

**Leonard M. Estos**

***Cybersecurity Researcher & Technical Author***

Edmonton, Alberta, Canada

## **Project Name: Microsoft Defender Email Forensic Investigation**

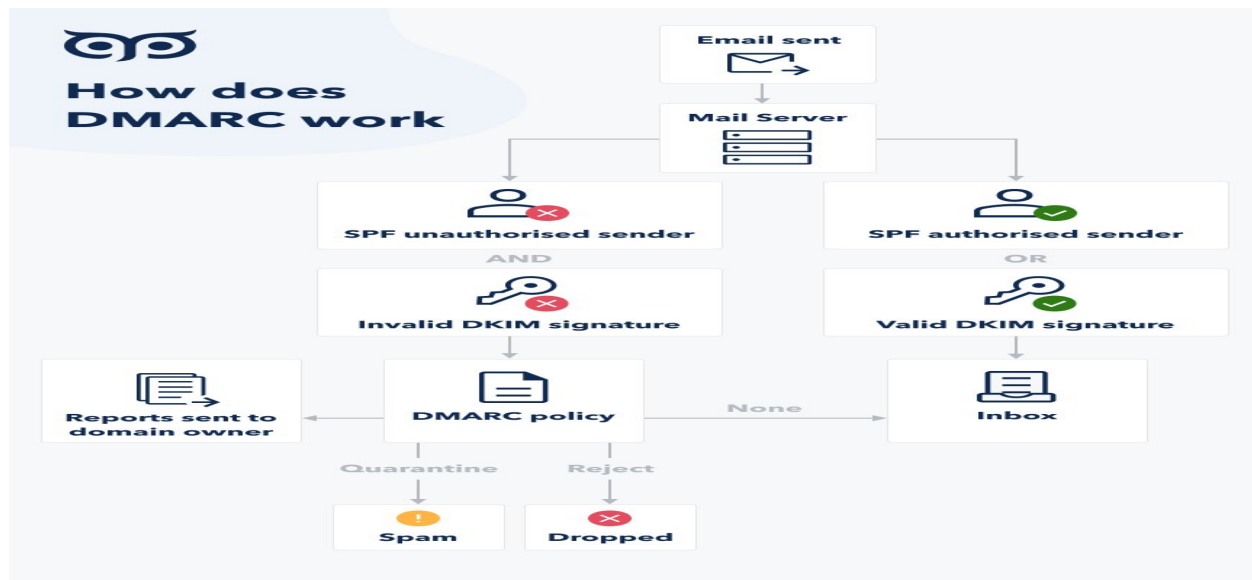
**Project Overview:** This documentation provides a comprehensive guide to email headers - the metadata-rich component of email communication that plays a critical role in cybersecurity, forensic analysis, and troubleshooting. It is designed to help technical professionals, SOC analysts, and IT administrators 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):

