Leonard M. Estos
Cybersecurity Researcher & Technical Author
Edmonton, Alberta, Canada

Project Name: Microsoft Defender Email Forensic Investigation

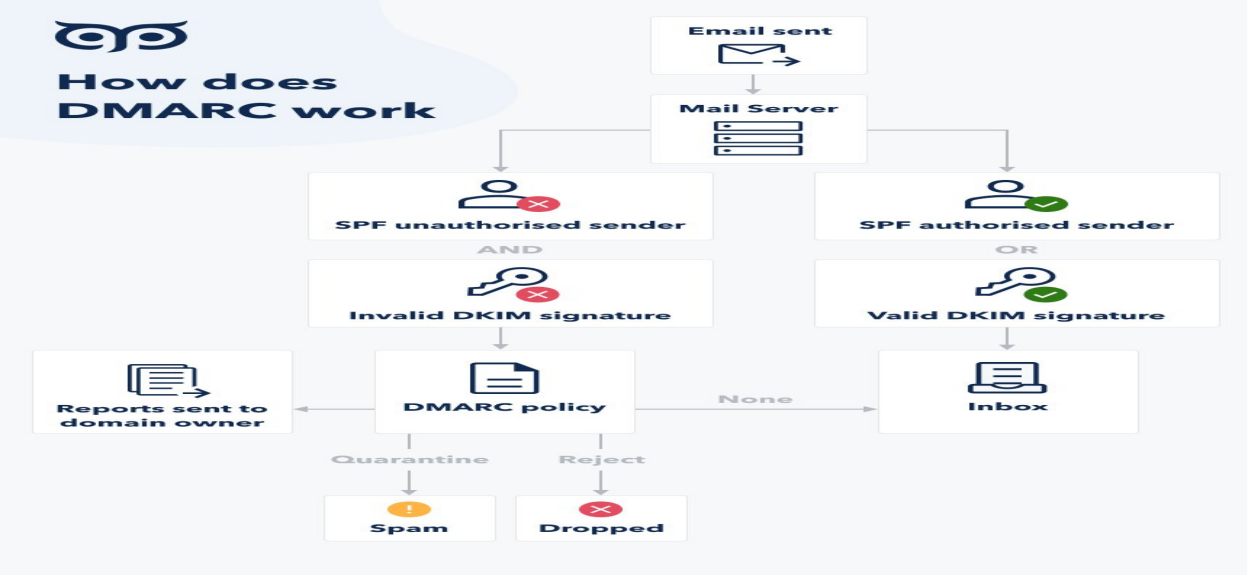
Project Overview: This documentation provides a comprehensive guide to email headers - the metadata-rich component of email communication that plays a critical role in cybersecurity, forensic analysis, and troubleshooting. It is designed to help technical professionals, SOC analysts, and IT administrators understand what email headers are, how to interpret them, and how to use them effectively in threat detection and incident response.

- **Educate** readers on the anatomy and function of email headers in digital communication.
- **Equip** cybersecurity practitioners with practical techniques to analyze headers for phishing, spoofing, and spam detection.
- **Demystify** header fields and their relevance to email authentication protocols (SPF, DKIM, DMARC).
- **Support** incident response workflows by enabling accurate source tracing and timeline reconstruction.
- **Promote** best practices for email header analysis using open-source tools and manual inspection.

The content is structured into three core sections:

1. **What is an Email Header** – A foundational explanation of email header structure and purpose.
2. **How to Analyze an Email Header** – Step-by-step guidance on parsing headers for source verification, relay tracing, and threat indicators.
3. **What an Email Header Contains** – A breakdown of key fields such as *Received*, *From*, *Return-Path*, *Message-ID*, *DKIM*, *SPF*, and *X-* custom headers.

Email Model:



SPF (Sender Policy Framework):

SPF is a DNS record that lists the authorized mail servers for a domain.

