spok

As discussed, you called us today to change your credit card ... essfully 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

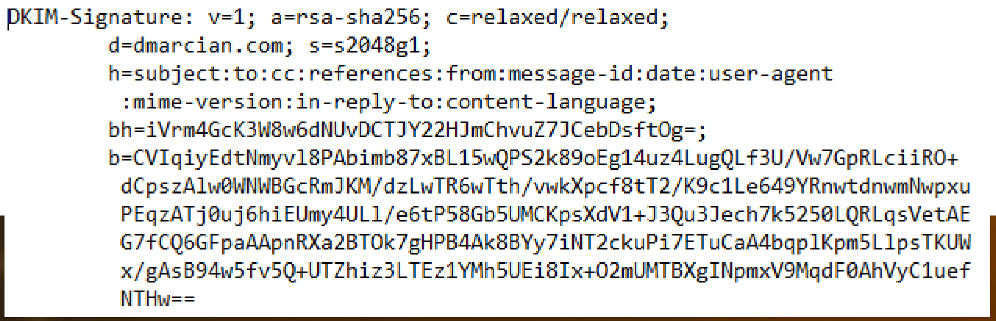
```
Authentication-Results-Original: spf=fail (sender IP is 80.255.3.116)
 smtp.mailfrom=august-debouzy.com; infoworld.com; dkim=none (message not
 signed) header.d=none;infoworld.com; dmarc=none action=none
 header.from=onmicrosoft.com;
Received-SPF: Fail (protection.outlook.com: domain of august-debouzy.com
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

How to Investigate Email Phishes

DKIM

- **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).

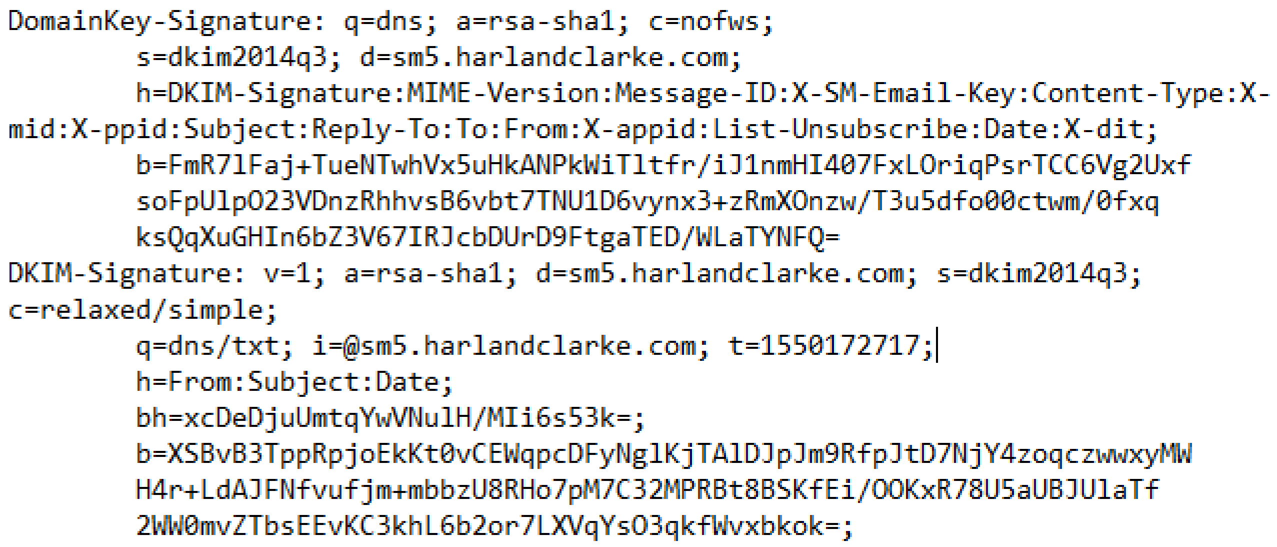


```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=dmarcian.com; s=s2048g1;
        h=subject:to:cc:references:from:message-id:date:user-agent
         :mime-version:in-reply-to:content-language;
        bh=iVrm4GcK3W8w6dNUvDCTJY22HJmChvuZ7JCebDsftOg=;
        b=CVIqiyEdtNmyvl8PAbimb87xBL15wQPS2k89oEg14uz4LugQLf3U/Vw7GpRLciiRO+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

DKIM

Domain Keys Identified Mail (DKIM)

Example DKIM Signature in Email Header

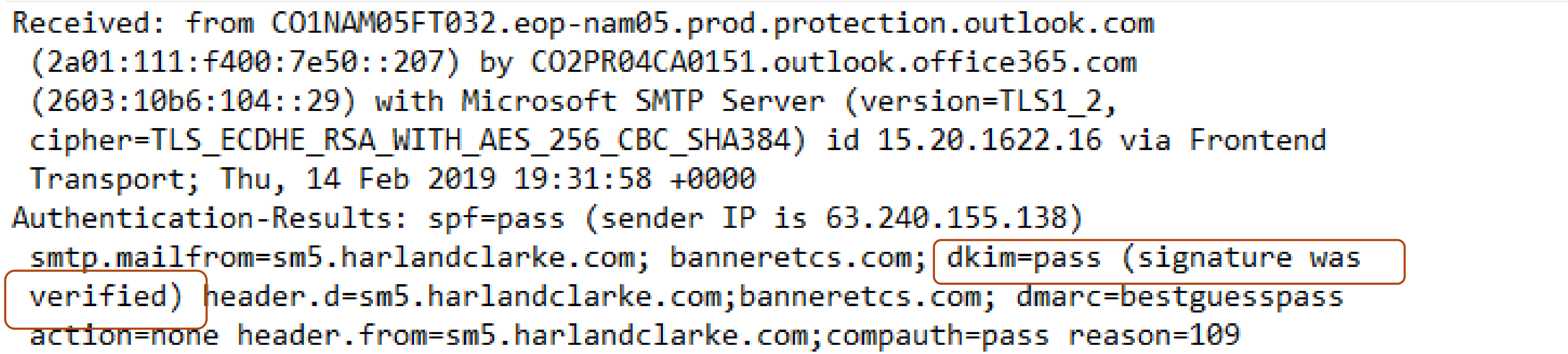


```
DomainKey-Signature: q=dns; a=rsa-sha1; c=nofws;
        s=dkim2014q3; d=sm5.harlandclarke.com;
        h=DKIM-Signature:MIME-Version:Message-ID:X-SM-Email-Key:Content-Type:X-
mid:X-ppid:Subject:Reply-To:To:From:X-appid:List-Unsubscribe:Date:X-dit;
