

Phishing Email Analysis

Email Header Analysis

STEP 1: Go through how the email body looks

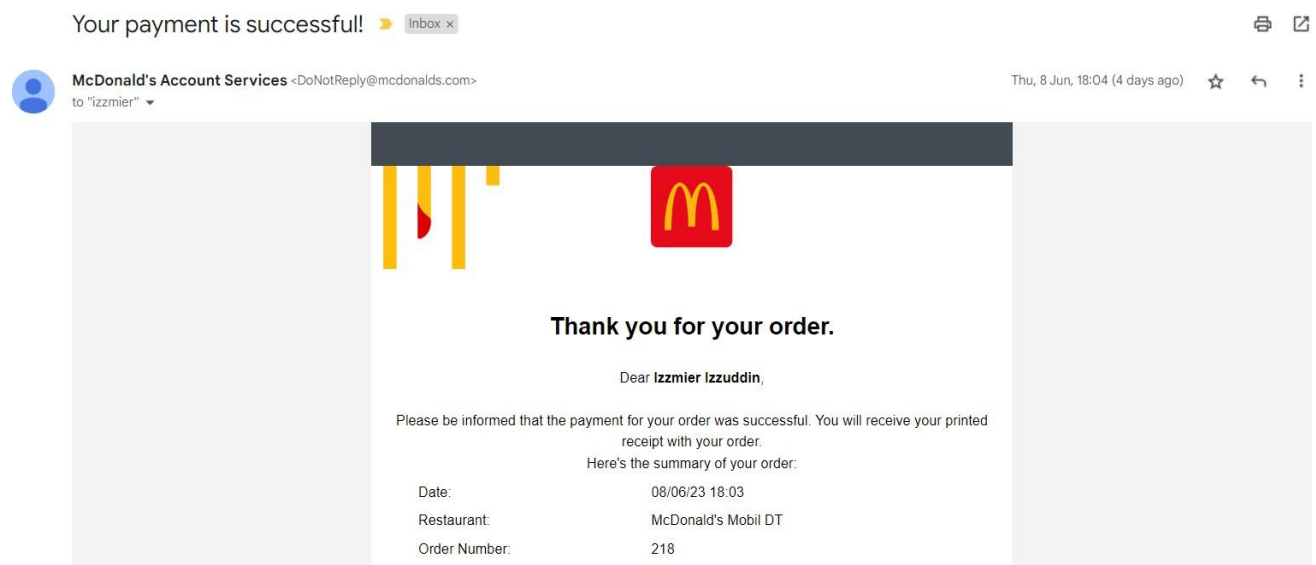
If there are URLs and Attachments, you will need to test them in a sandbox environment (Virtual Machine).

Sandbox Environment — (static & dynamic analysis):

To test the links/attachments in sandbox environment, make use of:

- Virus Total (URL reputation check / file hash check)
- Urlscan.io
- Whois
- Domaintools
- HavelBeenPwned
- Google dorks
- AnyRun

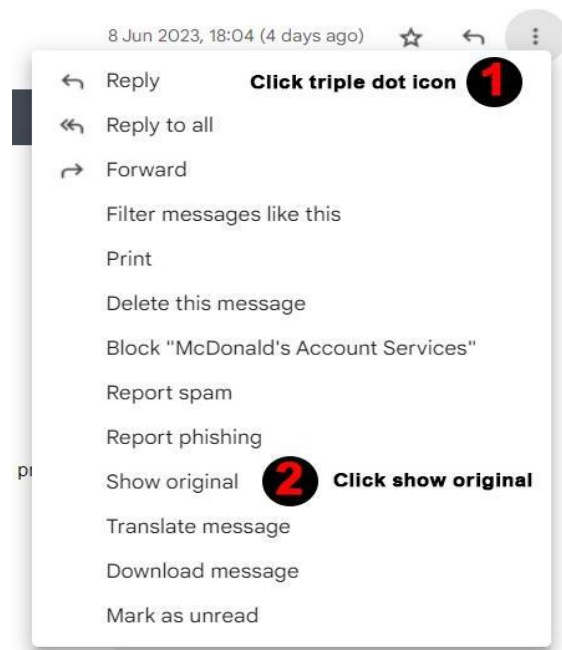
You can also use **other OSINT tools** for analysing the links/attachments.



STEP 2: Download the email in .eml format

Go to Gmail → click “three dots” on email → Show original → then:

- Click “Download Original” (to get .eml file)
- OR click “Copy to Clipboard” (and paste it in email header analyzer tool)



STEP 3: Download the Email Header for Analysis

You will be greeted with the Original Message page.