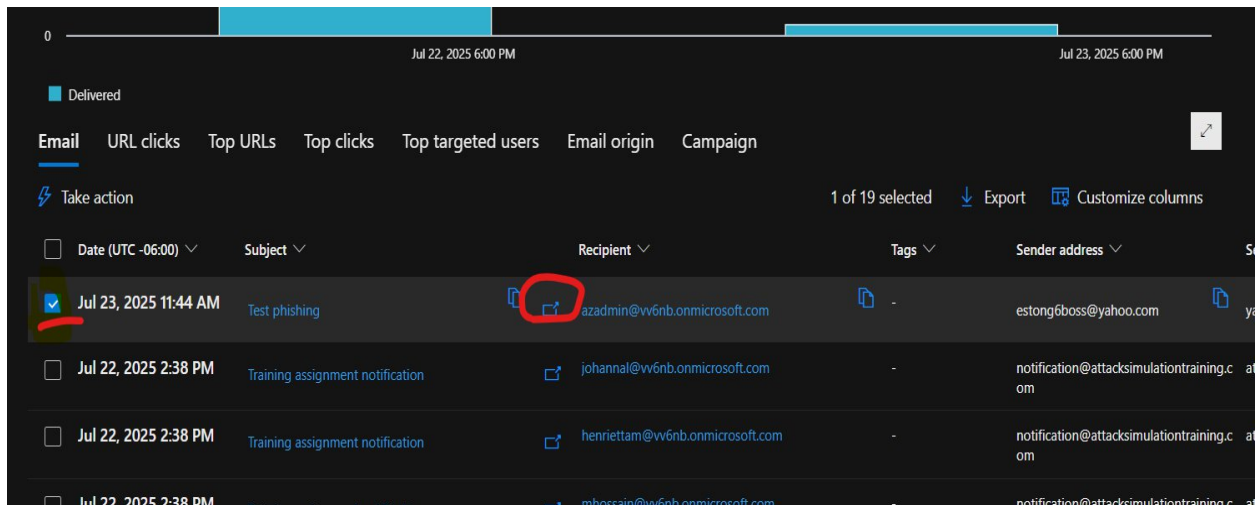
DKIM adds a digital signature to email headers. This signature is verified using a public key published in the sending domain's DNS records.

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

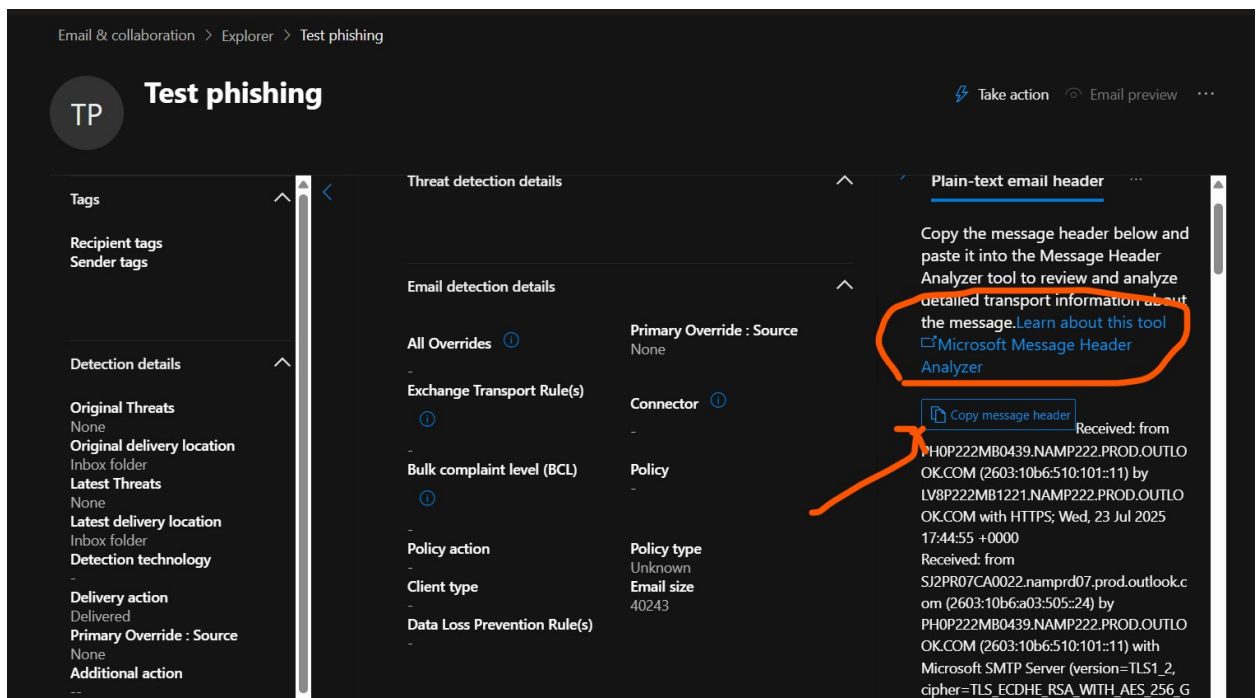
DMARC builds upon SPF and DKIM. It allows domain owners to specify what to do with emails that fail SPF and/or DKIM checks, such as rejecting or quarantining them. DMARC also provides reporting mechanisms to help domain owners monitor email authentication attempts and identify potential abuse.

