STEP BY STEP TO ANALYSE AND RESPOND POTENTIALLY MALICIOUS EMAIL

BY IZZMIER IZZUDDIN

Step-by-Step Guide to Analysing a Potentially Malicious Email

Step 1: Initial Email Body Review

1. **Read the Email Carefully**:
   - Check for any urgent or threatening language.
   - Look for requests for sensitive information or actions (e.g., clicking a link, downloading an attachment).
2. **Identify Links and Attachments**:
   - Note any links or attachments in the email.

Step 2: Save and Examine the Email

1. **Save the Email**:
   - Save the email in .eml or .msg format for detailed analysis.
2. **Open the Email Header**:
   - Use an email client or web-based service to view the email header information.

Step 3: Analyse the Email Header

1. **Copy the Email Header**:
   - Copy the entire header information for analysis.
2. **Use an Email Header Analyser**:
   - Go to a tool like MXToolbox Email Header Analyser and paste the header.
   - Click "Analyse Header".
3. **Check Key Fields**:
   - **Received**: Check the sequence of servers the email passed through.
   - **From and Reply-To**: Ensure these fields are from legitimate sources and match each other.
   - **Message-ID**: Verify if it matches the domain of the sender.
   - **SPF, DKIM, DMARC**: Review the results for these authentication mechanisms.

Step 4: Verify Sender Authenticity

1. **SPF Record Lookup**:
   - Use MXToolbox SPF Check to verify the SPF record of the sender’s domain.

2. **DKIM Record Lookup**:
   - Use MXToolbox DKIM Check to check the DKIM signature.
3. **DMARC Record Lookup**:
   - Use MXToolbox DMARC Check to verify the DMARC policy.

Step 5: URL Analysis (if applicable)

1. **Copy the URL from the Email**:
   - Identify and copy any URL from the email.
2. **Analyse the URL with VirusTotal**:
   - Go to VirusTotal.
   - Paste the URL and start the scan.
   - Review the results for any indications of malicious behaviour.
3. **Analyse the URL with URLscan.io**:
   - Go to URLscan.io.
   - Paste the URL and start the scan.
   - Review the results for suspicious activities or redirections.

Step 6: Attachment Analysis (if applicable)

1. **Save the Attachment**:
   - Save the attachment from the email.
2. **Upload the Attachment to a Sandbox**:
   - Use a service like VirusTotal or Joe Sandbox.
3. **VirusTotal Analysis**:
   - Go to VirusTotal and upload the attachment.
   - Review the scan results for any detection of malicious content.
4. **Joe Sandbox Analysis**:
   - Go to Joe Sandbox and upload the attachment.
   - Perform a full dynamic analysis to see the behaviour of the file when executed in a controlled environment.

Step 7: Remediation and Mitigation

1. **Immediate Actions**:
   - Delete the email and any attachments from all user mailboxes.

- Block the sender's domain if it is identified as malicious.
- Report any suspicious URLs or attachments to security vendors.

2. **Long-term Actions**:
    - Enhance email filtering rules to catch similar phishing attempts in the future.
    - Educate users on identifying phishing emails and suspicious attachments.
    - Implement multi-factor authentication for sensitive accounts.

Examples

Example 1: Email Withou Attachment

Step 1: Email Body Review

We have the email body and header as follows:

Email Body:

Dear User,

We have detected unusual activity in your account. Please verify your account immediately by clicking the link below:

<a href="http://malicious.com/verify">Verify Now</a>

Thank you,

Trusted Service Team

Email Header:

Received: from infected.com (192.168.1.2) by yourdomain.com with SMTP; Wed, 26 Jun 2024 10:30:00 -0400

From: "Trusted Service" <service@trusted.com>

To: victim@yourdomain.com

Subject: Urgent: Account Verification Required

Date: Wed, 26 Jun 2024 10:29:00 -0400

Reply-To: "Trusted Service" <noreply@trusted.com>

Message-ID: <001a1141f93d$7a0e8e00$5400a8c0@trusted.com>

Content-Type: text/html; charset="UTF-8"

MIME-Version: 1.0

Step 2: Analyse the Email Header with MXToolbox

Go to the MXToolbox Email Header Analyser.

1. Copy the entire email header.
2. Paste it into the header analysis tool and click "Analyse Header."

Analysis Results:

- **Received**: Look at each server the email passed through. Any unknown or suspicious servers should be noted.
- **From and Reply-To**: Ensure these fields are from legitimate sources. If they differ significantly, it’s a red flag.
- **SPF, DKIM, DMARC**: Check these fields in the analysis report.

Step 3: SPF, DKIM, and DMARC Records

Use MXToolbox to check the SPF, DKIM, and DMARC records:

- **SPF Record Lookup**: MXToolbox SPF Check
- **DKIM Record Lookup**: MXToolbox DKIM Check
- **DMARC Record Lookup**: MXToolbox DMARC Check

Results:

- **SPF**: Ensure that the Return-Path domain is authorized to send emails on behalf of the domain in the From field.
- **DKIM**: Verify the DKIM signature to ensure the email content has not been altered.
- **DMARC**: Check the domain’s DMARC policy to see how it handles authentication failures.

Step 4: URL Analysis with VirusTotal and URLscan.io

1. Copy the URL http://malicious.com/verify.
2. Go to VirusTotal.
3. Paste the URL and scan it.
4. Review the results for any indications of malicious behaviour.

Next, analyse the URL with URLscan.io:

1. Paste the URL into the search bar and start the scan.
2. Review the results for any suspicious activities or redirections.

Results from VirusTotal:

Scan Date: 2024-06-26

Detection Ratio: 28/72

Tags: Phishing, Malware

Detailed Report: https://www.virustotal.com/gui/url/malicious.com/details

Results from URLscan.io:

Scan Date: 2024-06-26

Analysis: The URL redirects to multiple suspicious sites.