From here, you can either:

- Click “Download Original” to download the email in .eml format for offline header analysis,
OR
- Click “Copy to Clipboard” to directly copy the full header and paste it into any email header analyzer tool for online analysis.

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 successfull |
| 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: ACH4U24ZJ7Gq433Xg3v1kShAH12pGDUxSR999bhKEwDqdyoRk0npZHFDDC8RK7PnTrdY0bkCP4c
X-Received: by 2002:a05:620a:211b:b0:75e:4492:740e with SMTP id 127-2002a05620a211b00b0075e4492740emr4841878qk1.33.168621868993;
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=VP1Q3rDndalla/L/VQFzccDdpA/wadcfwcosU1TbmQuVuburGYslwRt8+qBAZ8oc5
ow8IZN08ttgDjRvkvY9GHIJ84VCVuj5HRB2+++YBUh33W5Y2h03T4z10Qs+sNPVOUae
z1jvceTyK1CCR1H2bEpU+HqnfHj1L86a3d71GVO120ZrVvRS1k1WuFuPx60n3Mk/1pm
oLda0rt5MkFw1gLn3geZy5KtVwITgoVcd8Nk8QhgCI7Hx70gqRc51e/AwKu2E389pJ8
8v0DBElyf/+eS0toE2GkNo0IOYfT6R40k1e8+dEwXsncDHF3JGhpT1BV4b+ou8K9S
8f0g==
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 Message

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 successfull |
| SPF: | PASS with IP 54.240.11.45 Learn more |
| DKIM: | 'PASS' with domain mcdonalds.com Learn more |
| DMARC: | 'PASS' Learn more |

 [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: ACH4U24ZJ7Gq433Xg3v1kShAH12pGDUxSR999bhKEwDqdyoRk0npZHFDDC8RK7PnTrdY0bkCP4c
X-Received: by 2002:a05:620a:211b:b0:75e:4492:740e with SMTP id 127-2002a05620a211b00b0075e4492740emr4841878qk1.33.168621868993;
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=VP1Q3rDndalla/L/VQFzccDdpA/wadcfwcosU1TbmQuVuburGYslwRt8+qBAZ8oc5
ow8IZN08ttgDjRvkvY9GHIJ84VCVuj5HRB2+++YBUh33W5Y2h03T4z10Qs+sNPVOUae
z1jvceTyK1CCR1H2bEpU+HqnfHj1L86a3d71GVO120ZrVvRS1k1WuFuPx60n3Mk/1pm
oLda0rt5MkFw1gLn3geZy5KtVwITgoVcd8Nk8QhgCI7Hx70gqRc51e/AwKu2E389pJ8
8v0DBElyf/+eS0toE2GkNo0IOYfT6R40k1e8+dEwXsncDHF3JGhpT1BV4b+ou8K9S
8f0g==

 Your payment is s....eml



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

Use **MXToolbox** to analyze the email header.

Check if the following pass:

- SPF Alignment
- SPF Authentication
- DKIM Alignment
- DKIM Authentication

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

From pt11-45.smtp-out.amazonses.com to mx.google.com

| Hop | Delay | From | By | With | Time (UTC) | Blacklist |
|-----|----------|---|------------------------------------|--------|----------------------|-----------|
| 1 | - | pt11-45.smtp-out.amazonses.com 54.240.11.45 | mx.google.com | ESMTPS | 6/5/2023 10:04:40 AM | |
| 2 | 1 Second | | 2902 a05.7208.4007 60.66.5853 9521 | SMTP | 6/5/2023 10:04:41 AM | |

How to Detect Spoofing

1. Click the three dots (:) on the email → Select **"Show original"**
2. Check the **Message ID** and **From address**
 - If they are different, the email might be spoofed

SPF & DKIM Checks

- **SPF Alignment:**
Passes only if the **Return-Path domain matches the From domain**
If they differ, it could be a spoof

- **SPF Authentication:**
Fails if the sender's IP address is **not authorized** to send on behalf of the domain
- **DKIM Alignment:**
Compare the d= value in the DKIM signature with the From domain
If they don't match, alignment fails
- **DKIM Authentication:**
If the b= signature value is not verified, the email might be modified or fake

What Is SPF, DKIM, and DMARC?