## 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\_Entral  
D\_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 Analyzser) and copy the message header.



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

<https://mha.azurewebsites.net/>

Message Header Analyzer

Insert the message header you would like to analyze

M5-Exchange-Processed-By-Bcfoldering: 15.20.8964.019  
 -Microsoft-Antispam-Mailbox-Delivery: ucf0jmr0auth0dest:ENG(910005)(944506478)(944626604)(4710137)(4712097)(4999163)(920097)(930097)(140003)(1310096);  
 -Microsoft-Antispam-Message-Info:  
 jRat1ag3N0del.S66w/H0CmMnoS+2EC/Zc+wxu6MlmPttQC0pR4qmozoG6KgNtnLialOhib2PuXlzhXbaz8qEloG99gEK41gsEXKcGEFZYZD8H4cPzbiQHggTeMoZ4eyH88fm2Eg053JRuakRdexio01hUcPHDATGmd110T0GufU2WipyvNpWsuqTgngr24JlCQX5UkdjorK1QTW3uAzY0hwpa  
 Yh1tXefzpjEjSew6wjcA9Y99XUPl7CA2/Bc9pG6Tg1uzMn+KgnM770thrLFolkYMTir+F9zVNTYVgovPcl.9/FQo85CQZF0n1Wbwz75uZc6S5KNQ89yminvMo5/8LVoJaZkPby1EcmRUZ22RMDvuyBXufKp1Etw6Ho271RCvSzmhdJ/cy0ayqRpdEACmVHW5G3ldw3DK/SM0AeDwrsMqZcvpEm  
 hRgfc0MpmM+4nu0zP1Bzxts+VnGznk/QT7XdtVnqVAg0U9walZFQuIAjNR0eMrGjCLOo46z0ebXo/ikhTm5Pp8Eysfth9/QZ/muXcnlw28a2O/ICDC//Apk4TSLgDq6zqneYfQmAfCsQSAv91OT/3IBHk5/tCoB31EwHA12FkzPvNG9SE+H1+HISU9JOvap2ORg1oGKITNy0iLAFgTgU/3PHye2QDG  
 zlnbqzNZER1ms5+g+ABIMCRQqQadsA87YgAGOV3gOagWtdX1pe278wDcSuyM+uW58P0Xly/HhWZPp12zt1T0PgRTeqn10BcekdzUx9VP6eKJWX+bYbNYhu5FG5ty+FuAhnsipCOXelmNZUyTC3eYlHEOhuAly9G5ovbn1TQc5uOjypE4F1R0GJC25teWuNSDf8ztfT962WjB0De  
 KJLIJAnWpJpLk1+8eJUMJFzJR9nTbZ2ZJnKpHY5UgOw6Vf3SqbhMQVUX+V80kxTZKZY21Nl68gS5QY3mAOm8eKJtWYyWmQd4jKvGREaMqulBhCnuod4OOo5YjIM7d1R651jA1T7Yk4PbcQ2Igw730RuHMGfHNV5SE/Z33agwLFN8/ZED05j0wvSR6512822z12PznmY2ZvWpX  
 I119XM8rAOKpL6UHEF82:8r5T5W8BNpmtf2a/Br8Ba7kXucbZzbocmJQ2HNLZvQZIRm9oxLAqWazYLBvz1HGALUK5IPhIP0WbHmH/O4/gwOQdQeLZ10BGVmal.d21Bg1APVUwGvBZCSQ57AE815TR4urSgqf6eV7nyQaegbowjw/KYMCUL47+XHX3qg+F9TNUAW06bnfmcNjGe2ZnyuBfurlT4  
 06f2mbJuyYbCkV9U5LUSL5sJslGjKzgrsDyabbEGJ8FQ8x1fnz3X4HlboC5Gv8+h57ghyp1ggFKUvOVepg7K6oorb9AMe7qhtbun6f1rW62Aw03Cdaz276Vd+PoZC80xyosXkK1UH0EogOkRacdE2uWI+kE0yakIVSgJqAtAg4A+1NqH0U5jwywACXESrJld4q2Pbsq6b44JqUCclz1JLunwgw6  
 UzhM4rtXkO085mcpvTA506On7Rb916r9G+JxU4COWTdsKMyAE04zU7oWOW1mvo9psVVu+U+vtG8lufmL81PzTXMUIdrH0WomueaP1U2R8KH50Hq+UHZFjXqSdgrCtRT0TLvAced4d09UKYb1HmawphtxidMcBokmA1NyzalZUJHk/THh/Xfsg95GJNV0BdCS+KODUISZ8C1  
 j+X28kr4qpAMuvwVQ6FztlnKAwqHqX3ZkQp88MOadK8ZlQyT3m1Uy98DhNeneQgQU/b6532Efpk8AF/Blp/Hmmztsmbk2UNAQImSjloZ+j0jeq4ZuZvNrPES7zvhdg5oUlm1aLGCg8f3+GPW57JfgWHR3CMOC3e8+uBX675yEikaxLh08/BZVLx1yUkSDDRhVpC4uRlnluYgAY+Q  
 c5ZcB7ymIS69gaNtU0eZedH274D8pEFMT0bx92tNkI/r7GlvbwfzhSjQGPb7zergdShd+bBJ1H5uXpVZb7ZyWagCa+2D3wvxn/dTxyu5MZYVVC0+zu/ak++Q0ER/mT5789LOpMPla83DC2HPC1r0WAdApeieezsgRReUORANXgRR7bzg9Y6KgLnHl+on7QvoMLUBlWIRWfBokaUBKq52Sro5n  
 JUU60+HHqIQDScvZgn+ghzu18/E3wM+CVgltg1jDkHfuzb61

