Internship Task 2 : Phishing Investigation

1.Task Overview

The objective of this task was to investigate a suspicious email suspected to be part of a phishing attempt. The task involved analyzing the email's structure, verifying the legitimacy of the sender, examining attachments and embedded links, and identifying any signs of malicious intent or compromise. Interns were expected to use cybersecurity tools and analytical techniques to uncover potential threats, document indicators of phishing, and summarize their findings in a structured format.

This task simulated a real-world incident response scenario, aiming to enhance practical knowledge in:

- Email threat detection
- Phishing indicator identification
- Use of investigation tools (e.g., VirusTotal, WHOIS, sandboxing tools)
- Documentation and reporting of cybersecurity incidents

The successful completion of this task demonstrated the intern's ability to identify phishing attempts and contributed to their readiness for handling email-based threats in professional environments.

---

2. Tools Used

To conduct the phishing investigation, I used the following tools:

- **Email Header Analyzer** – To examine the routing path and authentication of the email.
- **VirusTotal** – For scanning file attachments and URLs for malware or suspicious content.
- **Any.Run** – A sandbox for dynamic analysis of suspicious files and behaviors.
- **Google Safe Browsing & Phishing Database** – For checking the reputation and safety of URLs.
- **Browser Developer Tools (Inspect Element)** – To analyze webpage source code and embedded elements.
- **WHOIS Lookup Services** – To gather information about the domain's registration and legitimacy.

