EMAIL HEADER ANALYSIS
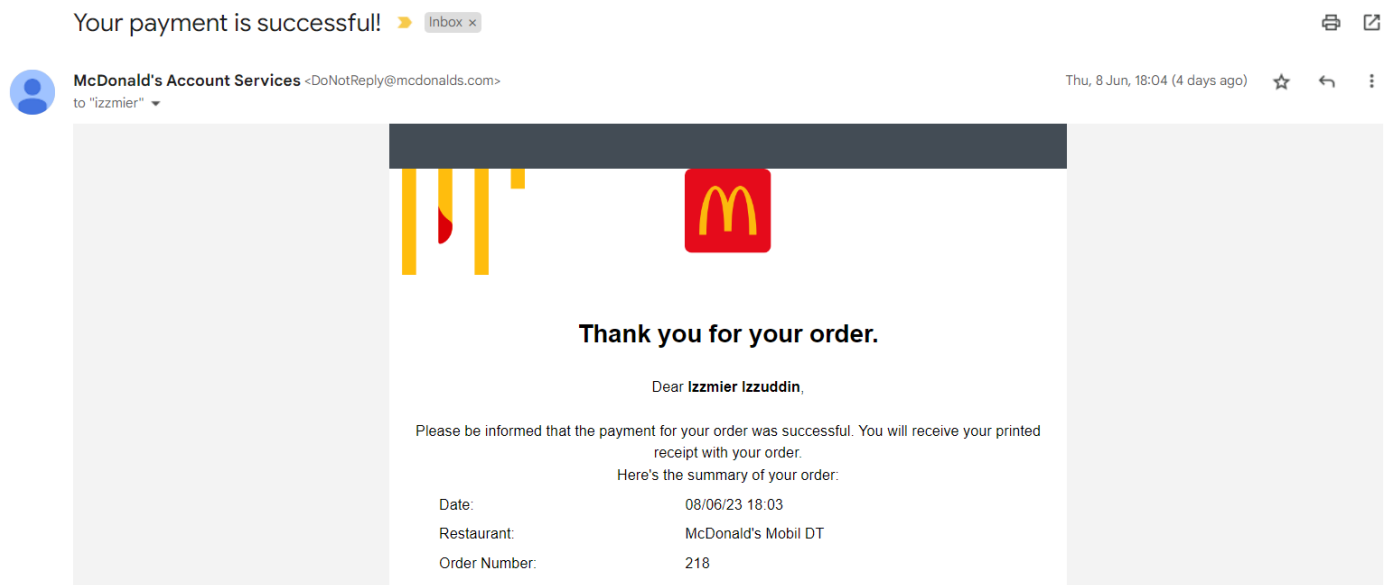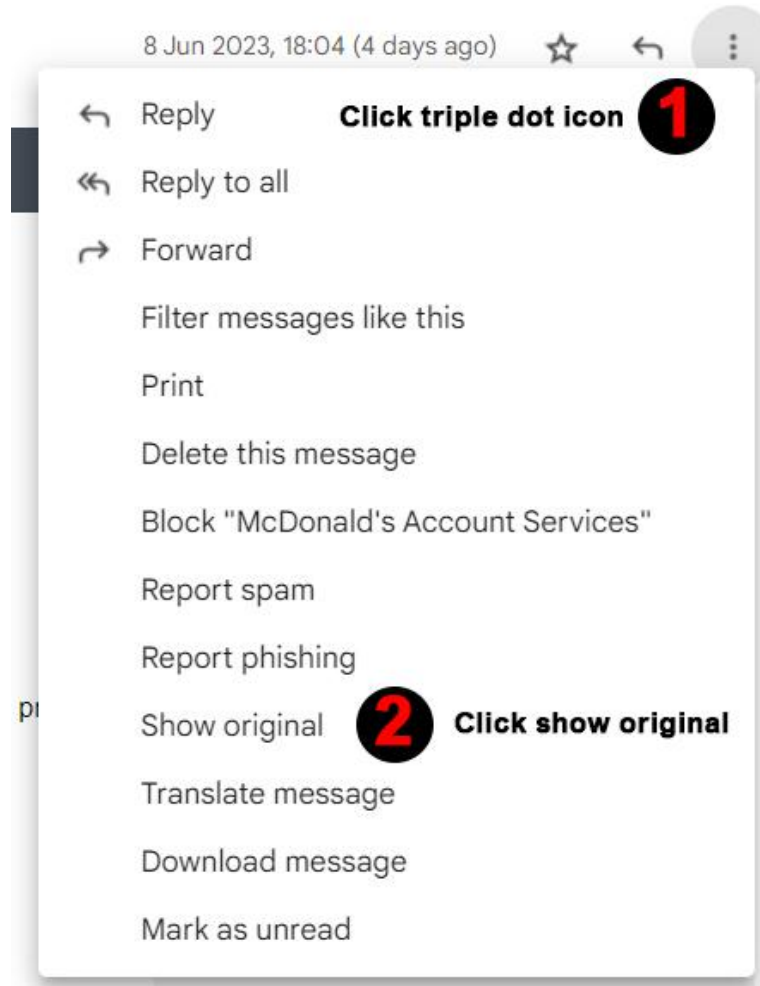
Email Header Analysis [Gmail]