Analyze headers Clear Copy

Submit feedback on github

Summary

Received headers

Hops	Submitting host	Receiving host	Time	Delay	Type
1		hermes-production-gq1-74d64bb7d7-s661 (Yahoo Inc. Hermes SMTP Server)	7/23/2025 11:44:48 AM		ESMTPA
2	sonic.gate.mail.ne1.yahoo.com	sonic317.consmr.mail.ne1.yahoo.com	7/23/2025 11:44:51 AM	3 seconds	HTTP
3	sonic317-32.consmr.mail.ne1.yahoo.com (66.163.184.43)	SJ1PEPF00023DA.mail.protection.outlook.com (10.167.244.75)	7/23/2025 11:44:52 AM	1 second	Microsoft SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384)
4	SJ1PEPF00023DA.namprd21.prod.outlook.com (2603:10b6:a03:505:cafe:68)	SJ2PR07CA0022.outlook.office365.com (2603:10b6:a03:505:24)	7/23/2025 11:44:52 AM	0 seconds	Microsoft SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384)

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

## What is Email Header

Summary

Subject: test 4  
 Message Id: <PNZPR01MB513628451DASE14390761514A3389@PNZPR01MB5136.INDRPD01.PROD.OUTLOOK.COM>  
 Creation time: Fri, 4 Jun 2021 14:02:27 +0000 (Delivered after 0 seconds)  
 From: User C <userc@365conceptsLabs.onmicrosoft.com>  
 To: Amit Kumar <Admin@365conceptsLabs.onmicrosoft.com>