Screenshot: Shows a fake login page mimicking Trusted Service.

Detailed Report: https://urlscan.io/result/malicious.com

Step 5: Email Header Analysis

Review the detailed results from MXToolbox:

- **Received**: The email passed through an unknown server infected.com.
- **Message-ID**: Does not match the sending domain, indicating potential spoofing.
- **Reply-To**: Mismatch between service@trusted.com and noreply@trusted.com.

Step 6: Remediation

- **Immediate Actions**:
  - Block the domain infected.com.
  - Report the URL malicious.com to security vendors.
  - Inform the user to ignore and delete the email.
- **Long-term Actions**:
  - Enhance email filtering rules to catch similar phishing attempts.
  - Educate users on identifying phishing emails.
  - Implement multi-factor authentication for sensitive accounts.

Example 2: Email With Attachment

Email Header:

Received: from unknownsender.com (203.0.113.5) by yourdomain.com with SMTP; Wed, 26 Jun 2024 10:30:00 -0400

From: "Customer Support" <support@knownservice.com>

To: employee@yourdomain.com

Subject: Important: Invoice Attached

Date: Wed, 26 Jun 2024 10:29:00 -0400

Reply-To: "Customer Support" <noreply@knownservice.com>

Message-ID: <001a1141f93d$7a0e8e00$5400a8c0@knownservice.com>

Content-Type: multipart/mixed; boundary="000000000000b0d39005e7e64f9a"

MIME-Version: 1.0

Email Body:

--000000000000b0d39005e7e64f9a

Content-Type: text/plain; charset="UTF-8"

Dear User,

Please find the attached invoice for your recent transaction. Contact us if you have any questions.

Thank you,

Customer Support Team

--000000000000b0d39005e7e64f9a

Content-Type: application/vnd.ms-excel; name="invoice.xls"

Content-Disposition: attachment; filename="invoice.xls"

Content-Transfer-Encoding: base64

```
<base64-encoded attachment>

--000000000000b0d39005e7e64f9a--
```

Step 1: Email Body Review

- **Check for URLs and Attachments**:
  - Attachment: invoice.xls
  - No URLs in this email.

Step 2: Download the Email

- Save the email in .eml format for detailed analysis.

Step 3: Open the Email Header

- Use tools like MXToolbox or a similar email header analyser.
  - MXToolbox Email Header Analyser

Step 4: Analyse SPF, DKIM, and DMARC

- **SPF**: Verify if the Return-Path domain matches the From domain.
  - Result: Potential spoof detected if they don't match.
- **DKIM**: Check the DKIM signature field.
  - Result: If the DKIM signature is missing or fails verification, the email might have been tampered with.
- **DMARC**: Evaluate DMARC policies.
  - Result: Check for none, quarantine, or reject policies.

Step 5: Email Header Analysis

- **Received**: Check the sequence of servers through which the email passed.
  - Result: Look for discrepancies or unknown servers.
- **Message-ID**: Unique identifier that should match the sending domain.

    - Result: Mismatch indicates potential spoofing.
- **Reply-To**: Ensure it aligns with the sender's domain.
    - Result: Discrepancy can indicate a phishing attempt.

Step 6: URL and Attachment Analysis

- **URLs**: Not applicable in this email.
- **Attachment Analysis**:
    - Save the attachment invoice.xls.
    - Use a sandbox environment to safely analyse the attachment.

Step 7: Analyse Attachment in Sandbox Environment

1. **Upload the Attachment to a Sandbox**:
    - Use a service like VirusTotal or Joe Sandbox.
2. **VirusTotal Analysis**:
    - Go to VirusTotal and upload invoice.xls.
    - Review the scan results for any detection of malicious content.
3. **Joe Sandbox Analysis**:
    - Go to Joe Sandbox and upload invoice.xls.
    - Perform a full dynamic analysis to see the behaviour of the file when executed in a controlled environment.

Results from VirusTotal:

Scan Date: 2024-06-26

Detection Ratio: 15/60

Tags: Malware, Trojan

Detailed Report: https://www.virustotal.com/gui/file/invoice.xls/details

Example Results from Joe Sandbox:

Analysis Date: 2024-06-26

Behaviour Analysis: The file attempts to download additional payloads from the internet.

Screenshots: Shows the file executing and connecting to suspicious IPs.

Detailed Report: https://www.joesecurity.org/report/invoice.xls

Step 8: Remediation and Mitigation

- **Immediate Actions**:
  - Delete the email and the attachment from all user mailboxes.
  - Block the sender's domain unknownsender.com.
  - Report the attachment invoice.xls to security vendors.
- **Long-term Actions**:
  - Enhance email filtering rules to catch similar phishing attempts.
  - Educate users on identifying phishing emails and suspicious attachments.
  - Implement multi-factor authentication for sensitive accounts.

Detailed Analysis:

Using MXToolbox to Analyse the Email Header:

1. Copy the email header.
2. Paste it into the MXToolbox Email Header Analyser and click "Analyse Header".

MXToolbox Results:

- **Received**: Shows that the email originated from 203.0.113.5, which is not a known server for knownservice.com.
- **SPF**: Fail - The IP address 203.0.113.5 is not authorized to send emails for knownservice.com.
- **DKIM**: Fail - The DKIM signature is either missing or invalid.
- **DMARC**: None - No DMARC policy is in place for knownservice.com.

Using VirusTotal to Analyze the Attachment:

1. Go to VirusTotal.
2. Upload the file invoice.xls.
3. Review the results.

VirusTotal Results:

File: invoice.xls

Detection Ratio: 15/60

- Microsoft: Trojan:Win32/Emotet

- Kaspersky: HEUR:Trojan.Win32.Generic

- McAfee: Excel/Phish-Gen

Detailed Report: https://www.virustotal.com/gui/file/invoice.xls/details

Using Joe Sandbox to Analyse the Attachment:

1. Go to Joe Sandbox.
2. Upload the file invoice.xls.
3. Perform a full dynamic analysis.

Joe Sandbox Results:

File: invoice.xls

Behaviour Analysis: The file attempts to execute a macro that downloads additional payloads from the internet.