STEP 1: Go through how the email body looks, if there are URLs and Attachments you will need to test them in sandbox environment [Virtual Machine]

Sandbox Environment — (static & dynamic analysis)

To test the links/attachments in sandbox environment make use of Virus Total for URL reputation check/ file hash check, Urlscan.io, palo alto url filtering, whois domaintools, haveibeenpwned, Inspect element of webpage -> check network activity, google dorks, Browserling, can run E-discovery check for user click actions on the links/attachments. You can also use other OSINT tools for analysing the links/attachments within sandbox environment.

STEP 2: To analyse the email header and email body begin with downloading the email in .eml format.

STEP 3: You will be greeted with Original Message page. If you select "Download Original" you will be able to download email in .eml format for header analysis or if you prefer using "Copy to Clipboard" to directly copy the header and paste in any email header analyzer tool for header analysis.

Copy to clipboard

Original message

Message ID	<010001889a7727cb-a48a90df-9eee-44a3-88e6-8a07458d3211-000000@email.amazonses.com>
Created on:	8 June 2023 at 18:04 (Delivered after 0 seconds)
From:	McDonald's Account Services <DoNotReply@mcdonalds.com>
To:	"izzmier"@gmail.com
Subject:	Your payment is successful!
SPF:	PASS with IP 54.240.11.45 Learn more
DKIM:	'PASS' with domain mcdonalds.com Learn more
DMARC:	'PASS' Learn more

Download original   Copy to clipboard

```
Delivered-To: izzmier@gmail.com
Received: by 2002:a05:7208:4007:b0:6b:58f3:9521 with SMTP id e7csp342251rbb;
        Thu, 8 Jun 2023 03:04:41 -0700 (PDT)
X-Google-Smtp-Source: ACHHUZ4ZMJGMq33Xg3vlWSHaH1ZpGDUx9R999bhKEwvDqdYoRk6MpZhFDDc8RK7PnTRdY0bkCP4c
X-Received: by 2002:a05:620a:211b:b0:75e:4492:740e with SMTP id l27-20020a05620a211b00b0075e4492740emr4841878qkl.33.1686218680993;
        Thu, 08 Jun 2023 03:04:40 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1686218680; cv=none;
        d=google.com; s=arc-20160816;
        b=YP1Q3rDWdaUa/L/YQFzzczdDepA/wadcfwcosUiTbmQuVUburGYsiwRt8+q8AZ8ocS
         ow8IZMO8ttqjDjRvkWY9GHiJ84VCVuj5hRB2+++YBuhJ3W5YZh03T4ziOQs+sNPVOUAe
         z1jvceTyKlCCRIHZbEpU+HQnfMjlL86a3d7lGYOlZ0ZrVuRSlkiWNuFuPx60n3Wk/ipm
         oLda0rt5MkfwigLn3ge2ZYSKTVWITgoVcd8NkBQHgCI7Hx7OgqRcSIe/AwKu2E389pjB
         8vODbEWyf/+eS0IoJEZGXno0IOYfTGR40kle8+dEWoXsnccDHf3JGHpTlBV4b+ou8K9S
         gcQg==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=feedback-id:content-transfer-encoding:content-id:mime-version:to
         :message-id:subject:date:from:dkim-signature:dkim-signature;
```