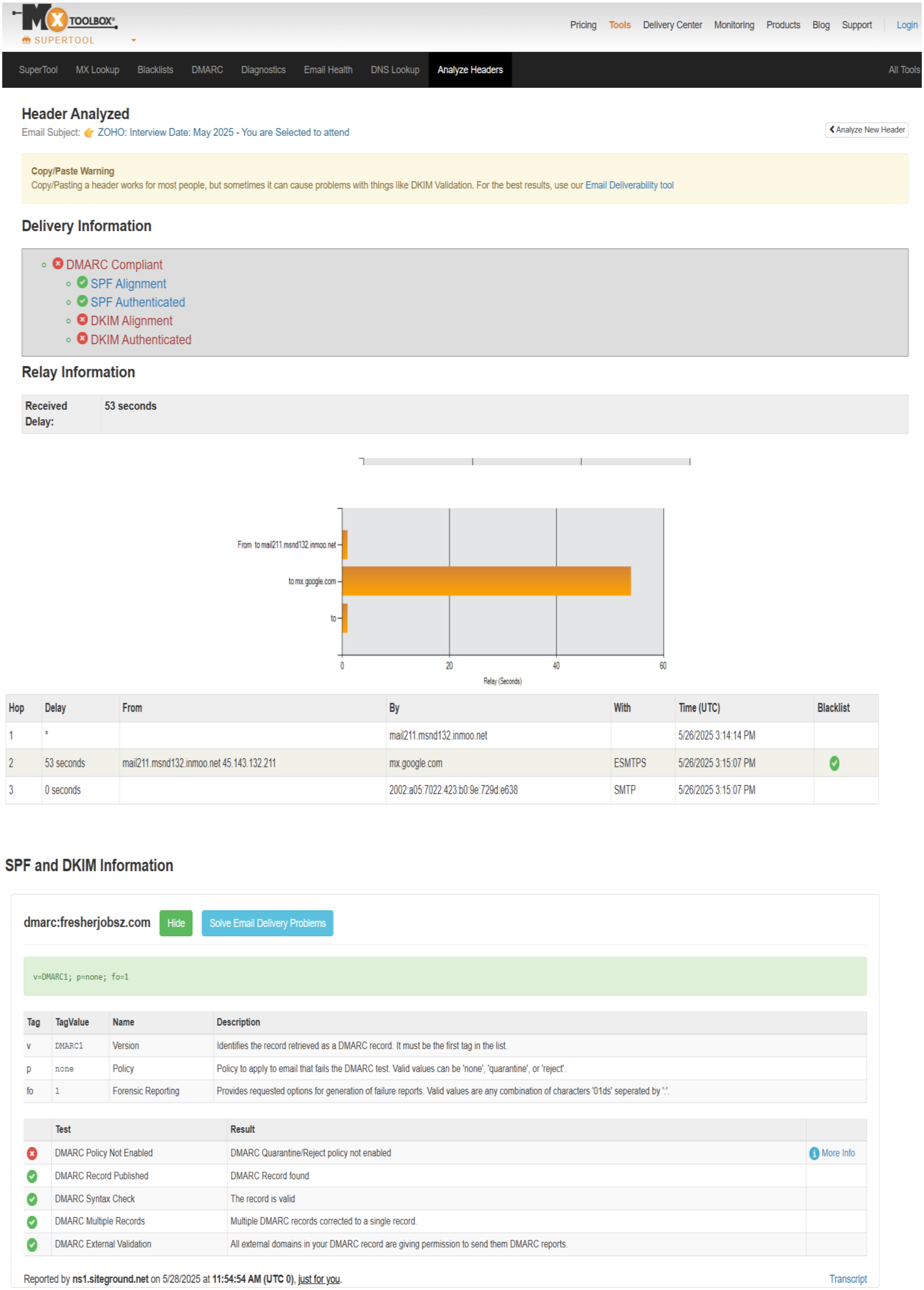
---

3. Steps Followed

1. **Preliminary Email Analysis**
    - Reviewed the sender's email address and domain name for inconsistencies.
    - Identified signs of social engineering such as urgency, vague language, and grammatical errors.
2. **Header and Authentication Checks**
    - Analyzed email headers to verify SPF, DKIM, and DMARC status.
    - Traced the origin IP address to detect any suspicious routing.
3. **File and Link Analysis**
    - Uploaded the attached file and hyperlinks to VirusTotal and Any.Run.
    - Monitored for redirection to fake login pages or malicious scripts.
4. **Source Code Inspection**
    - Used browser tools to inspect the HTML of the landing page for phishing forms or obfuscated JavaScript.
5. **Domain Reputation Verification**
    - Conducted WHOIS lookups and blacklist checks for domains linked in the email.
6. **Report Generation**
    - Compiled all observed phishing indicators and created a detailed summary for documentation and learning.

---

4. Screenshots



Header Analyzed

Email Subject: 👉 ZOHO: Interview Date: May 2025 - You are Selected to attend

Copy/Paste Warning
Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our Email Deliverability tool

Delivery Information

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

Relay Information

Received Delay:	**53 seconds**

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*		mail211.msnd132.inmoo.net		5/26/2025 3:14:14 PM	
2	53 seconds	mail211.msnd132.inmoo.net 45.143.132.211	mx.google.com	ESMTPS	5/26/2025 3:15:07 PM	✓
3	0 seconds		2002:a05:7022:423:b0:9e:729d:e638	SMTP	5/26/2025 3:15:07 PM	