DKIM (DomainKeys Identified Mail):

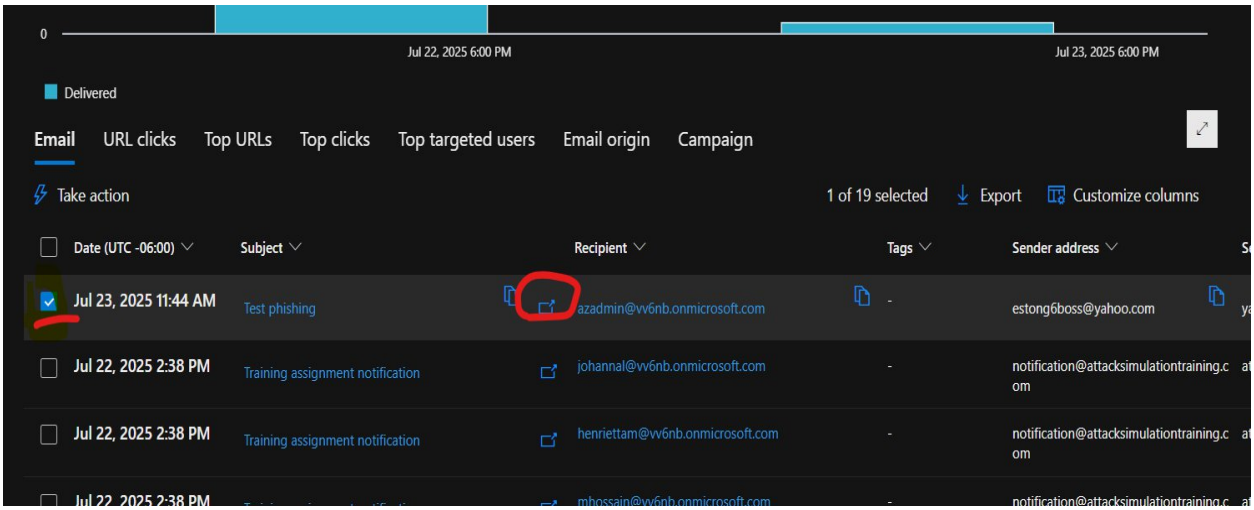
DKIM adds a digital signature to email headers. This signature is verified using a public key published in the sending domain's DNS records.

DMARC (Domain-based Message Authentication, Reporting & Conformance):

DMARC builds upon SPF and DKIM. It allows domain owners to specify what to do with emails that fail SPF and/or DKIM checks, such as rejecting or quarantining them. DMARC also provides reporting mechanisms to help domain owners monitor email authentication attempts and identify potential abuse.

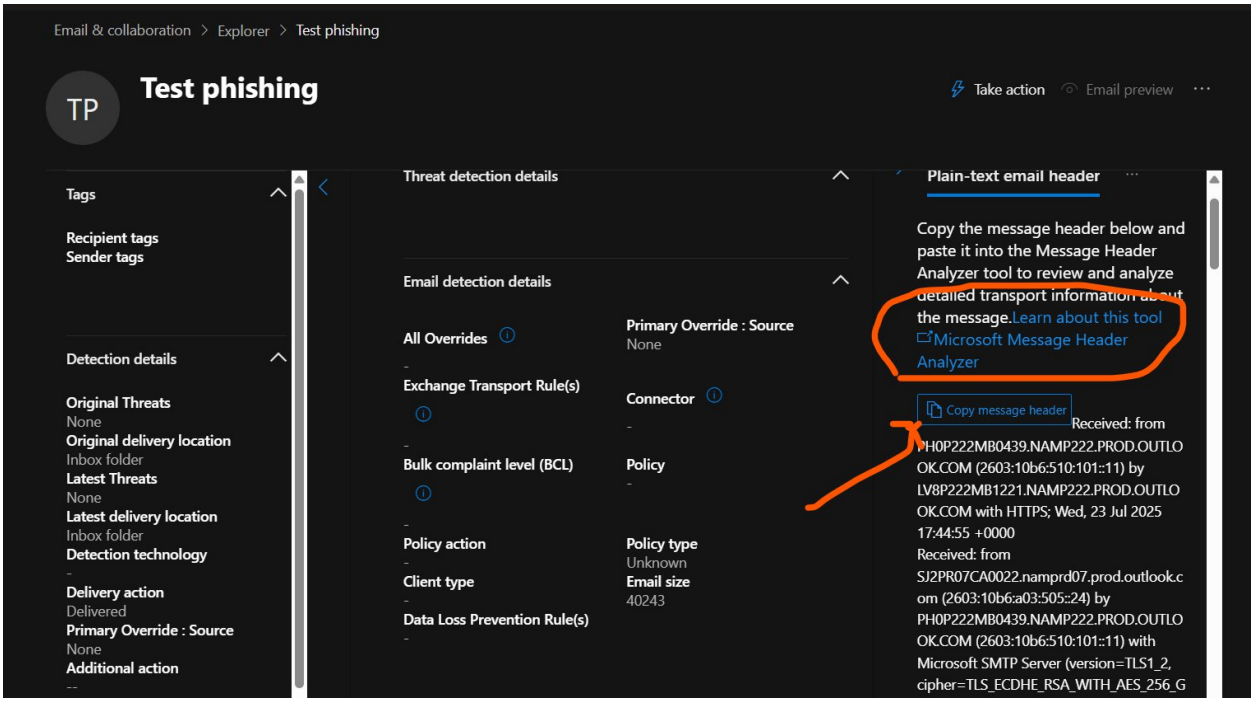
How to Analyst the Email for, Fishing, SPAM and Malware:

1. In the Microsoft Defender create your policy. See E:\Ogz\CyberSecurity\01_HowTo\1_Documentation\101_Cloud_MicrosoftAzure_EntraID_Intune\Microsoft_Defender file **TheMicrosoftDefender**
2. In **Microsoft Defender go to > Email & Collaboration > Explorer > All email > In Email** below check the email that you will investigate.
3. Tick the email and Open in the new Window.



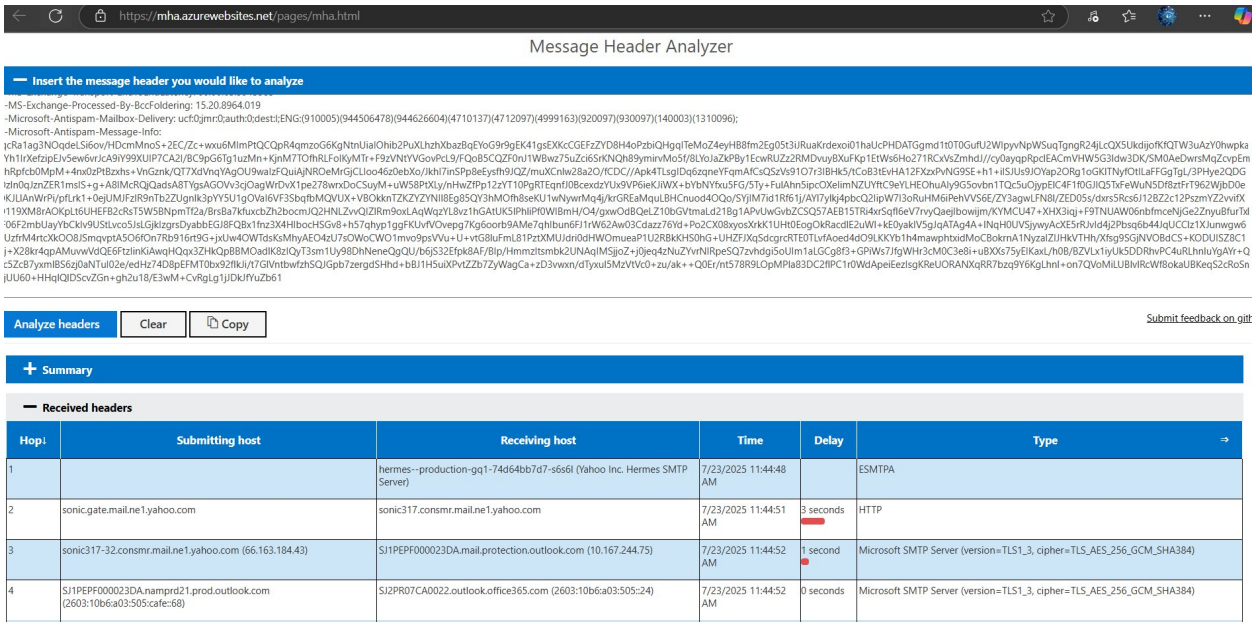
4. It will open the **New Window** for more gathering information's like the Timeline, Analysis, Attachments, URL, etc.

5. Click Analysis > Click the **Microsoft Message Header Analyzer** (it will open the new Window for Message Header Analyszer) and copy the message header.