Download original

Original message

Message ID	<010001889a7727cb-a48a90df-9eee-44a3-88e6-8a07458d3211-000000@ema...
Created on:	8 June 2023 at 18:04 (Delivered after 0 seconds)
From:	McDonald's Account Services <DoNotReply@mcdonalds.com>
To:	"izzmier"@gmail.com
Subject:	Your payment is successful!
SPF:	PASS with IP 54.240.11.45 Learn more
DKIM:	'PASS' with domain mcdonalds.com Learn more
DMARC:	'PASS' Learn more

**1** Download original

```
Delivered-To: izzmier@gmail.com
Received: by 2002:a05:7208:4007:b0:6b:58f3:9521 with SMTP id e7csp342251rbb;
        Thu, 8 Jun 2023 03:04:41 -0700 (PDT)
X-Google-Smtp-Source: ACHHUZ4ZMJGMq33Xg3vlWSHaH1ZpGDUx9R999bhKEwvDqdYoRk6MpZhFDDc8RK7PnTRdY0bkCP4c
X-Received: by 2002:a05:620a:211b:b0:75e:4492:740e with SMTP id l27-20020a05620a211b00b0075e4492740e...
        Thu, 08 Jun 2023 03:04:40 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1686218680; cv=none;
        d=google.com; s=arc-20160816;
        b=YP1Q3rDWdaUa/L/YQFzzczdDepA/wadcfwcosUiTbmQuVUburGYsiwRt8+q8AZ8ocS
         ow8IZMO8ttqjDjRvkWY9GHiJ84VCVuj5hRB2+++YBuhJ3W5YZh03T4ziOQs+sNPVOUAe
         z1jvceTyKlCCRIHZbEpU+HQnfMjlL86a3d7lGYOlZ0ZrVuRSlkiWNuFuPx60n3Wk/ipm
         oLda0rt5MkfwigLn3ge2ZYSKTVWITgoVcd8NkBQHgCI7Hx7OgqRcSIe/AwKu2E389pjB
         8vODbEWyf/+eS0IoJEZGXno0IOYfTGR40kle8+dEWoXsnccDHf3JGHpTlBV4b+ou8K9S
         gcQg==
```

📄 Your payment is s....eml **2**

STEP 4: Email Header Analysis: SPF, DKIM, DMARC, SCL & BCL score

Header analysis is done on MxtoolBox
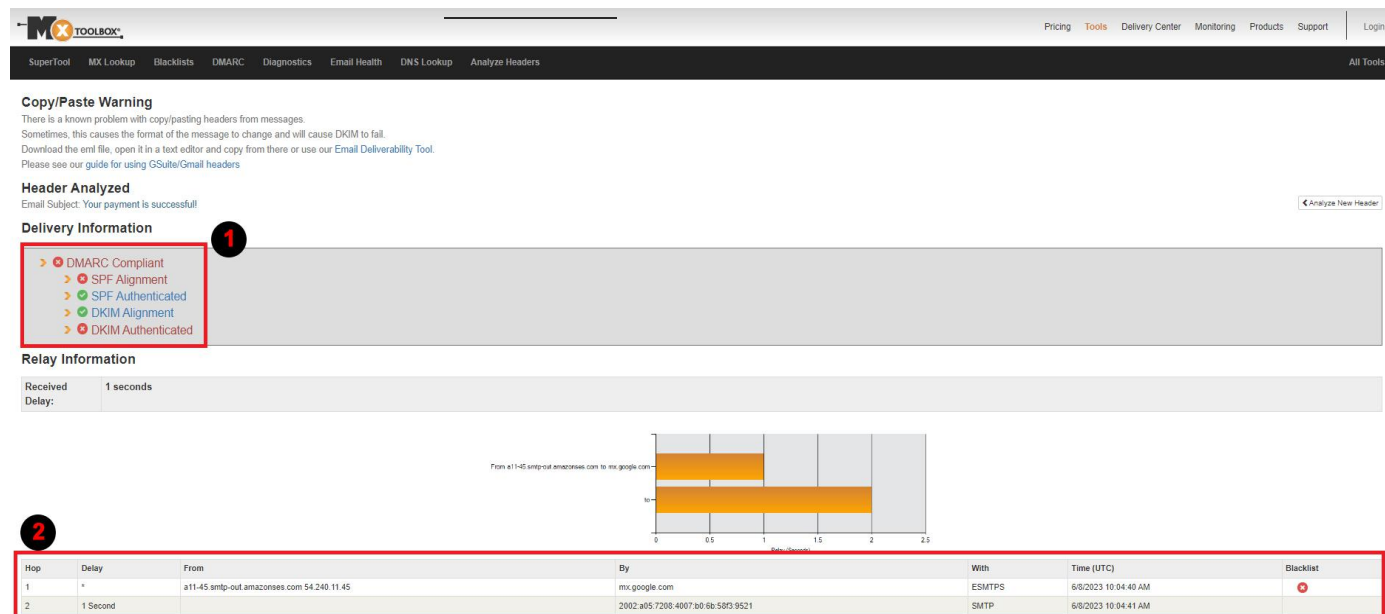
We see that SPF Alignment, SPF Authenticated, DKIM Alignment, and DKIM Authenticated all are PASS.