        b=FmR71Faj+TueNTwhVx5uHkANPkWiTltfr/iJ1nmHI407FxLOriqPsrTCC6Vg2Uxf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

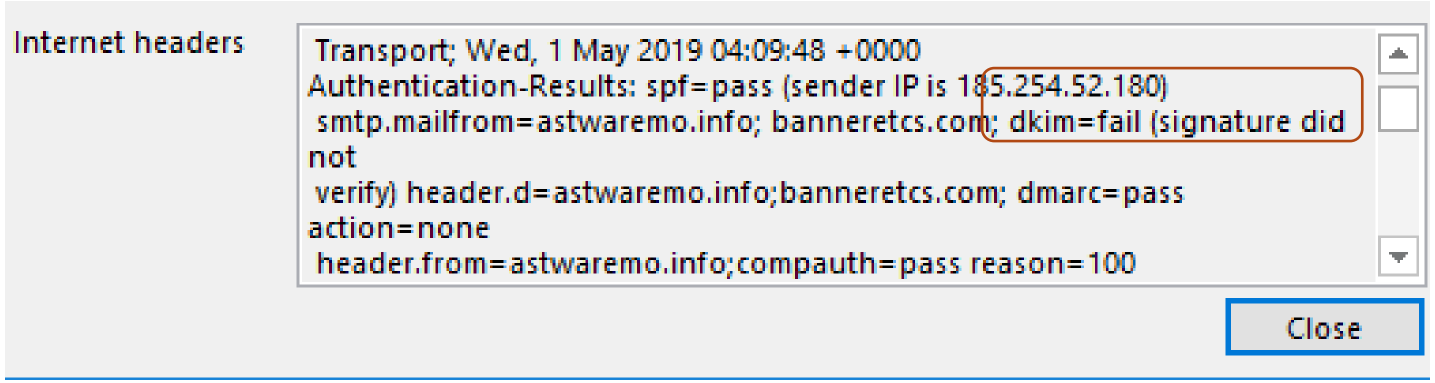


```
Received: from CO1NAM05FT032.eop-nam05.prod.protection.outlook.com
 (2a01:111:f400:7e50::207) by CO2PR04CA0151.outlook.office365.com
 (2603:10b6:104::29) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384) id 15.20.1622.16 via Frontend
 Transport; Thu, 14 Feb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



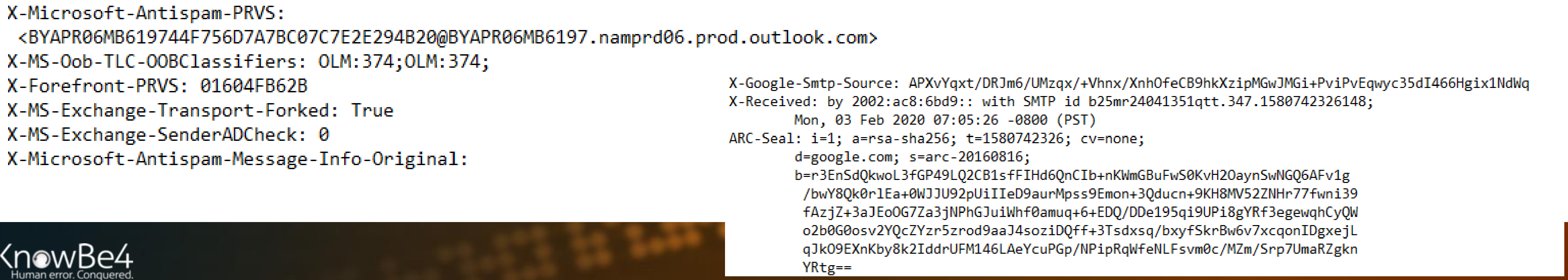
```
 Transport; Wed, 1 May 2019 04:09:48 +0000
Authentication-Results: spf=pass (sender IP is 185.254.52.180)
 smtp.mailfrom=astwaremo.info; banneretcs.com; dkim=fail (signature did
not
 verify) header.d=astwaremo.info;banneretcs.com; dmarc=pass
action=none
 header.from=astwaremo.info;compauth=pass reason=100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

How to Investigate Email Phishes

Email Header

X- headers

- X stands for “extra” or “experimental”
- Can be added by an MTA
- Can be used to store useful information or to track users



```
X-Microsoft-Antispam-PRVS:
 <BYAPR06MB619744F756D7A7BC07C7E2E294B20@BYAPR06MB6197.namprd06.prod.outlook.com>
X-MS-Oob-TLC-OOBClassifiers: OLM:374;OLM:374;
X-Forefront-PRVS: 01604FB62B
X-MS-Exchange-Transport-Forked: True
X-MS-Exchange-SenderADCheck: 0
X-Microsoft-Antispam-Message-Info-Original:
```

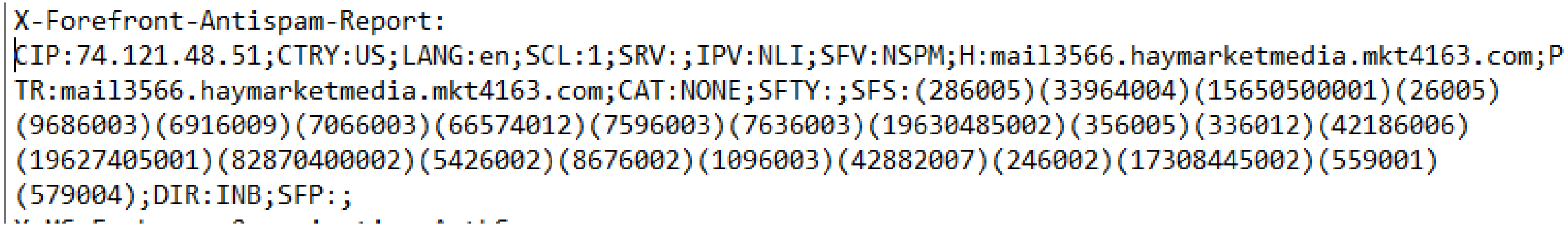
```
X-Google-Smtp-Source: APXvYqxt/DRJm6/UMzqx/+Vhnx/XnhOfeCB9hkXzipMGwJMGi+PviPvEqwyc35dI466Hgix1NdWq