- **SPF (Sender Policy Framework):**
Defines which IPs can send email from a domain
Example: v=spf1 ip4:123.123.123.123 ~all
 - ~all = soft fail
 - -all = hard fail
- **DKIM (DomainKeys Identified Mail):**
Uses a digital signature to confirm the email was not changed and is from the stated domain
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance):**
Tells the receiver what to do if SPF or DKIM checks fail
DMARC policy examples:
 - none – deliver the message
 - quarantine – send to spam
 - reject – block or bounce the message
 Example DMARC record:
v=DMARC1; p=none; rua=mailto:user@example.com

SCL & BCL Scores

- **SCL (Spam Confidence Level):**
Indicates how likely a message is to be spam
(Can be checked via mail flow rules)
- **BCL (Bulk Complaint Level):**
Measures how likely a message is considered graymail (e.g., marketing emails)
Higher BCL scores suggest more chance of user complaints

| 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. |

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

v=DHARC1; p=none; rua=mailto:dmarc_agg@dmarc.everest.email; fo=1; pct=100; rf=afr

spf:amazonses.com:54.240.11.45 [Show](#)

```
vrsfpl ip4:199.255.192.0/22 ip4:199.127.232.0/22 ip4:54.240.0.0/10 ip4:69.169.224.0/20 ip4:23.249.200.0/20 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

[View Public Record](#)

Okim Signature:

```
wiki; mrsa-sh256; qdm/tot; curland/simple; s6sbvrfds7grgoaswesc2t4ay; dmcDonalds.com; ts168212880; h=FromDate:Subject:Message-ID:To:POB-Version:Content-Type:Content-ID:Content-Transfer-Encoding; bhyqyZcnral8aykr1CXL0080tJ6seFr3qivz; byJ4U06Q270F9B9d6tp0q;05E0C0
```

dkim:amazonses.com:224i4yxa5dv7c2xz3womw6peuasteono [Show](#)

[Data Privacy Notice](#)

Dkim Signature:

url: a=s-a-sha256; q=0/mt; c=relaxed/singles; s=22414yx867/c2x3hewdpeasteno; d=amazon.com; t=168612888; h=From:Date-Subject:Message-Id-to:MD5-Version:Content-Type:Content-Id:Content-Transfer-Encoding-Feedback-Id; b=lyqjZ53nra18qKjP1C1uX1a0t3a1wF7RqWq; b=akqkQoWmsD2qkU11

Breaking Down an Email (Header-wise)

Important headers:

- Thrishank Reddy

- **Received:** Details of mail servers email passed through
- **Received-SPF:** SPF status (pass/fail)
- **Delivered-To:** Final recipient address

Additional headers:

- **ARC-Seal**
- **ARC-Message-Signature**
- **ARC-Authentication-Results**
(Used when intermediaries forward the email)

STEP 5: Email Body Analysis

Check:

- **Subject**
- **Sender**
- **Sender Domain**
- **Recipient**
- **Recipient Domain**
- **Network Message ID**
- **Original & Latest delivery**

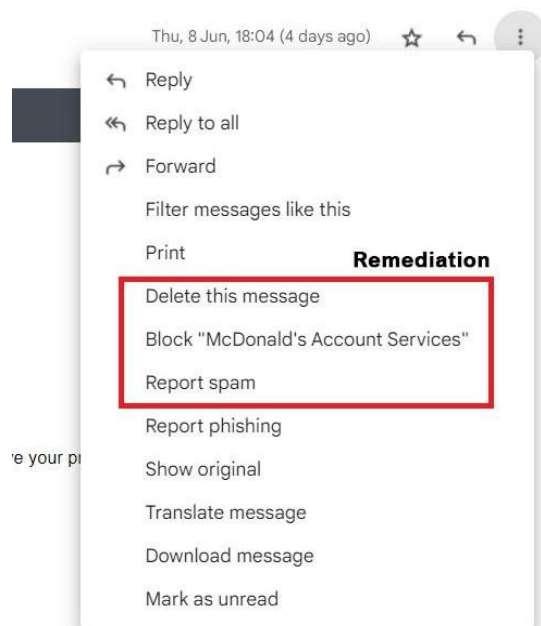
Analyze:

- The **tone** of the email
- Look for embedded **URLs** or **Attachments**
- Right-click and copy links/files — **do not click**
- Use sandbox/VirusTotal for scanning
- Use Inspect Element > Network tab to monitor redirects

STEP 6: Remediation/Mitigation

If email is found malicious:

- Enable **MFA** on user accounts
- **Purge email** from all mailboxes
- **Report** the email as Phishing/Spam
- Notify your email service provider or IT team
- **Block URLs/domains** if malicious
- Submit decommission request for base/redirect URLs
- Check how many users **clicked** the link/file
- If clicked, **reset credentials** for those users



STEP 7: User Awareness / Phishing Simulation

- Design **awareness banners, brochures**
- Schedule **phishing simulation events**
- Evaluate employee responses
- Educate on how to identify and report phishing