· To check Spoof → click on three dots

→ original message → check Message ID [If there is difference between Message ID value and "From" Field value, then indication is of spoofing]

· SPF Alignment — The SPF Alignment is PASS only when "Return-Path" And "From" domain is same. Different between which helps us understand email could be spoofed.

· SPF Authentication — If SPF authentication is FAIL, it means the sender IP address is not authorized to send email on behalf of the legit domain.

· DKIM Alignment- compare the DKIM Signature field [d=domain.com] with "From" , if it does not match then the result marks DKIM Alignment as FAIL.

· DKIM Authentication- If DKIM Signature field [b=........] is not verified so we can say that the email has been modified or tempered.

What is SPF, DKIM, DMARC?

Sender Policy Framework (SPF) is a way for a domain to list all the servers they send emails from. Think of it like a publicly available employee directory that helps someone to confirm if an employee works for an organization.

```
SPF record typically looks like v=spf1 ip4:123.123.123.123 ~all
```

SPF distinguishes between **"soft" and "hard" fails**. Writing `~all` in your header indicates a soft fail when an unauthorized sender is encountered; `-all` instructs the receiving server to use a hard fail.

The email will be discarded entirely in a hard fail scenario. Soft fails may permit the email to be delivered to the recipient's junk folder. Now DMARC is widely available, which we'll see below, it's generally recommended to use `~all` (soft fail). This avoids false positives with legitimate emails, hands more control to DMARC, and can aid debugging in later verification stages.

DomainKeys Identified Mail (DKIM) enables domain owners to automatically "sign" emails from their domain, just as the signature on a check helps confirm who wrote the check. The DKIM "signature" is a digital signature that uses cryptography to mathematically verify that the email came from the domain.

Domain-based Message Authentication Reporting and Conformance (DMARC) tells a receiving email server what to do given the results after checking SPF and DKIM. A domain's DMARC policy can be set in a variety of ways — it can instruct mail servers to quarantine emails that fail SPF or DKIM (or both), to reject such emails, or to deliver them.

```
DMARC DNS Record v=DMARC1; p=none; rua=mailto:user@example.com
```

Unlike SPF and DKIM, DMARC gives domain owners a way to specify what happens when an email server receives a message without proper authentication. There are three supported actions:

· none — The server can continue to deliver the message.

· quarantine — Deliver the message to junk or spam.

· reject — Reject and bounce the message.

DMARC also provides a reporting mechanism. You can specify a server endpoint that receiving mail servers will call when they get an email purporting to be from your domain. This gives you a cross-internet view of the servers that are sending as your domain.

Another important part to know about SCL and BCL score?

Use mail flow rules to set the spam confidence level (SCL) in messages. Similar to the SCL, the **bulk complaint level** (BCL) identifies bad bulk email (also known as Gray mail). A higher BCL indicates a bulk mail message is more likely to generate complaints (and is therefore more likely to be spam).

SCL	Definition	Default action
-1	The message skipped spam filtering. For example, the message is from a safe sender, was sent to a safe recipient, or is from an email source server on the IP Allow List. For more information, see Create safe sender lists in EOP.	Deliver the message to recipient Inbox folders.
0, 1	Spam filtering determined the message wasn't spam.	Deliver the message to recipient Inbox folders.
5, 6	Spam filtering marked the message as **Spam**	Default anti-spam policy, new anti-spam policies, and Standard preset security policy: Deliver the message to recipient Junk Email folders. Strict preset security policy: Quarantine the message.
8, 9	Spam filtering marked the message as **High confidence spam**	Default anti-spam policy and new anti-spam policies: Deliver the message to recipient Junk Email folders. Standard and Strict preset security policies: Quarantine the message.