Received headers

Hops	Submitting host	Receiving host	Time	Delay	Type
1	PNZPR01MB5136.INDRPD01.PROD.OUTLOOK.COM ([fe80:11a6:3fe5:6c54:b7f2])	PNZPR01MB5136.INDRPD01.PROD.OUTLOOK.COM ([fe80:11a6:3fe5:6c54:b7f2])	6/4/2021 7:32:27 PM		mail
2	PNZPR01MB5136.INDRPD01.PROD.OUTLOOK.COM (2603:1096:c01:3c:14)	PN1PR0101MB1423.INDRPD01.PROD.OUTLOOK.COM (2603:1096:c00:1a:c:22)	6/4/2021 7:32:27 PM	0 seconds	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)
3	PN1PR0101MB1423.INDRPD01.PROD.OUTLOOK.COM (2603:1096:b00:c:26)	BMXP01MB3927.INDRPD01.PROD.OUTLOOK.COM	6/4/2021 7:32:27 PM	0 seconds	HTTPS

Forefront Antispam Report Header

Language: en  
 Spam Confidence Level: -1  
 Spam Filtering Verdict: SKI  
 IP Filter Verdict: NLI  
 HELO/EHLO String: PNZPR01MB5136.INDRPD01.PROD.OUTLOOK.COM  
 Connecting IP Address: 255.255.255.255  
 Protection Policy: NONE  
 Category:  
 Source header: CIP:255.255.255.255;CTRY=US;LANG=en;CL=-1;SRV=IPVNU;SPV=SKI;H=PNZPR01MB5136.INDRPD01.PROD.OUTLOOK.COM;PTR=CAT:NONE;SFS=DIR:INB;  
 Unknown fields: DIR:INB;

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

Unknown fields: unknown;

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++Fu3ngOVmw9s; h=From:Date:Subject:To:References:From:Subject:Reply-To; b=f041IU; v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1753292691; bh=1U4yxGHejS8NjMN03s9MhT6MoSuY6ALTIn1GUl+Kj; h=X-Sonic-MF:From:Date:Subject:To:From:Subject; b=noCw8E6srKD13QX; YL5xPQVM1nsktOFCQ84rLHKAlT\_06Yb4gm4UE.17G24G\_99KcJ3nI2ezxnp50 yYcs0c4d0fbc.dWGUdGF1q7\_ylr1D78XQyLSDV66WThAmMyeXBZKcBcSxznjqe8ydx09CG45Bsh UXvWexU11sdEulnkCNDr7eXBLVRkg8WpJ.DQoQCBevO3J9Mf<estong6boss@yahoo.com>

27e9df05-62ff-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

## What is Email Header



Authentication-Results	spf=pass (sender IP is 209.85.218.43) smtp.mailfrom=gmail.com; dkim=pass (signature was verified) header.d=gmail.com; dmarc=pass action=none header.from=gmail.com; compauth=pass reason=100
Received-SPF	Pass (protection.outlook.com: domain of gmail.com designates 209.85.218.43 as permitted sender) receiver=protection.outlook.com; client-ip=209.85.218.43; helo=mail-ej1-f43.google.com;
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=20161025; h=mime-version:from:date:message-id:subject:to; bh=Ik1b7vUjDow491fE6KbEPYjgplfmWZjeNy4P8LToE=; b=s46V7GT4r0LS1RJMq347exzV4Xnb+p6MS34xLGkamcknp7k5UavxcgK9uVW6 nuyfGhWw9aa273gckSQbukLkVP4kctzTQKK+Big3YVvduFBPmYIK/h6tPstXyTfbJa CVx1MVGGgDuKLAfStCGw2qXmMGjIWHmWZT8RwhcyehOcbCq/9N5afX28mHJgj2i2vVT gGOLY03W04Jy/6BwrsKC3MYnN+e5pg2K0aT29AqzS2kTawKFC0c2Y3fuuNE2R/ZElp IT1NZrlpPLGq6SqPKclA3LqCiqLunZbKucKCGfHMGAM3pxR0fgW0j32VkonSkdQ0 JD2g==
X-Originating-IP	[45.251.48.218]
Return-Path	userc@365conceptsLabs.onmicrosoft.com
X-MS-Exchange-CrossTenant-AuthAs	Internal