X-Received: by 2002:ac8:6bd9:: with SMTP id b25mr24041351qtt.347.1580742326148;
        Mon, 03 Feb 2020 07:05:26 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1580742326; cv=none;
        d=google.com; s=arc-20160816;
        b=r3EnSdQkwoL3fGP49LQ2CB1sfFIHd6QnCIb+nKWmGBuFwS0KvH2OaynSwNGQ6AFv1g
         /bwY8Qk0rlEa+0WJJU92pUiIIeD9aurMpss9Emon+3Qducn+9KH8MV52ZNHr77fwni39
         fAzjZ+3aJEoOG7Za3jNPhGJuiWhf0amuq+6+EDQ/DDe195qi9UPi8gYRf3egewqhCyQW
         o2b0G0osv2YQcZYzr5zrod9aaJ4soziDQff+3Tsdxsq/bxyfSkrBw6v7xcqonIDgxejL
         qJkO9EXnKby8k2IddrUFM146LAeYcuPGp/NPipRqWfeNLFsvm0c/MZm/Srp7UmaRZgkn
         YRtg==
```

How to Investigate Email Phishes

Email Header – X-header-Example

0365 X- headers

- X-Forefront-Antispam-Report



```
X-Forefront-Antispam-Report:
CIP:74.121.48.51;CTRY:US;LANG:en;SCL:1;SRV:;IPV:NLI;SFV:NSPM;H:mail3566.haymarketmedia.mkt4163.com;P
TR:mail3566.haymarketmedia.mkt4163.com;CAT:NONE;SFTY:;SFS:(286005)(33964004)(1565050001)(26005)
(9686003)(6916009)(7066003)(66574012)(7596003)(7636003)(19630485002)(356005)(336012)(42186006)
(19627405001)(82870400002)(5426002)(8676002)(1096003)(42882007)(246002)(17308445002)(559001)
(579004);DIR:INB;SFP:;
```

- https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-message-headers

How to Investigate

Opening URLs or File Attachments

- Don’t do on phone or regular device/computer

Can lead to:

- Immediate exploitation
- Sending your password hash
- Sending your IP address
- Leaking more information
  - OS, browser, location, etc.