SPF and DKIM Information

dmarc:mcdonalds.com [Show] [Solve Email Delivery Problems]

```
v=DMARC1; p=none; rua=mailto:dmarc_agg@dmarc.everest.email; fo=1; pct=100; rf=afrf
```

spf:amazonses.com:54.240.11.45 [Show]

```
v=spf1 ip4:199.255.192.0/22 ip4:199.127.232.0/22 ip4:54.240.0.0/18 ip4:69.169.224.0/20 ip4:23.249.208.0/20 ip4:23.251.224.0/19 ip4:76.223.176.0/20 ip4:54.240.64.0/19 ip4:54.240.96.0/19 ip4:52.82.172.0/22 ip4:76.223.128.0/19 -all
```

dkim:mcdonalds.com:sbihrvfdaa75rgervod6avew5c2t24ka [Show]

Dkim Public Record:
```
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCzukfeWAkfx+Wk/4XklwCBlBW7obziDmARe0dajx0xCKa6ZTSUhxZdQhC9knUeJhFtO/n6CIrrFR+4XmW1fAq9mJZn/rBSSuefgIQgYH0BsDKdurP4GCAUU/65lUx3qPTHfVyUQNhzGJMha1htb3AYuR0bPpFlqflEWEtgdN6+GQIDAQAB
```

Dkim Signature:
```
v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; s=sbihrvfdaa75rgervod6avew5c2t24ka; d=mcdonalds.com; t=1686218680; h=From:Date:Subject:Message-Id:To:MIME-Version:Content-Type:Content-Id:Content-Transfer-Encoding; bh=yKy2SznKraiB4syk3riCXLU3wUXht3aiwaFfrJWQVvI=; b=j4TuAD9gD2TOfHsGRbHExtpXBqLOStEOCC
```

dkim:amazonses.com:224i4yxa5dv7c2xz3womw6peuasteono [Show]

Dkim Public Record:
```
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCRg1AaPDkSgt5Z6xAH/eWWg0FGcAZphroLwtAIrkcGGKzFNkNEcKlrxZN6VRqchbVoDAV/FLG6NW4H0TGYwbJaeTeNGeJnzrjHem+9e5GbWSE5z9jkvp0WwC/vfiApjwMAnh7a4dLcmxy4G/0hctrYfIw+TUpmuq1V0ow2o5i/AwIDAQAB
```

Dkim Signature:
```
v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; s=224i4yxa5dv7c2xz3womw6peuasteono; d=amazonses.com; t=1686218680; h=From:Date:Subject:Message-Id:To:MIME-Version:Content-Type:Content-Id:Content-Transfer-Encoding:Feedback-ID; bh=yKy2SznKraiB4syk3riCXLU3wUXht3aiwaFfrJWQVvI=; b=aUMkpOuOmAoSZAlQ0UNilq
```