Screenshots: Shows the macro execution and network connections to suspicious IPs.

Detailed Report: https://www.joesecurity.org/report/invoice.xls

Scenario

A company receives multiple emails from what appears to be a well-known supplier, requesting immediate action to pay an outstanding invoice. This phishing campaign targets the finance department and aims to trick employees into transferring money to a fraudulent account.

Email Header:

Received: from suppliers.com (192.168.10.10) by yourdomain.com with SMTP; Wed, 26 Jun 2024 10:30:00 -0400

From: "Billing Department" <billing@supplier.com>

To: finance@yourdomain.com

Subject: Urgent: Overdue Invoice Payment Required

Date: Wed, 26 Jun 2024 10:29:00 -0400

Reply-To: "Billing Department" <noreply@supplier.com>

Message-ID: <001a1141f93d$7a0e8e00$5400a8c0@supplier.com>

Content-Type: multipart/mixed; boundary="000000000000b0d39005e7e64f9a"

MIME-Version: 1.0

Email Body:

--000000000000b0d39005e7e64f9a

Content-Type: text/plain; charset="UTF-8"

Dear Finance Team,

This is a reminder that invoice #45678 remains unpaid and is now overdue. Please see the attached document for details and remit payment as soon as possible to avoid any late fees.

If you have already made this payment, please disregard this message.

Thank you for your prompt attention to this matter.

Best regards,

Billing Department

Supplier Inc.

--000000000000b0d39005e7e64f9a

Content-Type: application/pdf; name="invoice_45678.pdf"

Content-Disposition: attachment; filename="invoice_45678.pdf"

Content-Transfer-Encoding: base64

<base64-encoded attachment>

--000000000000b0d39005e7e64f9a--

Step 1: Initial Email Body Review

- **Check for URLs and Attachments**:
  - Attachment: invoice_45678.pdf
  - No URLs in this email body.

Step 2: Download and Save the Email

- Save the email in .eml format for detailed analysis.

Step 3: Open the Email Header

- Use tools like MXToolbox or a similar email header analyser.
  - MXToolbox Email Header Analyser

Step 4: Analyse SPF, DKIM, and DMARC

- **SPF**: Verify if the Return-Path domain matches the From domain.
  - Result: Potential spoof detected if they don't match.

- **DKIM**: Check the DKIM signature field.
    - Result: If the DKIM signature is missing or fails verification, the email might have been tampered with.
- **DMARC**: Evaluate DMARC policies.
    - Result: Check for none, quarantine, or reject policies.

Step 5: Email Header Analysis

- **Received**: Check the sequence of servers through which the email passed.
    - Result: Look for discrepancies or unknown servers.
- **Message-ID**: Unique identifier that should match the sending domain.
    - Result: Mismatch indicates potential spoofing.
- **Reply-To**: Ensure it aligns with the sender's domain.
    - Result: Discrepancy can indicate a phishing attempt.

Step 6: URL and Attachment Analysis

- **URLs**: Not applicable in this email.
- **Attachment Analysis**:
    - Save the attachment invoice_45678.pdf.
    - Use a sandbox environment to safely analyse the attachment.

Step 7: Analyse Attachment in Sandbox Environment

1. **Upload the Attachment to a Sandbox**:
    - Use a service like VirusTotal or Joe Sandbox.
2. **VirusTotal Analysis**:
    - Go to VirusTotal and upload invoice_45678.pdf.
    - Review the scan results for any detection of malicious content.
3. **Joe Sandbox Analysis**:
    - Go to Joe Sandbox and upload invoice_45678.pdf.
    - Perform a full dynamic analysis to see the behaviour of the file when executed in a controlled environment.

Results from VirusTotal:

Scan Date: 2024-06-26

Detection Ratio: 10/60

Tags: Phishing, Trojan

Detailed Report: https://www.virustotal.com/gui/file/invoice_45678.pdf/details

Example Results from Joe Sandbox:

Analysis Date: 2024-06-26

Behaviour Analysis: The file attempts to download additional payloads from the internet when opened.

Screenshots: Shows the file displaying a fake invoice and network connections to suspicious IPs.

Detailed Report: https://www.joesecurity.org/report/invoice_45678.pdf

Detailed Analysis:

Using MXToolbox to Analyse the Email Header:

1. Copy the email header.
2. Paste it into the MXToolbox Email Header Analyser and click "Analyse Header".

MXToolbox Results:

- **Received**: Shows that the email originated from 192.168.10.10, which is not a known server for supplier.com.
- **SPF**: Fail - The IP address 192.168.10.10 is not authorized to send emails for supplier.com.
- **DKIM**: Fail - The DKIM signature is either missing or invalid.
- **DMARC**: None - No DMARC policy is in place for supplier.com.

Using VirusTotal to Analyse the Attachment:

1. Go to VirusTotal.
2. Upload the file invoice_45678.pdf.
3. Review the results.

VirusTotal Results:

File: invoice_45678.pdf

Detection Ratio: 10/60

- Microsoft: TrojanDownloader:PDF/Phish.gen

- Kaspersky: HEUR:Trojan.PDF.Generic

- McAfee: PDF/Phish-Gen

Detailed Report: https://www.virustotal.com/gui/file/invoice_45678.pdf/details

Using Joe Sandbox to Analyse the Attachment:

1. Go to Joe Sandbox.
2. Upload the file invoice_45678.pdf.
3. Perform a full dynamic analysis.

Joe Sandbox Results:

File: invoice_45678.pdf

Behaviour Analysis: The file attempts to execute a script that downloads additional payloads from the internet.