SPF and DKIM Information

dmarc:fresherjobsz.com

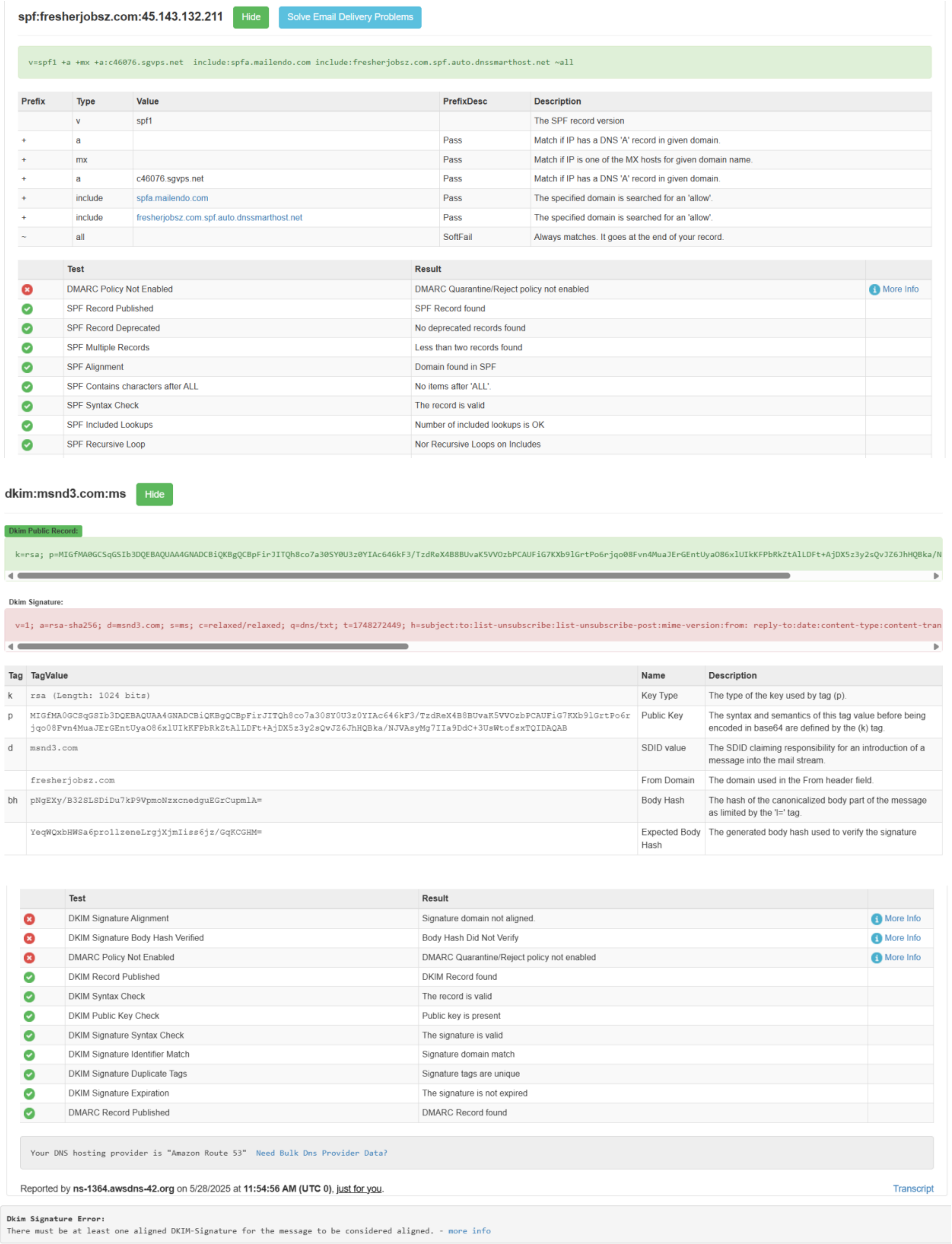
```
v=DMARC1; p=none; fo=1
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	none	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
fo	1	Forensic Reporting	Provides requested options for generation of failure reports. Valid values are any combination of characters '01ds' seperated by ':'.

	Test	Result	
☒	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	ℹ More Info
✓	DMARC Record Published	DMARC Record found	
✓	DMARC Syntax Check	The record is valid	
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.	
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.	

Reported by **ns1.siteground.net** on 5/28/2025 at **11:54:54 AM (UTC 0)**, just for you.

Transcript



spf:fresherjobsz.com:45.143.132.211

```
v=spf1 +a +mx +a:c46076.sgvps.net  include:spfa.mailendo.com include:fresherjobsz.com.spf.auto.dnssmarthost.net ~all
```

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	a		Pass	Match if IP has a DNS 'A' record in given domain.
+	mx		Pass	Match if IP is one of the MX hosts for given domain name.
+	a	c46076.sgvps.net	Pass	Match if IP has a DNS 'A' record in given domain.
+	include	spfa.mailendo.com	Pass	The specified domain is searched for an 'allow'.
+	include	fresherjobsz.com.spf.auto.dnssmarthost.net	Pass	The specified domain is searched for an 'allow'.
~	all		SoftFail	Always matches. It goes at the end of your record.

	Test	Result	
✗	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	ⓘ More Info
✓	SPF Record Published	SPF Record found	
✓	SPF Record Deprecated	No deprecated records found	
✓	SPF Multiple Records	Less than two records found	
✓	SPF Alignment	Domain found in SPF	
✓	SPF Contains characters after ALL	No items after 'ALL'.	
✓	SPF Syntax Check	The record is valid	
✓	SPF Included Lookups	Number of included lookups is OK	
✓	SPF Recursive Loop	Nor Recursive Loops on Includes	

dkim:msnd3.com:ms

Dkim Public Record:

```
k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCBpFirJITQh8co7a30SY0U3z0YIAc646kF3/TzdReX4B8BUvaK5VVOzbPCAUFiG7KXb9lGrtPo6rjqo08Fvn4MuaJErGEntUya086xlUIkKFPbRkZtAlLDFt+AjDX5z3y2sQvJZ6JhHQBka/N
```

Dkim Signature:

```
v=1; a=rsa-sha256; d=msnd3.com; s=ms; c=relaxed/relaxed; q=dns/txt; t=1748272449; h=subject:to:list-unsubscribe:list-unsubscribe-post:mime-version:from: reply-to:date:content-type:content-tran
```

Tag	TagValue	Name	Description
k	rsa (Length: 1024 bits)	Key Type	The type of the key used by tag (p).
p	MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCBpFirJITQh8co7a30SY0U3z0YIAc646kF3/TzdReX4B8BUvaK5VVOzbPCAUFiG7KXb9lGrtPo6rjqo08Fvn4MuaJErGEntUya086xlUIkKFPbRkZtAlLDFt+AjDX5z3y2sQvJZ6JhHQBka/NJVAsyMg7IIa9DdC+3UsWtofsxTQIDAQAB	Public Key	The syntax and semantics of this tag value before being encoded in base64 are defined by the (k) tag.
d	msnd3.com	SDID value	The SDID claiming responsibility for an introduction of a message into the mail stream.
	fresherjobsz.com	From Domain	The domain used in the From header field.
bh	pNgEXy/B32SLSDiDu7kP9VpmoNzxcnedguEGrCupmlA=	Body Hash	The hash of the canonicalized body part of the message as limited by the 'l=' tag.
	YeqWQxbHWSa6pro1lzeneLrgjXjmIiss6jz/GqKCGHM=	Expected Body Hash	The generated body hash used to verify the signature

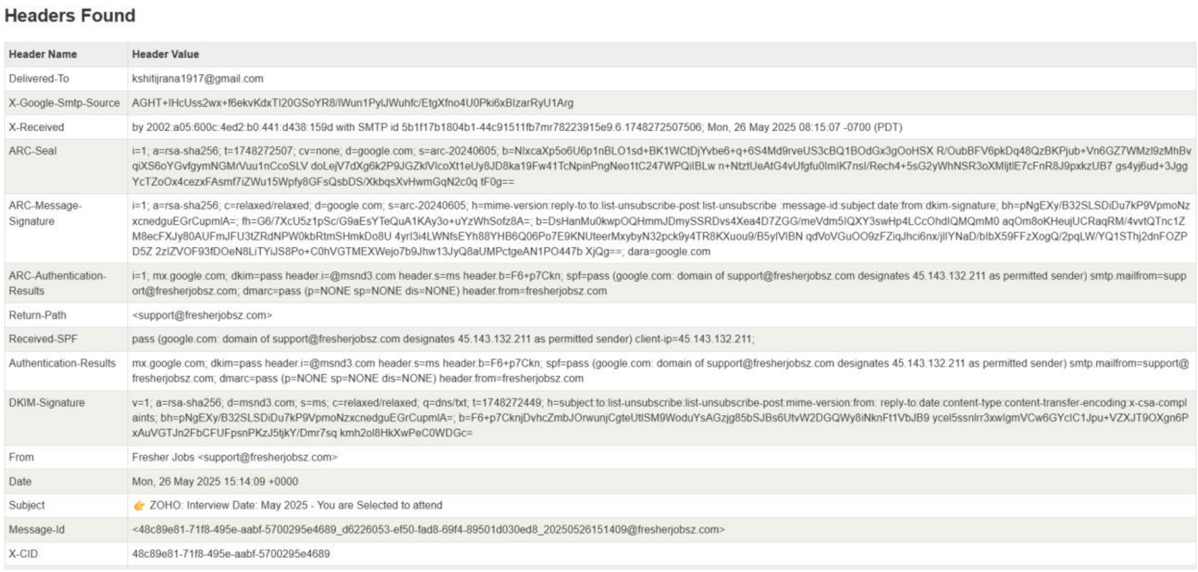
	Test	Result	
✗	DKIM Signature Alignment	Signature domain not aligned.	ⓘ More Info
✗	DKIM Signature Body Hash Verified	Body Hash Did Not Verify	ⓘ More Info
✗	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	ⓘ More Info
✓	DKIM Record Published	DKIM Record found	
✓	DKIM Syntax Check	The record is valid	
✓	DKIM Public Key Check	Public key is present	
✓	DKIM Signature Syntax Check	The signature is valid	
✓	DKIM Signature Identifier Match	Signature domain match	
✓	DKIM Signature Duplicate Tags	Signature tags are unique	
✓	DKIM Signature Expiration	The signature is not expired	
✓	DMARC Record Published	DMARC Record found	