Header Name	Header Value
Delivered-To	izzmier@gmail.com
X-Google-Smtp-Source	ACHHUZ4ZMJGMq33Xg3vlWSHaH1ZpGDUx9R999bhKEwvDqdYoRk6MpZhFDDc8RK7PnTRdY0bkCP4c
X-Received	by 2002:a05:620a:211b:b0:75e:4492:740e with SMTP id I27-20020a05620a211b00b0075e4492740emr4841878qkl.33.1686218680993; Thu, 08 Jun 2023 03:04:40 -0700 (PDT)
ARC-Seal	i=1; a=rsa-sha256; t=1686218680; cv=none; d=google.com; s=arc-20160816; b=YP1Q3rDWdaUa/L/YQFzzczdDepA/wadcfwcosUiTbmQuVUburGYsiwRt8+q8AZ8ocS ow8IZMO8ttqjDj wigLn3ge2ZYSKTVWlTgoVcd8NkBQHgCI7Hx7OgqRcSle/AwKu2E389pjB 8vODbEWyf/+eS0IoJEZGXno0IOYfTGR40kle8+dEWoXsnccDHf3JGHpTIBV4b+ou8K9S gcQg==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816; h=feedback-id:content-transfer-encoding:content-id:mime-version:to :message-id:subject:date:from:dkim-signatu oeDqckoa8EoYoOWdV5IOPmqoAi/5rKvKTvVmWIlqYDzESF0icB0J0YkYJ3e6sjmO HOcCk2XFhu+yp4uKCnssIIFPfO/aiKr0OJz0pua7Wv1wYFkIR8WhRoM5mYdXnWWQEwLM BEUE8 OP SraQ==
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@mcdonalds.com header.s=sbihrvfdaa75rgervod6avew5c2t24ka header.b=j4TuAD9g; dkim=pass header.i=@amazonses.com header.s=224i onses.com designates 54.240.11.45 as permitted sender) smtp.mailfrom=010001889a7727cb-a48a90df-9eee-44a3-88e6-8a07458d3211-000000@amazonses.com; dmarc=pass (p=N
Return-Path	<010001889a7727cb-a48a90df-9eee-44a3-88e6-8a07458d3211-000000@amazonses.com>
Received-SPF	pass google.com: domain of 010001889a7727cb-a48a90df-9eee-44a3-88e6-8a07458d3211-000000@amazonses.com designates 54.240.11.45 as permitted sender) client-ip=54.240
Authentication-Results	mx.google.com; dkim=pass header.i=@mcdonalds.com header.s=sbihrvfdaa75rgervod6avew5c2t24ka header.b=j4TuAD9g; dkim=pass header.i=@amazonses.com header.s=224i4yxa es.com designates 54.240.11.45 as permitted sender) smtp.mailfrom=010001889a7727cb-a48a90df-9eee-44a3-88e6-8a07458d3211-000000@amazonses.com; dmarc=pass (p=NONE
DKIM-Signature	v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; s=sbihrvfdaa75rgervod6avew5c2t24ka; d=mcdonalds.com; t=1686218680; h=From:Date:Subject:Message-Id:To:MIME-Version:Conten 5AiFzs6sxevHOrqj 6a7B7J2IPKRRT5OmC8xhoY2GmrU7OQhxB49uFoXDOUhRI7ERHFElYT1E73H93/TDg7K ukGpwTSOKbNMgfBS+mRAGpinrbMe/6+Yax09nS6o=
From	"McDonald's Account Services" <DoNotReply@mcdonalds.com>
Date	Thu, 8 Jun 2023 10:04:40 +0000
Subject	Your payment is successful!
Message-ID	<010001889a7727cb-a48a90df-9eee-44a3-88e6-8a07458d3211-000000@email.amazonses.com>
To	"izzmier"@gmail.com
MIME-Version	1.0
Content-Type	text/html; charset=utf-8
Content-Id	<DY4JBQCG5KU4.Q34JOA30H8H51@169.254.178.201>
Content-Transfer-Encoding	quoted-printable
Feedback-ID	1.us-east-1.uSkbSFk9Rxz1+oiPy3rSprgKsRG1IwJqynZ/FLF2s40=:AmazonSES
X-SES-Outgoing	2023.06.08-54.240.11.45

Breaking Down an Email:

Let us first go through some of the important headers to understand what they represent. It is ideal to read message headers from bottom to top to be able to properly understand where the email is originated from.

- **X-priority:** X-priority is an optional parameter in the email spec used to specify the priority of the email. Values can be 1 (Highest), 2 (High), 3 (Normal), 4 (Low) or 5 (Lowest). Three is default if the field is omitted. Most email programs don't fill it in unless it is set low or high. Client side programs will highlight the inbound message (!) if it is 1 or 2.

- **Content-Type:** This header specifies the type of content in the email. The preceding email is of plain text.

- **Reply-To:** This header specifies whom to send the reply when the receiver replies to the email received.

- **Message-Id:** Message Id is a unique identifier that can be used to identify the message.

- **From:** This header is used to display the username or email from which email is sent. Note that spoofed emails typically modify this header to appear to have come from a known source.

- **Received:** This header represents the recipient details. There can be multiple entries of this header as the email traverses through multiple servers.

- **Received-SPF:** This header represents the Sender Policy Framework (SPF) results, which tells whether the sender is a permitted sender or not.

- **Delivered-To:** This header represents the destination email id that the email is delivered to.

In addition to the headers discussed so far, we can see three additional headers as shown below.

- ARC-Seal

- ARC-Message-Signature

- ARC-Authentication-Results

ARC-XXXX headers help preserve email authentication results and verify the identity of email intermediaries that forward a message on to its final destination.

- **ARC Authentication Results:** This header contains email authentication results like SPF, DKIM, and DMARC

- **ARC-Message-Signature:** This is a DKIM-like signature and takes a snapshot of the message header information. This includes to, from, subject and body

- **ARC-Seal:** This header contains a signature which includes the ARC-Message-Signature and the ARC Authentication Results header information.