Screenshots: Shows the script execution and network connections to suspicious IPs.

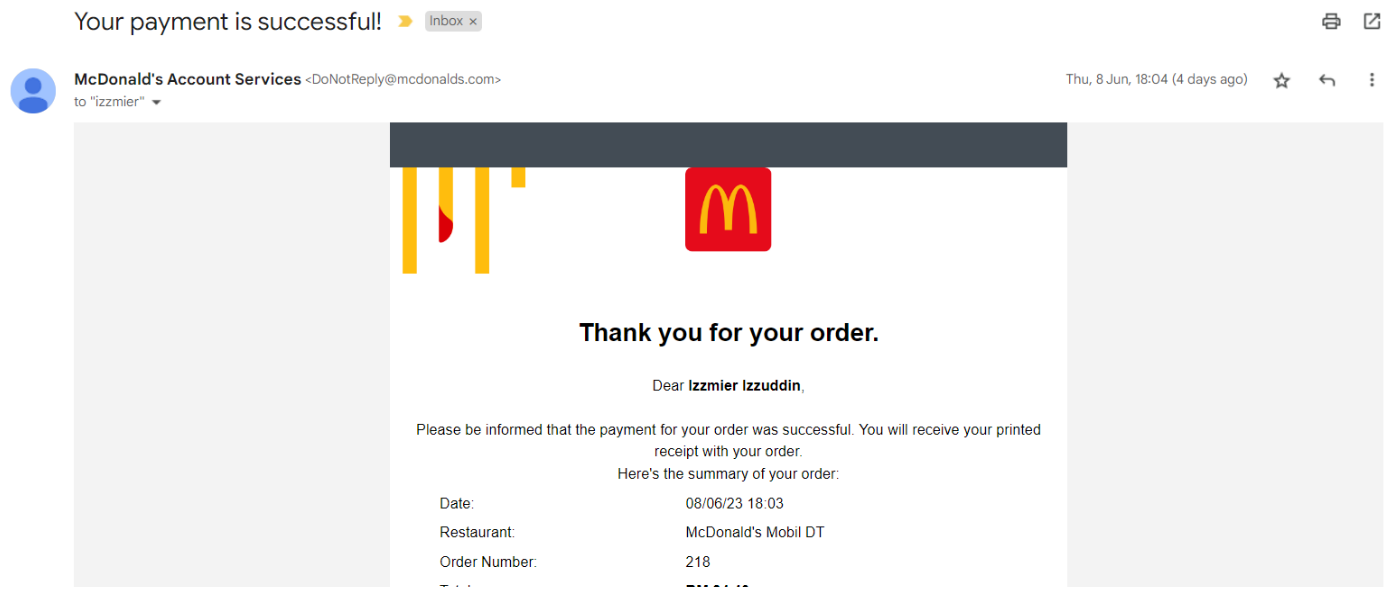
Detailed Report: https://www.joesecurity.org/report/invoice_45678.pdf

Remediation and Mitigation

- **Immediate Actions**:
  - Delete the email and the attachment from all user mailboxes.
  - Block the sender's domain unknownsender.com.
  - Report the attachment invoice_45678.pdf to security vendors.
- **Long-term Actions**:
  - Enhance email filtering rules to catch similar phishing attempts.
  - Educate users on identifying phishing emails and suspicious attachments.
  - Implement multi-factor authentication for sensitive accounts.

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]



Your payment is successful!

McDonald's Account Services <DoNotReply@mcdonalds.com>
to "izzmier"

Thu, 8 Jun, 18:04 (4 days ago)

Thank you for your order.

Dear **Izzmier Izzuddin**,

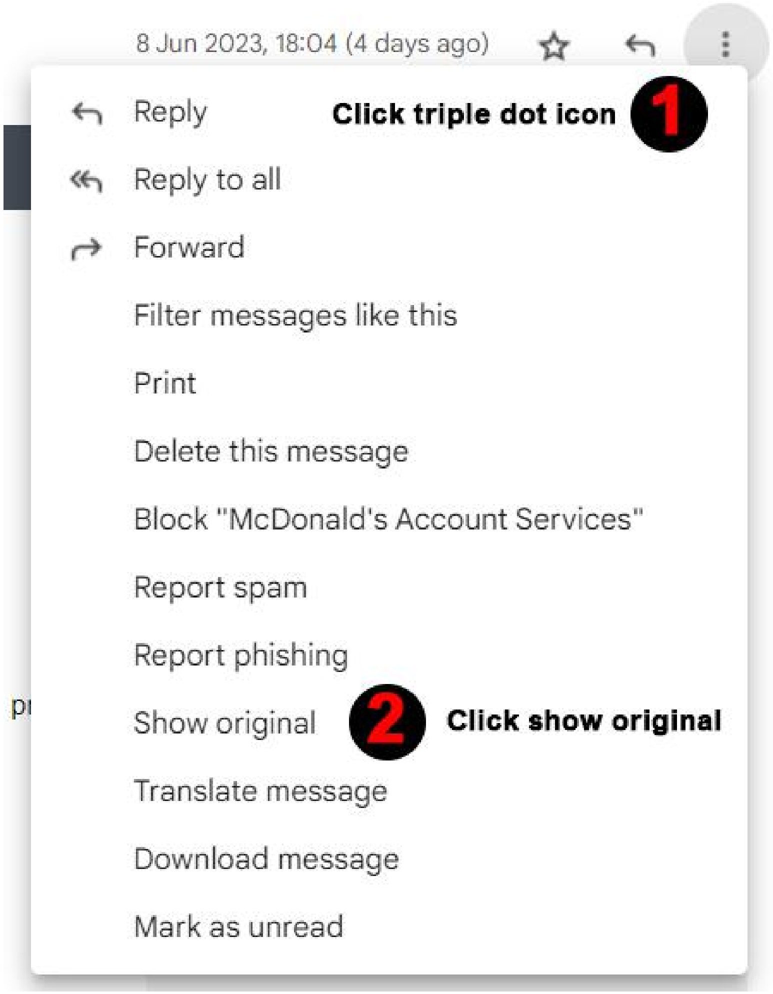
Please be informed that the payment for your order was successful. You will receive your printed receipt with your order.
Here's the summary of your order:

Date:	08/06/23 18:03
Restaurant:	McDonald's Mobil DT
Order Number:	218

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.