How to Investigate

Opening URLs or File Attachment

If you need to open a URL or file,

- Use free online service
- Turn over to a true forensic expert, who has the right equipment and tools
- Open in a safe virtual machine or isolated computer built for that purpose
  - Some malware can detect VM and not launch

Agenda

- How to Investigate
- Investigating Phishing
- Defenses

Best Defenses

Top Defenses for Most Organizations

- **Mitigate Social Engineering**
  - Policies, Technical Defenses, Education
- **Patch Internet-accessible software**
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- **Use Multifactor Authentication(MFA)/Non-Guessable passwords**
  - Use non-phishable MFA where you can
    - https://www.linkedin.com/pulse/my-list-good-strong-mfa-roger-grimes
  - Use unique, unguessable, different passwords for every website and service
- **Teach Everyone How to Spot Rogue URLs**
  - https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks
  - https://info.knowbe4.com/rogue-urls

All Anti-Phishing Defenses

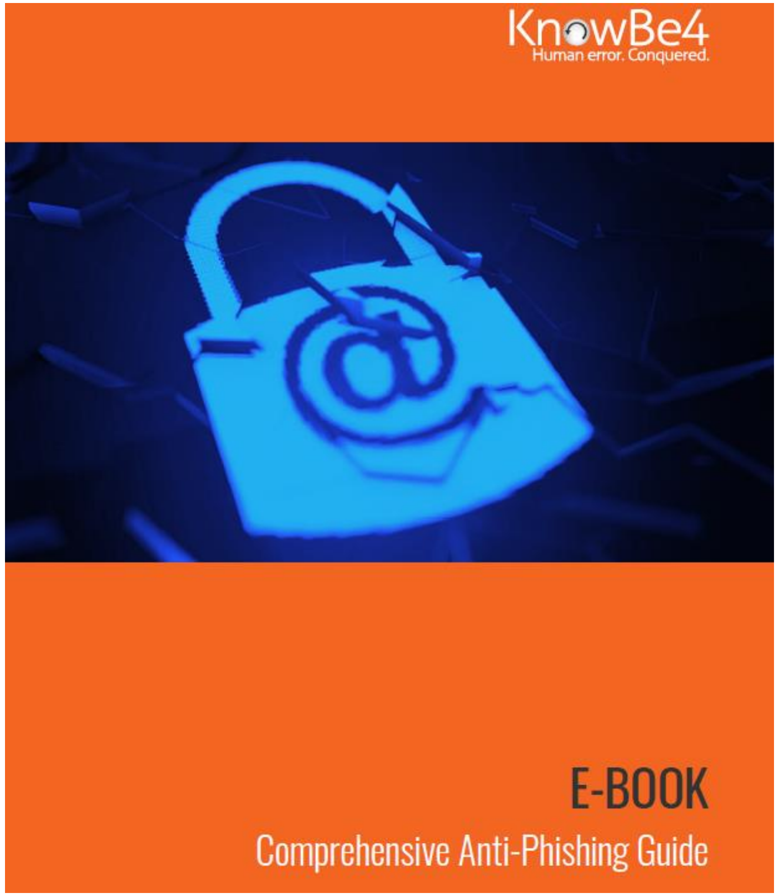
Everything You Can Try to Prevent Phishing

- Webinar
  - https://info.knowbe4.com/webinar-stay-out-of-the-net

ON-DEMAND WEBINAR

Stay out of the Net:

Your Ultimate Guide to Phishing Mitigation



KnowBe4

Human error. Conquered.

E-BOOK

Comprehensive Anti-Phishing Guide

- E-book
  - https://info.knowbe4.com/comprehensive-anti-phishing-guide

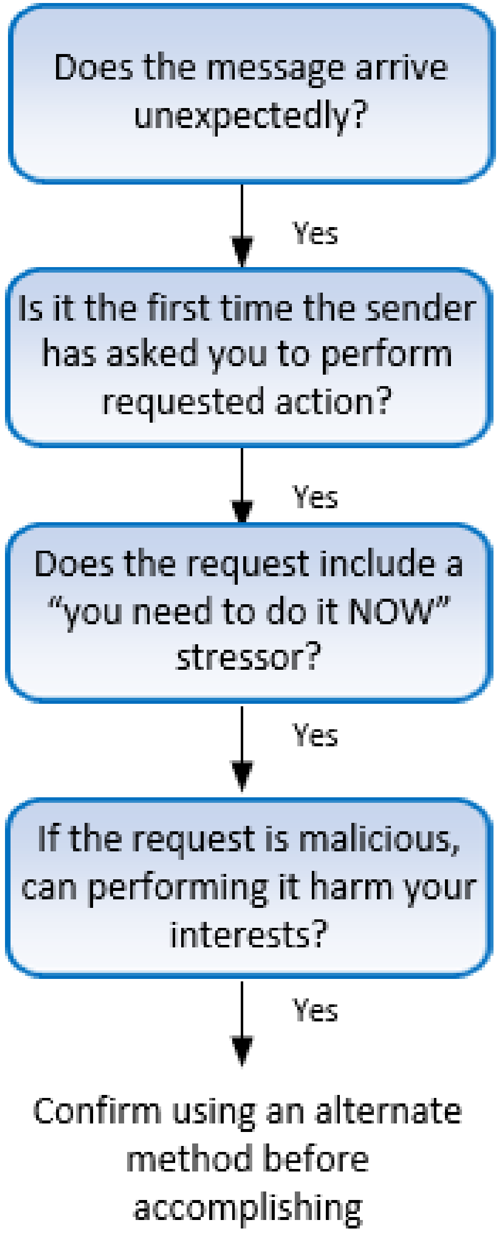
What Is the Goal of Security Awareness Training?

The overall goal is to help users make smarter security decisions every day

- To reach this goal you must make security awareness an integral part of your organizational culture that simply becomes reflexive

Training users to know

- How to spot bad things
- How to respond



Does the message arrive unexpectedly?

Yes

Is it the first time the sender has asked you to perform requested action?

Yes

Does the request include a “you need to do it NOW” stressor?