```
Your DNS hosting provider is "Amazon Route 53"  Need Bulk Dns Provider Data?
```

Reported by **ns-1364.awsdns-42.org** on 5/28/2025 at **11:54:56 AM (UTC 0)**, just for you.

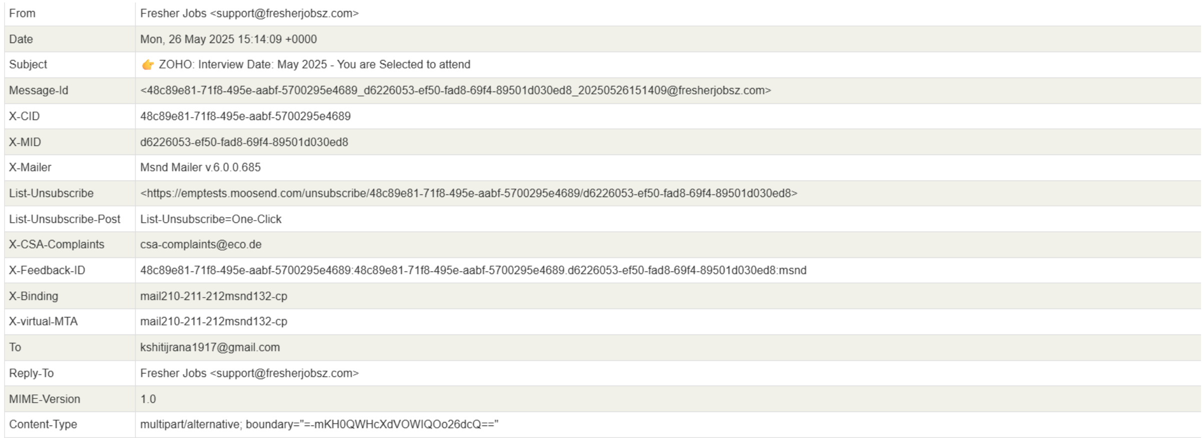
Transcript