STEP 5: Email Body Analysis: sender, subject, email body, embedded URL/Attachments

Check the subject of the email to understand what it is about. Check the sender domain in Virus Total, Whois DomainTools, Urlscan.io, Browserling, and Palo Alto Url Filtering. You can test your personal email ID in Have I been Pwned to check if your id is breached or safe. Don't enter professional/ Corporate email ID here — Have I been Pwned (as it is a public repo). Use of Inspect element -> Network is also important to check the redirected URL activity and real intent of the Base/original URL.

Fields to check are Subject, Sender, Sender Domain, Recipient, Recipient Domain, Network Message ID, Latest email delivery, Original email delivery.

Later check the tone of the email body/email content. If any link (URL) or Attachment is embedded in the email, extract the URL/Attachment not by clicking it (don't interact with it) Instead by coping it [Right click -> Copy Hyperlink / Copy] and paste to test the URL/File in Windows sandbox / Sandbox Environment or test the Attachment within the sandbox environment (example — windows sandbox)

REMEDIATION/MITIGATION- (Personal / Corporate)

STEP 6: Remediation/Mitigation — If the users have either received phishing or spam email

· Enable multi-factor authentication (MFA) systems in place for accounts that can contain personal (PII)/ confidential/ Highly-Confidential/ Sensitive information.

· Perform email purge (email deletion) from the mailbox.

· Report the email as abuse of Phishing/Spam to your email service provider.

· Educate the mail service provider (eg- gmail) or tool used within corporate environment by reporting it as either phishing or spam based on your findings.

· If needed, you can also perform URL block for Malicious/suspicious URL/Domain.

· Or Submit Request to decommission of base URL/ Redirected URL to your mail service provider.

· Now look for number of users who might have clicked on the URL/attachment of the email, if identified any reset credential for that/those user(s)

· You can also perform actions from the below image.
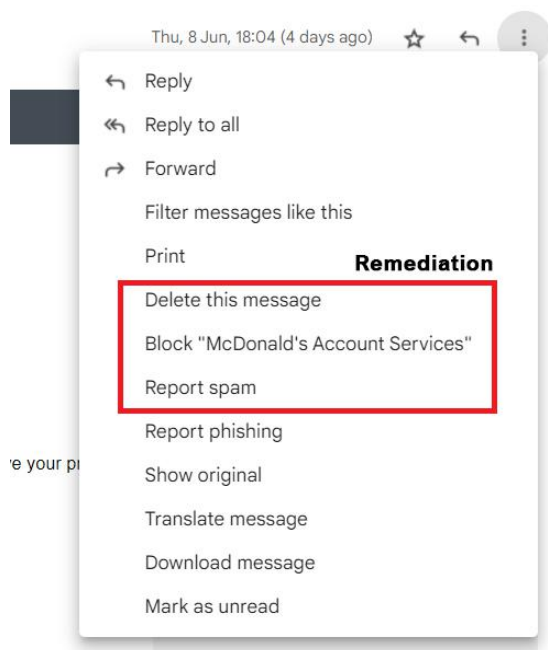
USER AWARENESS

STEP 7: USER Awareness / Phishing Simulation emails

Create awareness banners, brochures for the users to keep them educated on how to spot phishing email & protect themselves.

For company, Scheduled events on phishing simulation activity within the environment helps the organization evaluate employees' understanding about phishing attacks.

Exercise Email Header Analysis

What about that email from President Donald Trump?