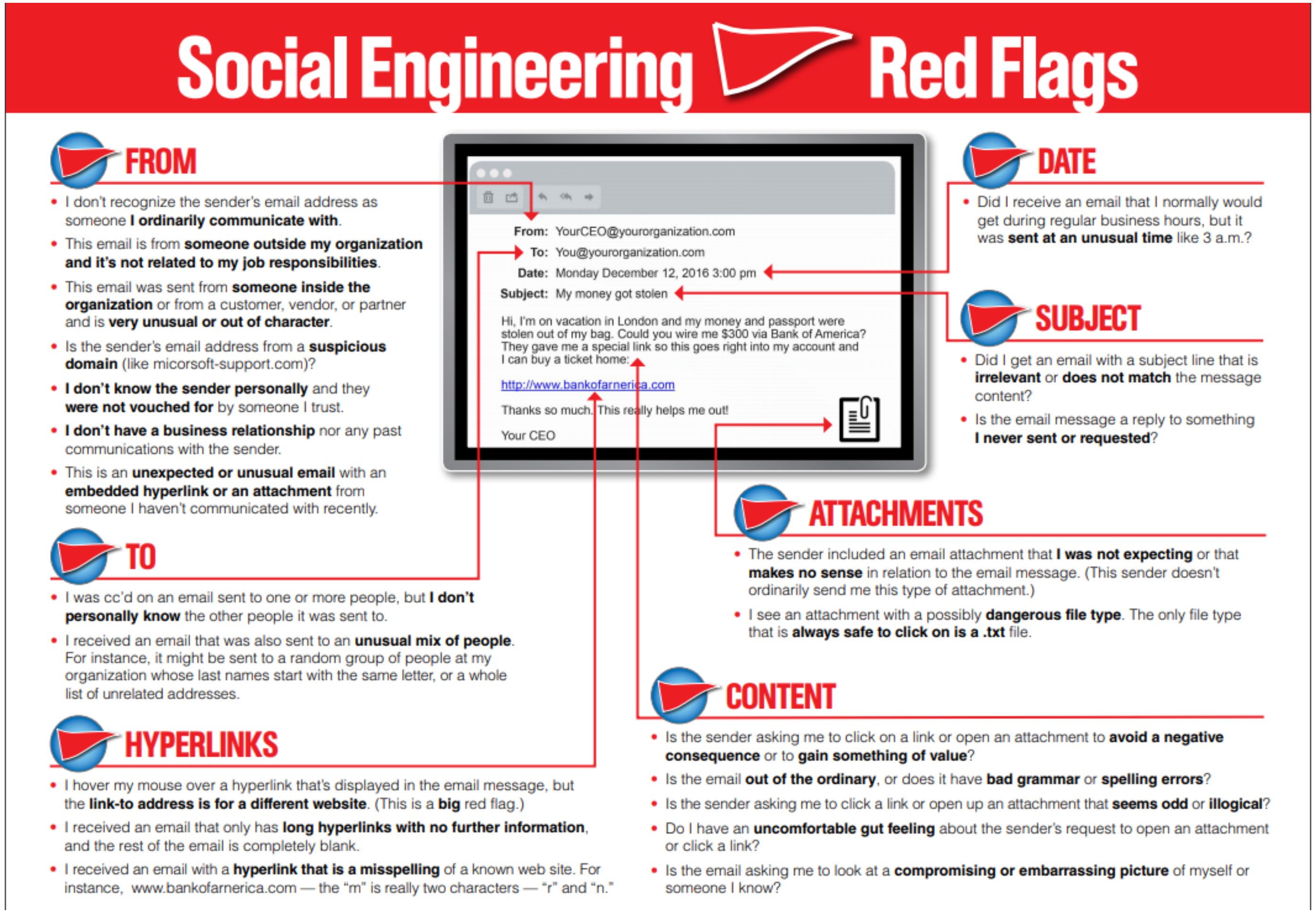
Yes

If the request is malicious, can performing it harm your interests?

Yes

Confirm using an alternate method before accomplishing

Give “Red Flags” Training



Social Engineering Red Flags

From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2016 3:00 pm
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the “m” is really two characters — “r” and “n.”