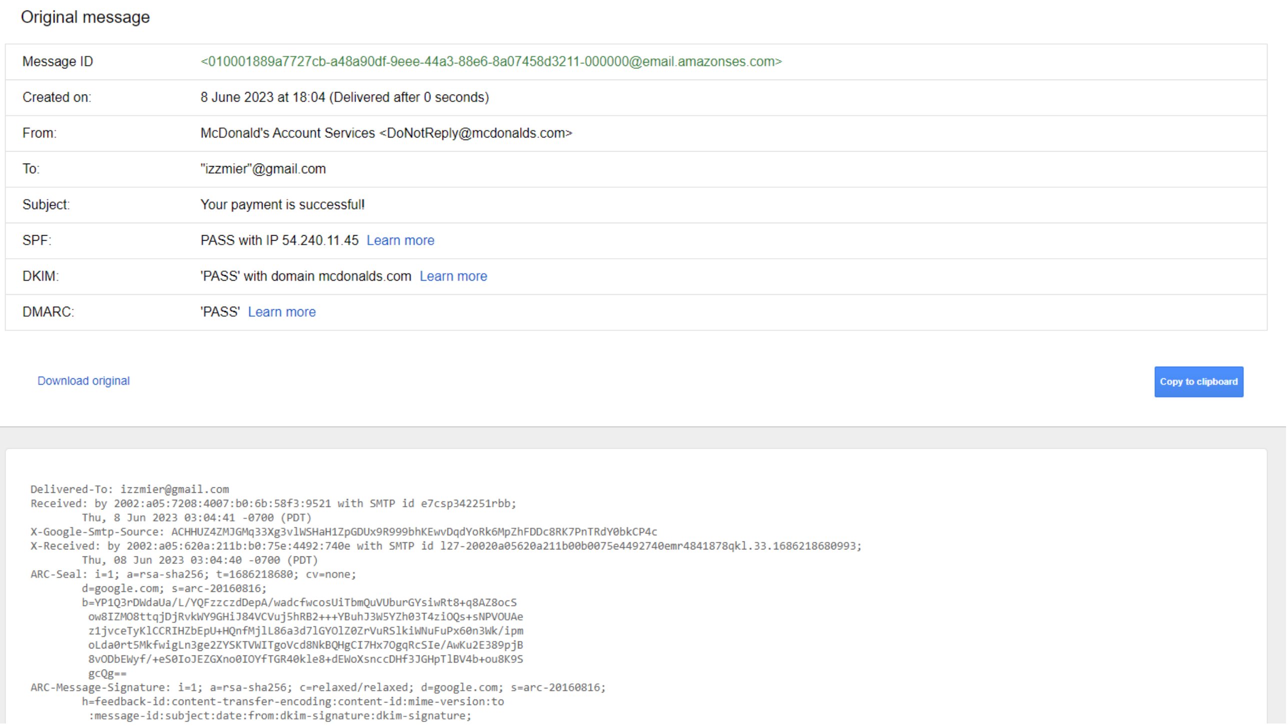


Click triple dot icon 1

2 Click show original

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

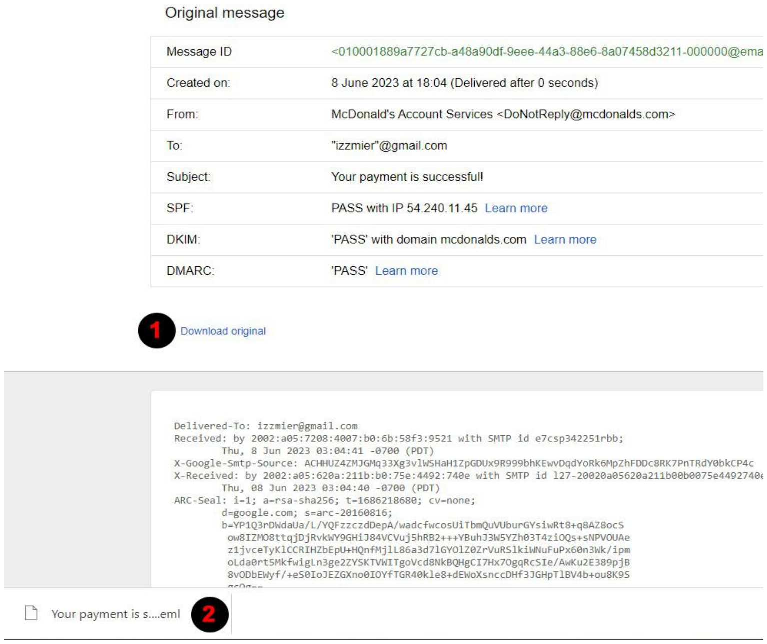


Original message

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

```
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



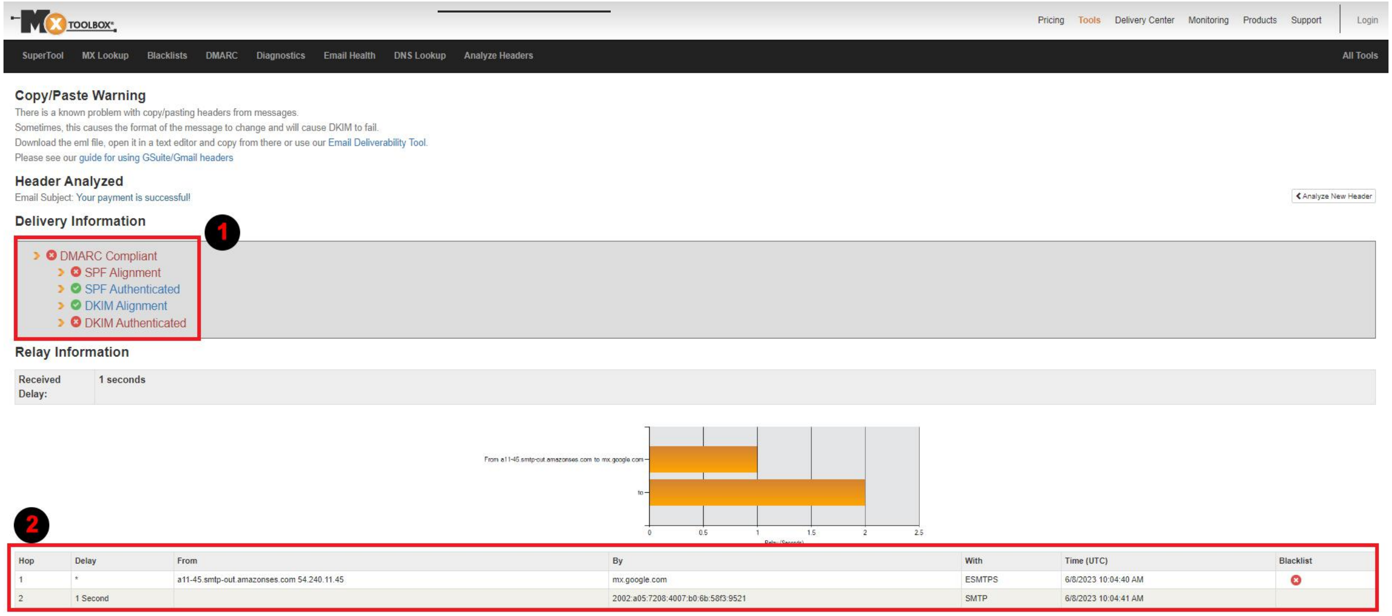
Original message

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