Here is the raw header:

```
Received: from CY1PR0701MB1819.namprd07.prod.outlook.com (10.163.42.152) by
 SN1PR0701MB1822.namprd07.prod.outlook.com (10.162.100.151) with Microsoft
 SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id 15.1.1240.13 via
 Mailbox Transport; Wed, 12 Jul 2017 22:49:17 +0000
Received: from SN1PR0701CA0032.namprd07.prod.outlook.com (10.162.96.42) by
 CY1PR0701MB1819.namprd07.prod.outlook.com (10.163.42.152) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id
 15.1.1261.13; Wed, 12 Jul 2017 22:49:16 +0000
Received: from BY2NAM01FT042.eop-nam01.prod.protection.outlook.com
 (2a01:111:f400:7e42::203) by SN1PR0701CA0032.outlook.office365.com
 (2a01:111:e400:5173::42) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256) id 15.1.1261.13 via
 Frontend Transport; Wed, 12 Jul 2017 22:49:16 +0000
Authentication-Results: spf=none (sender IP is 148.163.152.157)
 smtp.mailfrom=loki.ist.unomaha.edu; unomaha.edu; dkim=none (message not
 signed) header.d=none;unomaha.edu; dmarc=none action=none
 header.from=whitehouse.gov;
Received-SPF: None (protection.outlook.com: loki.ist.unomaha.edu does not
 designate permitted sender hosts)
Received: from mx0b-00261b01.pphosted.com (148.163.152.157) by
 BY2NAM01FT042.mail.protection.outlook.com (10.152.68.172) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id
 15.1.1240.9 via Frontend Transport; Wed, 12 Jul 2017 22:49:15 +0000
Received: from pps.filterd (m0104361.ppops.net [127.0.0.1])
    by mx0b-00261b01.pphosted.com (8.16.0.21/8.16.0.21) with SMTP id v6CMlhnA032537
    for <smartprof@unomaha.edu>; Wed, 12 Jul 2017 17:49:15 -0500
Authentication-Results-Original: ppops.net;    spf=none
 smtp.mailfrom=smartprof@loki.ist.unomaha.edu
Received: from loki.ist.unomaha.edu (loki.ist.unomaha.edu [137.48.187.123])
    by mx0b-00261b01.pphosted.com with ESMTP id 2bnsq8rykp-1
    for <smartprof@unomaha.edu>; Wed, 12 Jul 2017 17:49:15 -0500
Received: by loki.ist.unomaha.edu (Postfix, from userid 13823)
    id 958031E5EE0; Wed, 12 Jul 2017 17:49:14 -0500 (CDT)
To: <smartprof@unomaha.edu>
Subject: Make Cybersecurity Great Again!
X-PHP-Originating-Script: 13823:spoof.php
From: Donald Trump <therealdonaldtrump@whitehouse.gov>
Reply-To: Robin Gandhi <smartprof@unomaha.edu>
Content-Type: text/html; charset="ISO-8859-1"
Message-ID: <20170712224914.958031E5EE0@loki.ist.unomaha.edu>
Date: Wed, 12 Jul 2017 17:49:14 -0500
X-Proofpoint-Spam-Details: rule=inbound_notspam policy=inbound score=1 priorityscore=0 m
alwarescore=0
```

```
 suspectscore=10 phishscore=0 bulkscore=0 spamscore=1 clxscore=195
 lowpriorityscore=0 impostorscore=0 adultscore=0 classifier=spam adjust=0
 reason=mlx scancount=1 engine=8.0.1-1706020000 definitions=main-1707120363
Return-Path: smartprof@loki.ist.unomaha.edu
X-MS-Exchange-Organization-Network-Message-Id: c0790240-3fdc-4b35-078d-08d4c9783957
X-EOPAttributedMessage: 0
X-EOPTenantAttributedMessage: f1f4be86-d048-47e8-aa26-15b01dcdb13d:0
X-MS-Exchange-Organization-MessageDirectionality: Incoming
X-Forefront-Antispam-Report: CIP:148.163.152.157;IPV:NLI;CTRY:US;EFV:NLI;SFV:SKN;SFS:;DI
R:INB;SFP:;SCL:-1;SRVR:CY1PR0701MB1819;H:mx0b-00261b01.pphosted.com;FPR:;SPF:None;LANG:e
n;
MIME-Version: 1.0

<html><head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">   </head>   <
body style="word-wrap: break-word; -webkit-nbsp-mode: space; -webkit-line-break: after-w
hite-space;" class="">   Dear Dr. Gandhi,<br class="">   <br class="">   You are doin
g very very good work with the Gencyber Camp. <br class="">   Just let me know wha
t you need to make it bigly successful next year!<br class="">   Please put in your fun
ding request here: <a href="https://robinagandhi.github.io/phishing-demo/encoding.h
tml" class="">Grant Application</a><br class=""> <br class=""><div class="">~Yours Truly
<br class=""><font color="#ff2600" class="">Donald</font></div></body></html>
```

Questions:

- What are the `From` and `Return-Path` email addresses. Do they match? What are they?
- What is the name of the sending computer or server?
- Where is the sending computer geo-located?
- What website is linked to "Grant funding request." in the message?
- How likely is it that this message is spam?