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

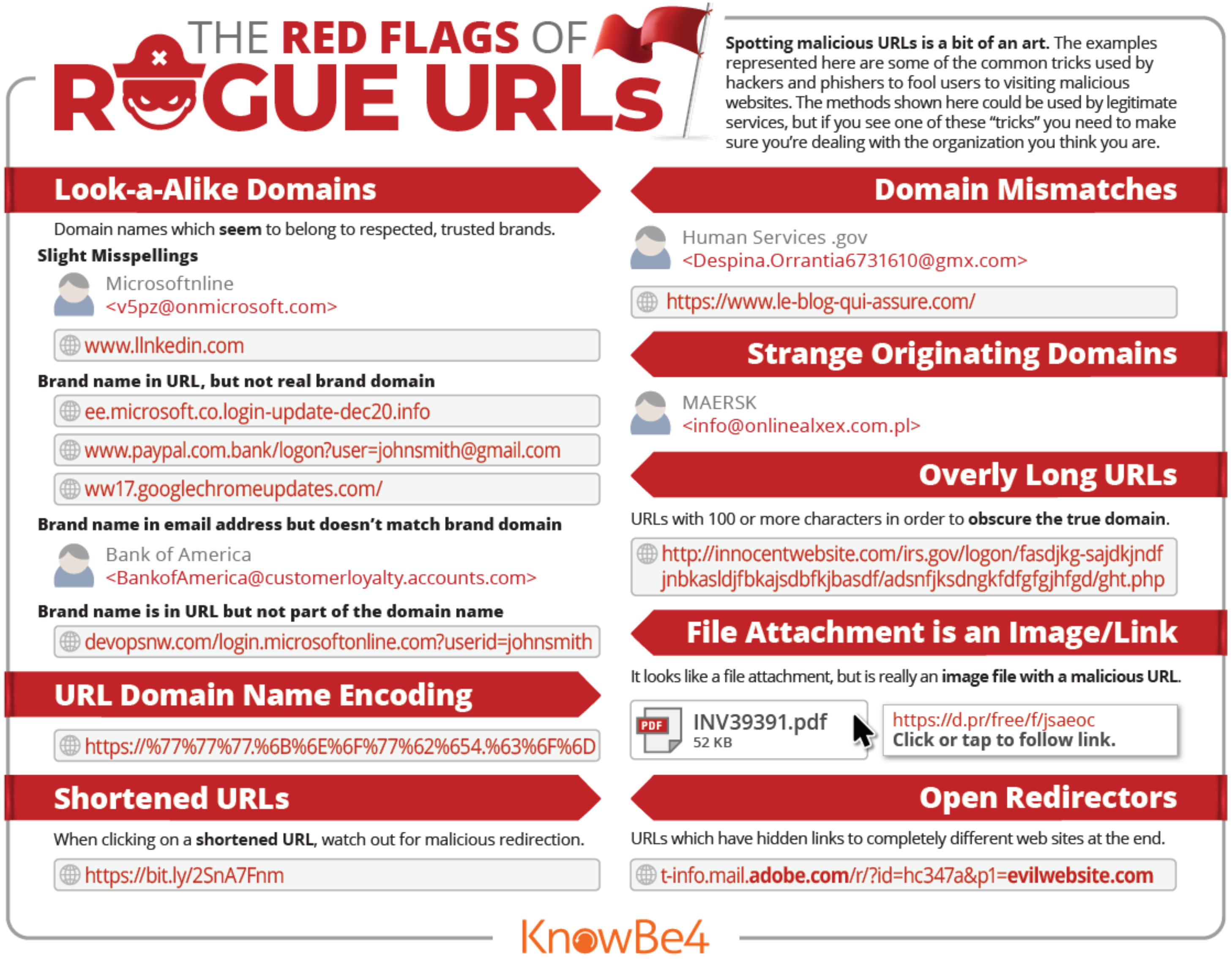
- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?



THE RED FLAGS OF ROGUE URLs

Spotting malicious URLs is a bit of an art. The examples represented here are some of the common tricks used by hackers and phishers to fool users to visiting malicious websites. The methods shown here could be used by legitimate services, but if you see one of these "tricks" you need to make sure you're dealing with the organization you think you are.

Look-a-Alike Domains

Domain names which **seem** to belong to respected, trusted brands.

Slight Misspellings

Microsoftnline
<v5pz@onmicrosoft.com>

www.lInkedin.com

Brand name in URL, but not real brand domain

ee.microsoft.co.login-update-dec20.info

www.paypal.com.bank/logon?user=johnsmith@gmail.com

ww17.googlechromeupdates.com/

Brand name in email address but doesn't match brand domain

Bank of America
<BankofAmerica@customerloyalty.accounts.com>

Brand name is in URL but not part of the domain name

devopsnw.com/login.microsoftonline.com?userid=johnsmith

URL Domain Name Encoding

https://%77%77%77.%6B%6E%6F%77%62%654.%63%6F%6D

Shortened URLs

When clicking on a **shortened URL**, watch out for malicious redirection.

https://bit.ly/2SnA7Fnm

Domain Mismatches

Human Services .gov
<Despina.Orrantia6731610@gmx.com>

https://www.le-blog-qui-assure.com/

Strange Originating Domains

MAERSK
<info@onlinealxex.com.pl>

Overly Long URLs

URLs with 100 or more characters in order to **obscure the true domain.**

http://innocentwebsite.com/irs.gov/logon/fasdjkg-sajdkjndf jnbkasldjfbkajsdbfkjbasdf/adsnfjksdngkfdfgfgjhfgd/ght.php

File Attachment is an Image/Link

It looks like a file attachment, but is really an **image file with a malicious URL.**

PDF INV39391.pdf
52 KB

https://d.pr/free/f/jsaeoc
Click or tap to follow link.