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

Source: [https://youtu.be/3wwaYc\\_Yuhc?si=HZX0JRFK8MRbbGQa](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 FIELD: UNKNOWN;

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+/Fu3ngOVmw9s=; h=From:Date:Subject:To:References:From:Subject:Reply-To; b=fo411Uu
v=1; a=rsa-sha256; c=relaxed/relaxed; d=yahoo.com; s=s2048; t=1753292691; bh=1U4yxGHeTjS8NjW03s9MmHt6MoSuV6ALTn1GUl+Kj=; h=X-Sonic-MF:From:Date:Subject:To:From:Subject; b=ncW8E6srKDL3QXI
YL5xPfQMINSktOFCQ84rLHKALT_06Yb4grm4UE.17G24G_99uKj3nN2ezxnp50 yYcsoc4d0fbc.dwgudGF1q7_yr3LD78XQyLSOV66WThAmYyexBNZKcBcSKznjqeBydx09CG45Bsh UXWwexU11sdEuHnkCndr7eXBLVRKg8WpJ.DQoQCBeVO39NfC
<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.

Message Header Analyzer

Insert the message header you would like to analyze

MS-Exchange-Processed-BY:BCF-olenting:15.20.3864.019

Microsoft-Antispam-Mailbox-Delivery:uf0gm0rauth0dest:ENG(910005)(944506478)(944626604)(4710137)(4712097)(4999163)(920097)(930097)(140003)(1310096)

Microsoft-Antispam-Message-Info

YH11XezrEpEJvSeWorJcAB9Y99UJPFCA2I/BC0pG6Tg1uzMn+KjnM77C0hRLf0kyMTI+P9zVNIYVGovPcL9/FQoB5CQZf0n1WbWz7SuZc65rKNQ89ymivMc5f/BLVazKpBy1EcwRUZz2RMDvuyBxUpK1EiW66Hoz71RcVv5Zmhdl/cy0eyqRpeACmVfW5G3ldw3DK/SM0AeDwrsMqZcVpEm

hRhc3b0MjM+4ndzPflBzsh+VnGzmk/DT7XgVnqYgCU9wzafQuA9hDeMrgCCLoop4k2ebx0/ik17n5PpIeJyH9H0ZJ/rmucNcnw2baZ0/RCDC/Apk4TLagDqezneYfQmACQZsV9107/31Bh5/RCob3Hv4A12FzxpVNG95E+h1+H5U9p0Yap2Orq1oGKI7NyeDhLafFgTg/3PpIye2QDQ

0n6qJmZFR1mst+g+ABMRCQZa6AATVgAUCOW3CjQwWd0x1Tpe27BwrdC5uqM+uW8B0Xy/mHwZP7122170gRTTqgR0CewdZ1XpXpKkLWx+1hRkHxwafP5/57y+FuAhh0pC2XelnnZU7YTC3wH1ECOnuAkyK50vsn1TC35u3ppIEC4f1T0G3C2TstWwWuN5D8tRf198zWjdDoe

KCUANWrpjrlk1+0qJmJFpR9mTbzZLgth3pYyU1gCvaw6Vf33bqBMcVUX+VBOcknTZKZYZYNIIBlg85QY3hMCM8baKU7wNyywMq4/KrGRIaMquLbHCnuod4CQw9YJm7d1R61jAY17yIq4pbc22lpW73oIuHmMhthvV566/ZY3agwLFNIB/ZE0D5z/dersRc6x132BZ2c13PzamyY2ZvixK

1179XMBwKdK6L6U4H5B2c6fTSW58NpmT5a3Brla9x2z3bsemQ2dHh2vxdQ2BrlroslAaWgY1BzThGAtUKS3h9P0WlBmH1C4AgwecQlQELZ10bQVymal.d13Bg1aP4u4wGvZC5Q25A1B157B4kafSgIseV7YnQan9b0wgm/YXACU47+NAH3ag+P97NtUAW06abfrecn9f22ZnydRfId