```
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
```

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

Header analysis is done on MxtoolBox



Copy/Paste Warning

There is a known problem with copy/pasting headers from messages.
Sometimes, this causes the format of the message to change and will cause DKIM to fail.
Download the eml file, open it in a text editor and copy from there or use our Email Deliverability Tool.
Please see our guide for using GSuite/Gmail headers

Header Analyzed

Email Subject: Your payment is successful!

Delivery Information

- ☒ DMARC Compliant
  - ☒ SPF Alignment
  - ✓ SPF Authenticated
  - ✓ DKIM Alignment
  - ☒ DKIM Authenticated

Relay Information

Received Delay:	1 seconds

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	a11-45.smtp-out.amazonses.com 54.240.11.45	mx.google.com	ESMTPS	6/8/2023 10:04:40 AM	☒
2	1 Second		2002:a05:7208:4007:b0:6b:58f3:9521	SMTP	6/8/2023 10:04:41 AM	

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 IDvalue 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.

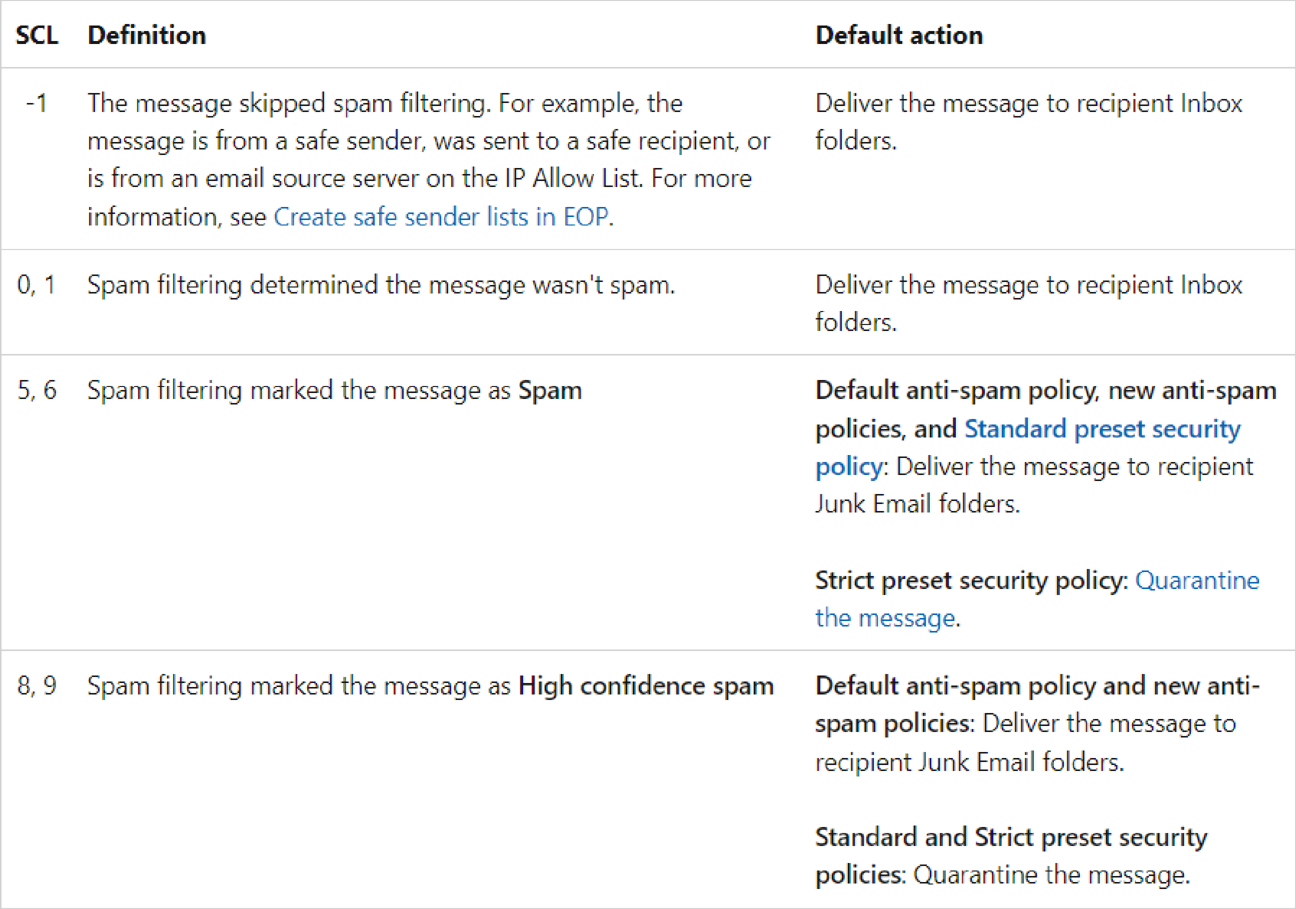
· quarantine — Deliver the message to junk or spam.

· reject — Reject and bounce the message.

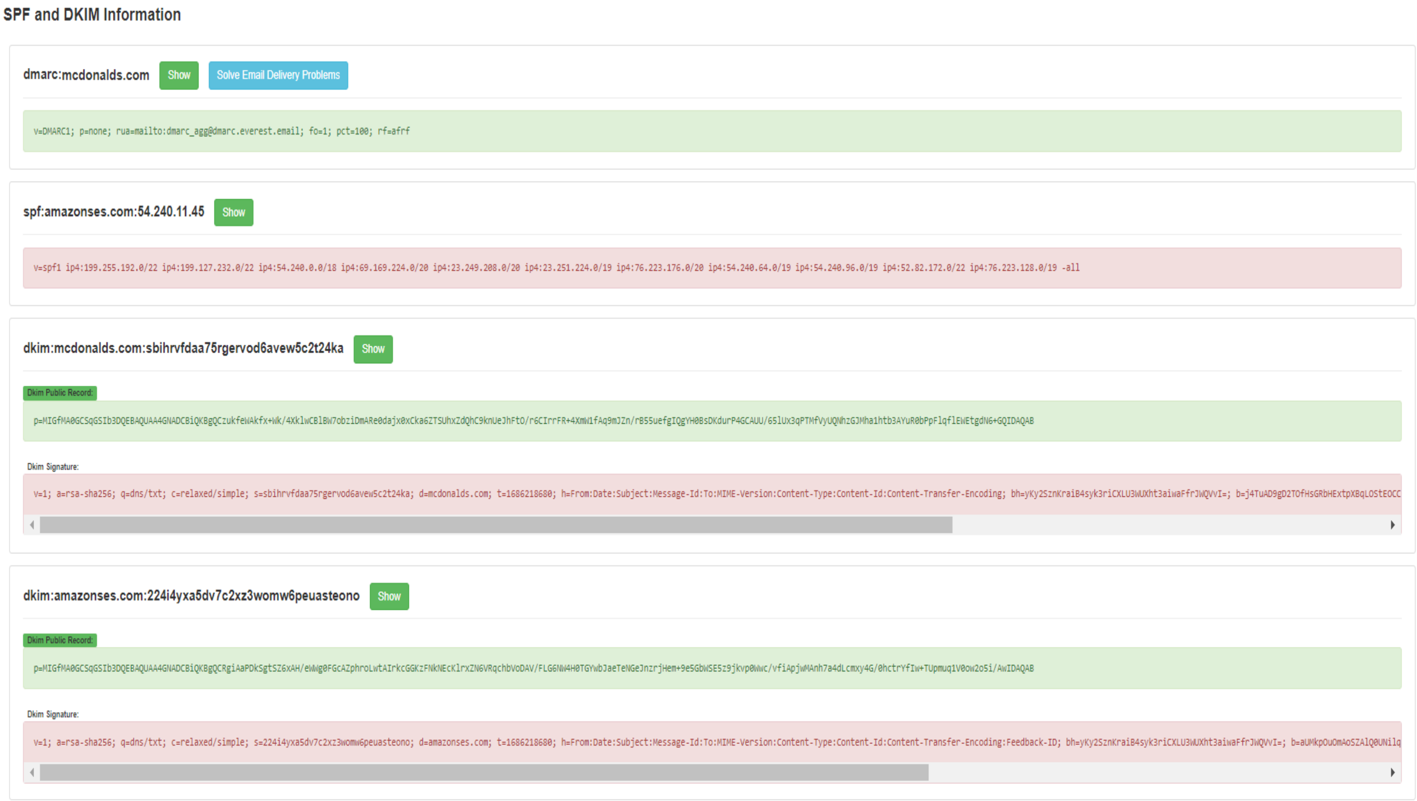
DMARC also provides a reporting mechanism. You can specify a server endpoint that receiving mail servers will call when they get an email purporting to be from your domain. This gives you a cross-internet view of the servers that are sending as your domain.

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

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

spf:amazonses.com:54.240.11.45

```
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

Dkim Public Record:

```
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCzukfeWAkfx+Wk/4XklwCBlBW7obziDmARe0dajx0xCka6ZTSUhxZdQhC9knUeJhFtO/r6CIrrFR+4XmW1fAq9mJZn/rB55uefgIQgYH0BsDKdurP4GCAUU/65lUx3qPTMfVyUQNhzGJMha1htb3AYuR0bPpFlqflEWEtgdN6+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
```