Open Redirectors

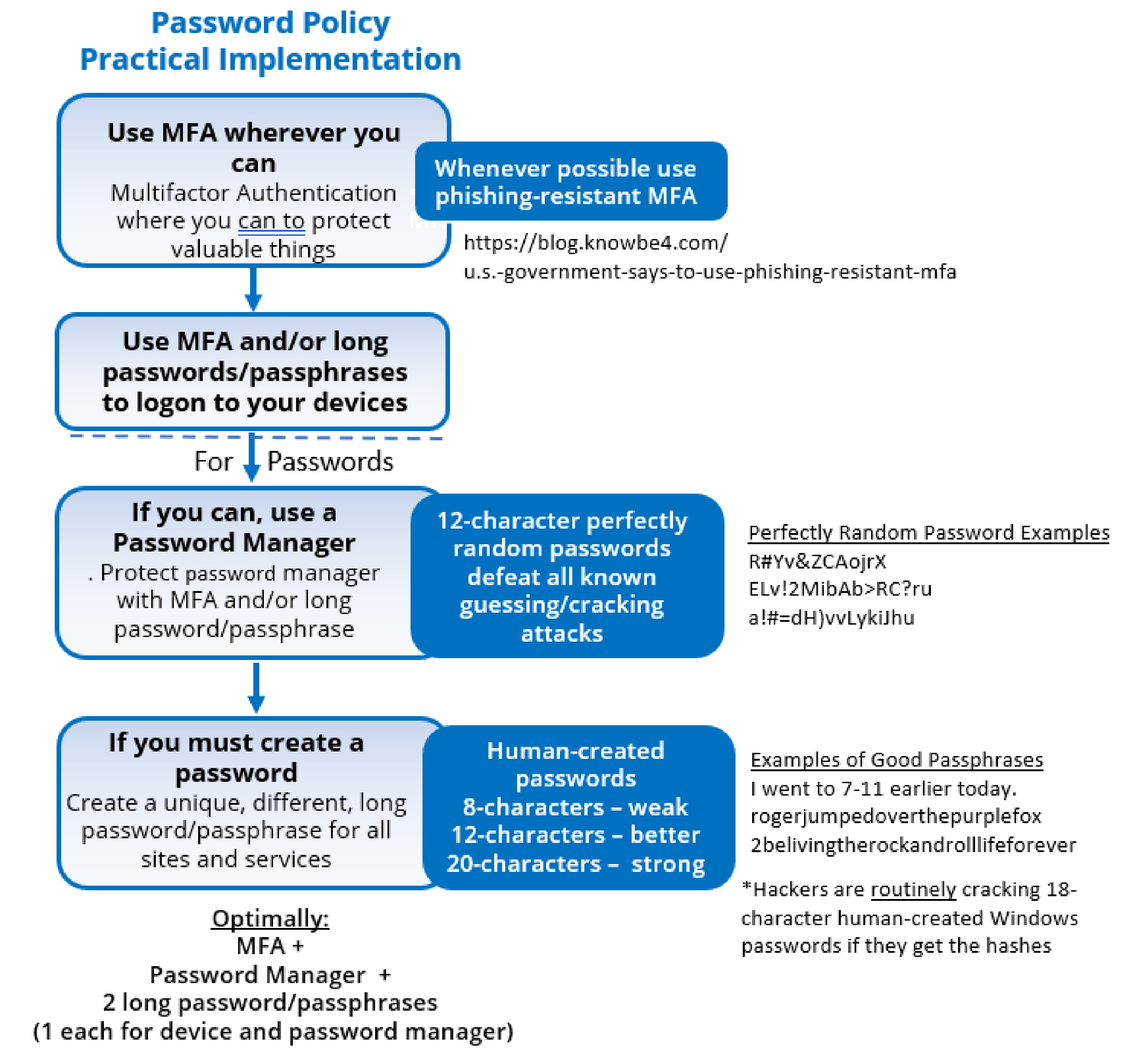
URLs which have hidden links to completely different web sites at the end.

t-info.mail.**adobe.com**/r/?id=hc347a&p1=**evilwebsite.com**

KnowBe4

https://blog.knowbe4.com/top-12-most-common-rogue-url-tricks

My Password Policy Advice



Password Policy
Practical Implementation

Use MFA wherever you can
Multifactor Authentication where you can to protect valuable things

Whenever possible use phishing-resistant MFA

https://blog.knowbe4.com/u.s.-government-says-to-use-phishing-resistant-mfa

Use MFA and/or long passwords/passphrases to logon to your devices

For Passwords

If you can, use a Password Manager
. Protect password manager with MFA and/or long password/passphrase

12-character perfectly random passwords defeat all known guessing/cracking attacks

Perfectly Random Password Examples
R#Yv&ZCAojrX
ELv!2MibAb>RC?ru
a!#=dH)vvLykiJhu

If you must create a password
Create a unique, different, long password/passphrase for all sites and services

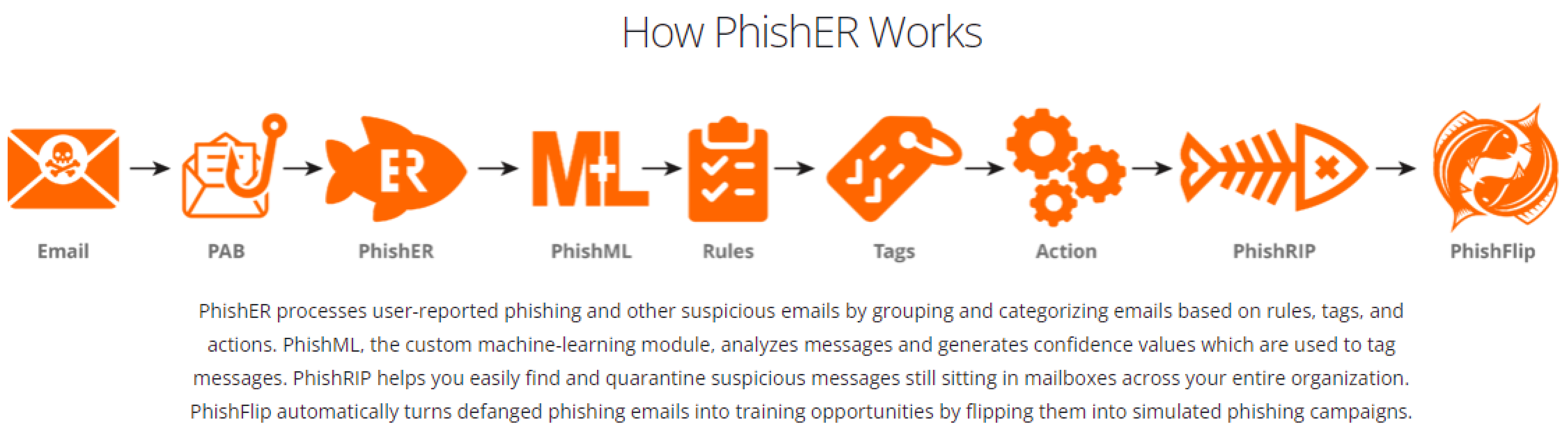
Human-created passwords
8-characters – weak
12-characters – better
20-characters – strong

Examples of Good Passphrases
I went to 7-11 earlier today.