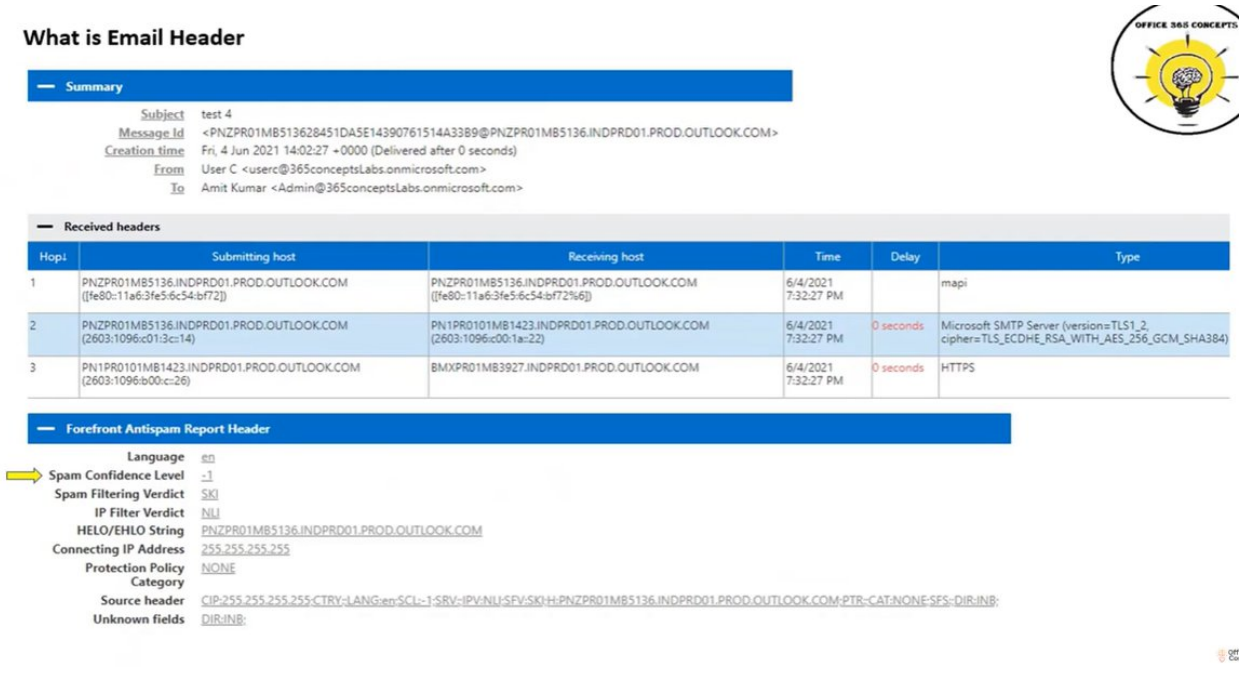


6. Copy the message Header and paste this to **Message Header Analyzer**:

   https://mha.azurewebsites.net/



The higher the SPAM confidence Level this will considered as SPAM or **SPM**

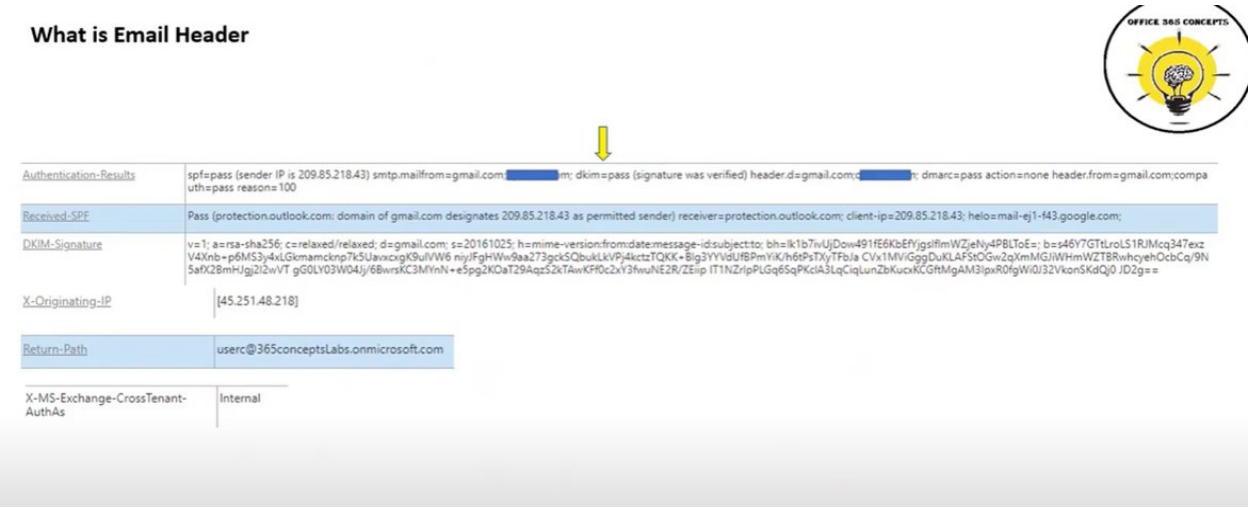


7. Use Mx Analyzer for more details = https://mxtoolbox.com/EmailHeaders.aspx
8. Note that the email will be legit if it passes the **spf, dkim and dmarc** process.