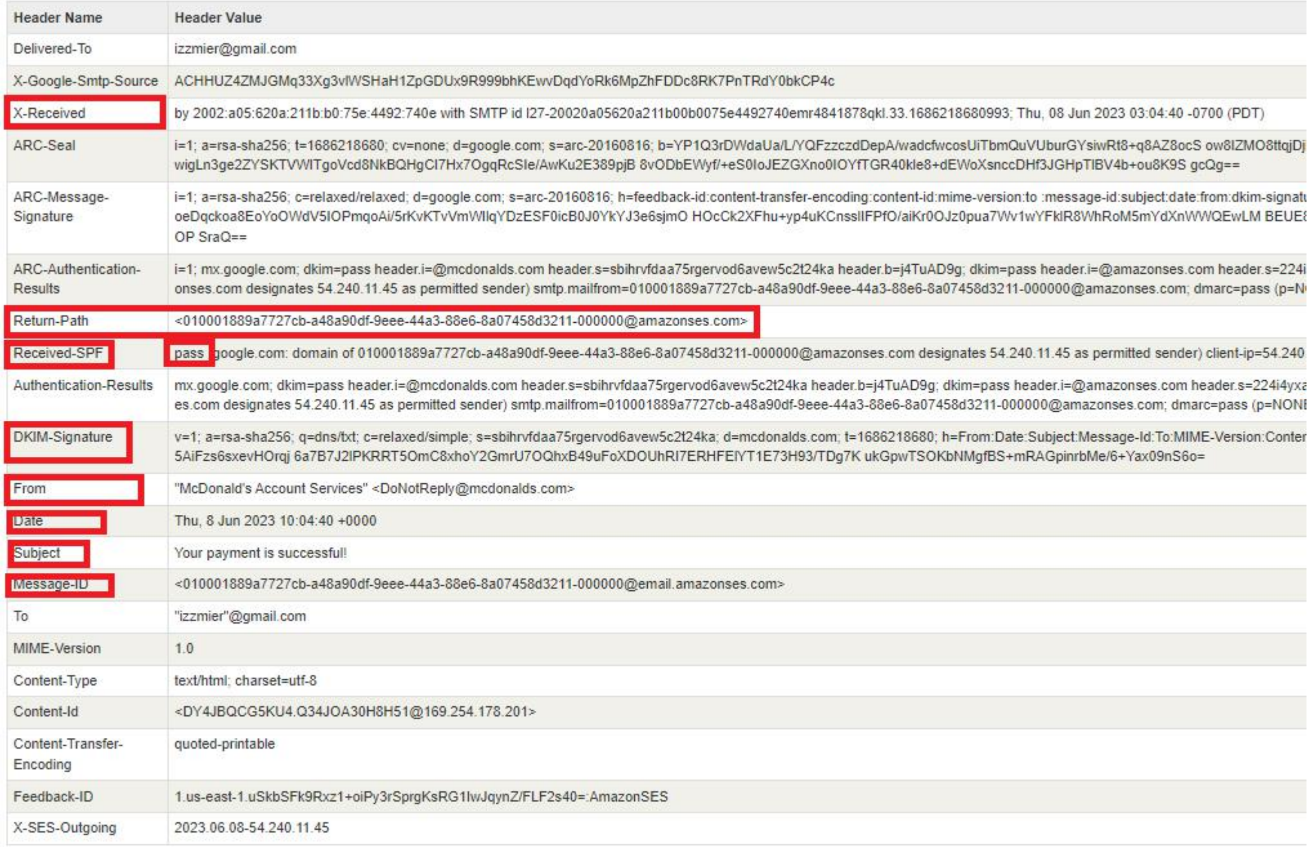
dkim:amazonses.com:224i4yxa5dv7c2xz3womw6peuasteono

Dkim Public Record:

```
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCRgiAaPDkSgtSZ6xAH/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 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 ow8IZMO8ttqjDj wigLn3ge2ZYSKTVWITgoVcd8NkBQHgCl7Hx7OgqRcSle/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-signatu oeDqckoa8EoYoOWdV5IOPmqoAi/5rKvKTvVmWIlqYDzESF0icB0J0YkYJ3e6sjmO HOcCk2XFhu+yp4uKCnssllFPfO/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 6a7B7J2lPKRRT5OmC8xhoY2GmrU7OQhxB49uFoXDOUhRI7ERHFEIYT1E73H93/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+oiPy3rSprgKsRG1lwJqynZ/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.

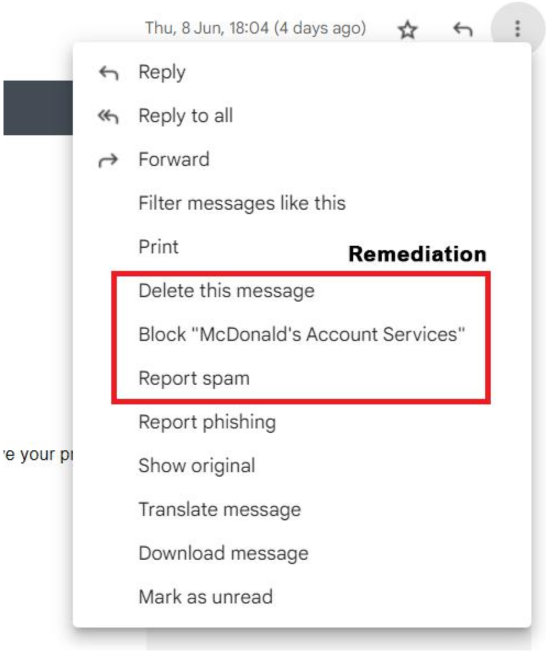
· Educate the mail service provider (eg- gmail) or tool used within corporate environment by reporting it as either phishing or spam based on your findings.

· 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.


Remediation

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 withinthe environment helps the organization evaluate employees' understanding about phishing attacks.