rogerjumpedoverthepurplefox
2belivingtherockandrolllifeforever

*Hackers are routinely cracking 18-character human-created Windows passwords if they get the hashes

Optimally:
MFA +
Password Manager +
2 long password/passphrases
(1 each for device and password manager)

PhishER & PhishFlip



How PhishER Works

PhishER processes user-reported phishing and other suspicious emails by grouping and categorizing emails based on rules, tags, and actions. PhishML, the custom machine-learning module, analyzes messages and generates confidence values which are used to tag messages. PhishRIP helps you easily find and quarantine suspicious messages still sitting in mailboxes across your entire organization. PhishFlip automatically turns defanged phishing emails into training opportunities by flipping them into simulated phishing campaigns.

- https://www.knowbe4.com/products/phisher

Generating Industry-Leading Results and ROI

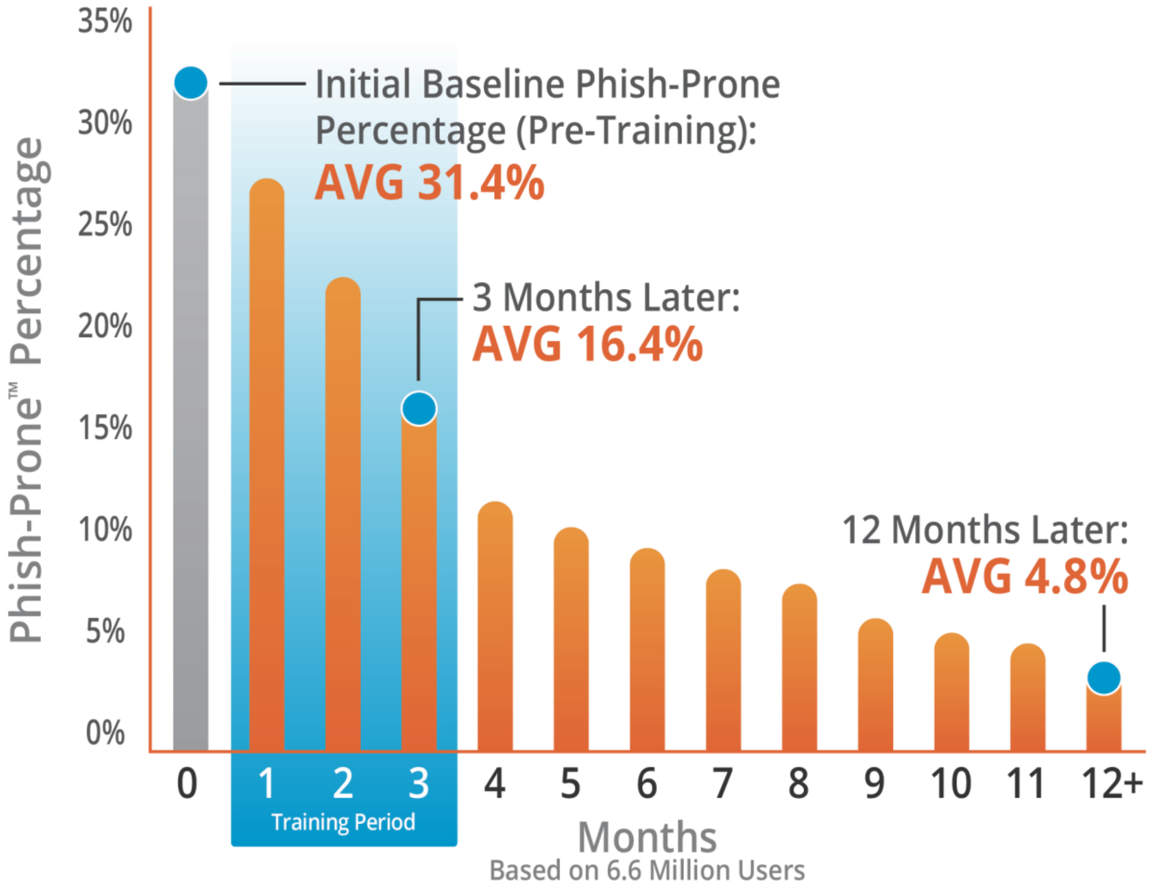
- Reduced Malware and Ransomware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

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/