Unknown fields: DLR:INB;

AntiSpamReport
Bulk Complaint Level: 0
Source header: BCL:0;ARA:13230040|7093399015|4102299003|43540500003;
Unknown fields: ARA:13230040|7093399015|4102299003|43540500003;

Other
spf=pass (sender IP is 66.163.184.43) smtp.mailfrom=yahoo.com; dkim=pass (signature was verified) header.d=yahoo.com;dmarc=pass action=none header.from=yahoo.com;compauth=pass reason=100
Pass (protection.outlook.com: domain of yahoo.com designates 66.163.184.43 as permitted sender) receiver=protection.outlook.com; client-ip=66.163.184.43; helo=sonic317-32.consmr.mail.ne1.y
v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1753292691; bh=S7X0uCYD83+ItteZiiMyPhBjAm76n++/Fu3ngOVnw9s=; h=From:Date:Subject:To:References:From:Subject:Reply-To; b=fo4I1U
v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1753292691; bh=1U4yxGHeEjS8NjNN03s9MnHt6MoSuY6AlTIn1GUl+Kj=; h=X-Sonic-MF:From:Date:Subject:To:From:Subject; b=noCw8E6srKDl3QXI
YL5xPfQVM1nSktOFCQ84rLHKAlT_06Yb4grm4UE.l7G24G_99WCj3nN2ezxnp50 yYcsOc4d0fbe.dWGUdGF1q7_yrJLDT8XQyLSDV66WThAmYyeXBNZKcBcSXznjqe8ydXo9CG45Bsh UXvWexUl1SdEuNnkCNdr7eXBLvRKg8WpJ.DQoQCBevOJ9WF
<estong6boss@yahoo.com>
27e9dfb5-62ff-41ba-ba9f-4ee8748f52b1
text/plain
7bit
1.0 (1.0)
iPhone Mail (22F76)
<AF3839B3-7802-4DEF-A1DA-CED10E2995E8.ref@yahoo.com>
25
estong6boss@yahoo.com
23 Jul 2025 17:44:52.5473 (UTC)
OriginalSubmit
1:00:00:00.0000000



9. For **Google or Yahoo** Email Header Analyzer and Forensic see tutorial below.

Source: https://youtu.be/3wwaYc_Yuhc?si=HZX0JRFK8MRbbGQa

Scenario:

1. You receive an email from “billing@yourcompany-invoice.com” with the subject: “Urgent: Outstanding Invoice #98347”. The sender urges you to click a link to view the invoice and avoid late penalties. The message is signed with your company’s name but from an unfamiliar domain.

   Question:
   What steps should you take to verify the legitimacy of this email, and what signs point to phishing?

   Below will be my take:

   1.1 Check the Sender's Email Address = **Check and verify** if the domain match with company official domain, if this is unfamiliar meaning it raise to suspicions.
   1.2 Do NOT click the link = **Hover** your cursor over the link (without clicking to preview the destination URL. If it looks suspicious, mismatched, or overly complex, do not engage.
   1.3 Contact the Company Directly = **Reach out** to your company's billing or finance department using official contact methods
   1.4 Scan for Spelling and Grammar Issues **= Mistakes** in punctuation, awkward phrasing, or odd formatting can be signs of a phishing attempt.
   1.5 Copy the message Header and paste this to **Message Header Analyzer or use Mx Analyzer** to check the legitimacy of the email. Note that the email will be legit if it passes the **spf, dkim and dmarc process**. See sample below if the email passed.

```
Unknown fields: DLR:1NB;

AntiSpamReport
Bulk Complaint Level: 0
Source header: BCL:0;ARA:13230040|7093399015|4102299003|43540500003;
Unknown fields: ARA:13230040|7093399015|4102299003|43540500003;

Other
spf=pass (sender IP is 66.163.184.43) smtp.mailfrom=yahoo.com; dkim=pass (signature was verified) header.d=yahoo.com;dmarc=pass action=none header.from=yahoo.com;compauth=pass reason=100
Pass (protection.outlook.com: domain of yahoo.com designates 66.163.184.43 as permitted sender) receiver=protection.outlook.com; client-ip=66.163.184.43; helo=sonic317-32.consmr.mail.ne1.y
v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1753292691; bh=S7X0uCYD83+ItteZiiMyPhBjAm76n++/Fu3ngOVnw9s=; h=From:Date:Subject:To:References:From:Subject:Reply-To; b=fo4I1U
v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1753292691; bh=1U4yxGHeEjS8NjNN03s9MnHt6MoSuY6AlTIn1GUl+Kj=; h=X-Sonic-MF:From:Date:Subject:To:From:Subject; b=noCw8E6srKDl3QX
YL5xPfQVM1nSktOFCQ84rLHKAlT_06Yb4grm4UE.l7G24G_99WCj3nN2ezxnp50 yYcsOc4d0fbe.dWGUdGF1q7_yrJLDT8XQyLSDV66WThAmYyeXBNZKcBcSXznjqe8ydXo9CG45Bsh UXvWeXUl1SdEuNnkCNdr7eXBLvRKg8WpJ.DQoQCBevOJ9WF
<estong6boss@yahoo.com>
27e9dfb5-62ff-41ba-ba9f-4ee8748f52b1
text/plain
7bit
1.0 (1.0)
iPhone Mail (22F76)
<AF3839B3-7802-4DEF-A1DA-CED10E2995E8.ref@yahoo.com>
25
estong6boss@yahoo.com
23 Jul 2025 17:44:52.5473 (UTC)
OriginalSubmit
1:00:00:00.0000000
```

Suspicious Element:
Unfamiliar domain name
Urgent tone with penalties
Link in the email
Generic or odd sign-off
Lack of contextual detail about the invoice

2. An email appears to be from your internal IT team, asking you to log in to a portal using a link provided to “verify your credentials due to a security update.” The link goes to *login-check.com*, and the branding looks authentic.

   Question:
   What should you do before clicking the link or providing credentials, and what risks are involved?

   Below will be my take:

   Steps You Should Take Before Clicking or Logging In

   2.1 **Scrutinize the Sender's Email Address** = Is it from your company’s verified domain? Attackers often mask malicious emails with familiar-looking addresses.

   2.2 **Inspect the Link (without clicking)**: Hover over it and examine the full URL. "login-check.com" doesn't sound like an internal company domain. If it's not one you've seen before, it's a major red flag

   2.3 **Contact Your Real IT Department**: Use internal channels (chat, phone, intranet) to confirm whether there's a legitimate update. Do not reply to the suspicious email directly.

   2.4 **Report the Email**: If your company has a “Report Phishing” button or a security team, share the message for further investigation.

   2.5 Copy the message Header and paste this to **Message Header Analyzer or use Mx Analyzer** to check the legitimacy of the email. Note that the email will be legit if it passes the spf, dkim and dmarc process. See sample below if the email passed.

   Risks If You Click or Enter Credential
   Credential Theft, Attackers may steal login info and access internal systems
   Network Compromise, could open doors to malware, ransomware, or data exfiltration
   Brand or Financial Damage and Data Privacy Violation

3. A high-ranking executive email you asking for help purchasing gift cards for client appreciation. The tone feels slightly off, and the signature is missing their usual tagline. You check and see the email domain is “@company-support.com” rather than “@company.com”.

   Question:
   What kind of attack could this be, and how can you confirm its authenticity

Below will be my take:

Business Email Compromise (BEC) or **Executive Impersonation** attack—a deceptive but highly effective phishing tactic often aimed at pressuring employees into acting quickly on fake requests. BEC attacks often rely on human instinct: urgency, helpfulness, and respect for authority. **The best defense?** Stay skeptical, pause before acting, and use official channels to confirm. Gift cards should never be requested via email.