06f2mbUayYbCKh9U5fLvc053dLgKjK9zDyabHfGJ8fQB1fnz3X4HlboocH5CvB+h57ghyp1ggfKUVV0vepg7K6o0orb9AMe7qhtbunf11W62Aw03Cdzaz76Vd+PoZC0Blyeo0Kk1UHH0eg0KfAcdd2UwH+KE0yakiV5gIqATAg4A+InqHOUV5jwywACX5fRld4j2Ppsq644IqJCC1z1XJunwgw6

U2H4Mrc0K0B5mcapfAS06f0n7B916t9K3+J4u4COW7SdK8MykAC4U7J0WocW01mvoPpVUu+U+Vc0B8uLm13P2XDMUdndH0W0nuap1U2K8BMZHS093+U4Z7Xg55d0grTE0TLVAcad40D9LKYb1H4mawphtsMocBoknA1NyzaiZUH4VTHhX7g95GhV0BdCS+KODUJ5Z8C1

1+X2B84qpmMuvwVE6f7pm0AwghH05p3ZHC3pBIBWCaiddBzCy13tm1Uy9BEBHNeenrQpZUhg5328FpKdAF/Bp/HemmttmnbcZUAgqM3lp2+JBeqEzNuzYwN8pR5CZ7zvdgIsolm1aUGCgRf3+GfWw7JgWHp3cM0C3eB+uB8X7y83Kae7h0LREZY+1nukSD09hPCuRlHnUgWY+Q

c5ZcB7ymIB56g9aNTu02e/ndh474D8pEFMTu0bx92fRkU/7GIVntbzfzFSQJGpb7zergdSHd+BB1H5uXpVzZb7ZyWagCa+zD3vwm/dTyuU5MzVIVC0+zu/ak+Q0Er/m578R9LOpMPla83DC2RfC10WdApeIeestgKReUORANgRR7bzq9Y6KglHnl+on7QV0MILUBWlRcWlBokaUBKq52cRo5n

IUU60+HhKqQD5ScvZGn+gh2u18/E3wM+CV6gUg1JDKUfVuzb61

Analyze headers

Clear

Copy

Submit feedback on github

Summary

Received headers

Hop#	Submitting host	Receiving host	Time	Delay	Type
1		hermes--production-gq1-7464b7d7-9668 (Yahoo Inc. Hermes SMTP Server)	7/23/2025 11:44:48 AM		ESMTPA
2	sonic.gate.mail.ne1.yahoo.com	sonic317.consmr.mail.ne1.yahoo.com	7/23/2025 11:44:51 AM	3 seconds	HTTP
3	sonic317-32.consmr.mail.ne1.yahoo.com (66.163.184.43)	SI1PEPF000023DA.mail.protection.outlook.com (10.167.244.75)	7/23/2025 11:44:52 AM	1 second	Microsoft SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384)
4	SI1PEPF000023DA.namprd21.prod.outlook.com (2603:10b6:a03:505:cafe:68)	SI2PR07CA0022.outlook.office365.com (2603:10b6:a03:505:24)	7/23/2025 11:44:52 AM	0 seconds	Microsoft SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384)



Unknown fields: unknown;

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++/Fu3ngOVmw9s=; 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=1U4yxGHejS8NjMN03s9MnHt6MoSuY6AlTIn1GUL+Kj=; h=X-Sonic-MF:From:Date:Subject:To:From:Subject; b=noCw8E6srKD13QXIYL5xPfQVM1nsktOfCQ84rLHKAlT\_06Yb4grm4UE.17G24G\_99wCj3nI2ezxnp50 yYcs0c4d0fbc.dWGUdGF1q7\_yrJLDT8XQyLSDV66WThAmYyeXBINZKcBcSXznjqe8ydxo9CG45Bsh UXvWexU11sdEulnkCNdr7eXBLVRkg8WpJ.DQoQCBevOJ9WfC<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 Estes*