Steps to Confirm Legitimacy

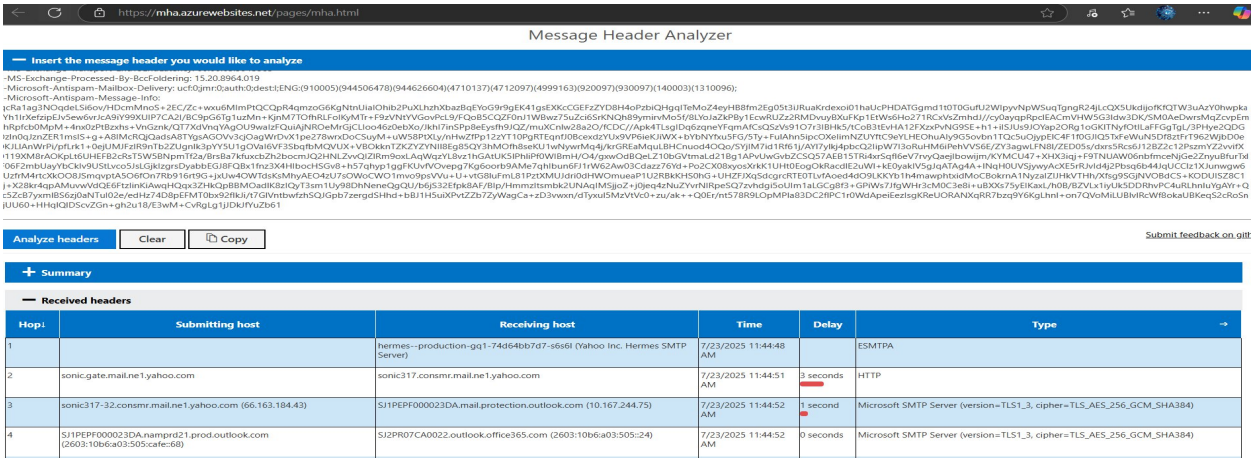
3.1 **Cross-Check the Domain**:
Look up "@company-support.com" using your company's IT or security documentation. If it's unlisted, it's suspect.

3.2 **Compare Past Emails**:
Reference older authentic emails from the executive. Look for formatting, signature details, phrasing, and salutations that are usually consistent.

3.3 **Contact the Executive Directly** (via a different channel):
Call, message, or reach out via verified internal tools to confirm whether they actually sent the request.

3.4 **Report to IT or Security Team**:
Forward the suspicious email using internal reporting procedures. Don't just ignore it—help the company stay vigilant.

3.5 Copy the message Header and paste this to **Message Header Analyzer or use Mx Analyzer** to check the legitimacy of the email. Note that the email will be legit if it passes the **spf, dkim and dmarc process**. See sample email forensic below if the email passed.



Unknown fields: DLR:INB;

AntiSpamReport
Bulk Complaint Level: 0
Source header: BCL:0;ARA:13230040|7093399015|4102299003|43540500003;
Unknown fields: ARA:13230040|7093399015|4102299003|43540500003;

Other
spf=pass (sender IP is 66.163.184.43) smtp.mailfrom=yahoo.com; dkim=pass (signature was verified) header.d=yahoo.com;dmarc=pass action=none header.from=yahoo.com;compauth=pass reason=100
Pass (protection.outlook.com: domain of yahoo.com designates 66.163.184.43 as permitted sender) receiver=protection.outlook.com; client-ip=66.163.184.43; helo=sonic317-32.consmr.mail.ne1.ya
v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1753292691; bh=S7X0uCYD83+ItteZiiMyPhBjAm76n++/Fu3ngOVnw9s=; h=From:Date:Subject:To:References:From:Subject:Reply-To; b=fo4I1U
v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1753292691; bh=1U4yxGHeEjS8NjNN03s9MnHt6MoSuY6AlTIn1GUl+Kj=; h=X-Sonic-MF:From:Date:Subject:To:From:Subject; b=noCw8E6srKDl3QXI
YL5xPfQVM1nSktOFCQ84rLHKAlT_06Yb4grm4UE.l7G24G_99WCj3nN2ezxnp50 yYcsOc4d0fbe.dWGUdGF1q7_yrJLDT8XQyLSDV66WThAmYyeXBNZKcBcSXznjqe8ydXo9CG45Bsh UXvWexUl1SdEuNnkCNdr7eXBLvRKg8WpJ.DQoQCBevOJ9WF
<estong6boss@yahoo.com>
27e9dfb5-62ff-41ba-ba9f-4ee8748f52b1
text/plain
7bit
1.0 (1.0)
iPhone Mail (22F76)
<AF3839B3-7802-4DEF-A1DA-CED10E2995E8.ref@yahoo.com>
25
estong6boss@yahoo.com
23 Jul 2025 17:44:52.5473 (UTC)
OriginalSubmit
1:00:00:00.0000000

” When you train Smarter, you defend Stronger”

Leonard Estos