```
Dkim Signature Error:
There must be at least one aligned DKIM-Signature for the message to be considered aligned. - more info
```

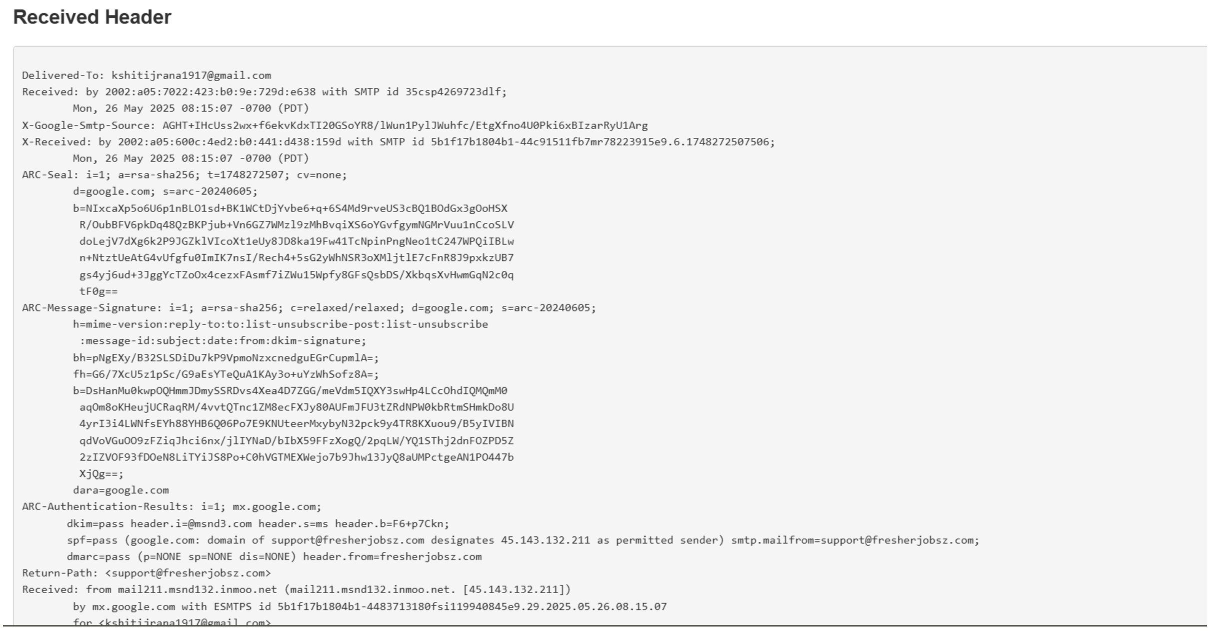


Headers Found

Header Name	Header Value
Delivered-To	kshitijrana1917@gmail.com
X-Google-Smtp-Source	AGHT+IHcUss2wx+f6ekvKdxTI20GSoYR8/lWun1PylJWuhfc/EtgXfno4U0Pki6xBIzarRyU1Arg
X-Received	by 2002:a05:600c:4ed2:b0:441:d438:159d with SMTP id 5b1f17b1804b1-44c91511fb7mr78223915e9.6.1748272507506; Mon, 26 May 2025 08:15:07 -0700 (PDT)
ARC-Seal	i=1; a=rsa-sha256; t=1748272507; cv=none; d=google.com; s=arc-20240605; b=NIxcaXp5o6U6p1nBLO1sd+BK1WCtDjYvbe6+q+6S4Md9rveUS3cBQ1BOdGx3gOoHSX R/OubBFV6pkDq48QzBKPjub+Vn6GZ7WMzl9zMhBvqiXS6oYGvfgymNGMrVuu1nCcoSLV doLejV7dXg6k2P9JGZklVIcoXt1eUy8JD8ka19Fw41TcNpinPngNeo1tC247WPQiIBLw n+NtztUeAtG4vUfgfu0ImIK7nsI/Rech4+5sG2yWhNSR3oXMljtlE7cFnR8J9pxkzUB7 gs4yj6ud+3JggYcTZoOx4cezxFAsmf7iZWu15Wpfy8GFsQsbDS/XkbqsXvHwmGqN2c0q tF0g==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605; h=mime-version:reply-to:to:list-unsubscribe-post:list-unsubscribe :message-id:subject:date:from:dkim-signature; bh=pNgEXy/B32SLSDiDu7kP9VpmoNzxcnedguEGrCupmlA=; fh=G6/7XcU5z1pSc/G9aEsYTeQuA1KAy3o+uYzWhSofz8A=; b=DsHanMu0kwpOQHmmJDmySSRDvs4Xea4D7ZGG/meVdm5IQXY3swHp4LCcOhdIQMQmM0 aqOm8oKHeujUCRaqRM/4vvtQTnc1ZM8ecFXJy80AUFmJFU3tZRdNPW0kbRtmSHmkDo8U 4yrI3i4LWNfsEYh88YHB6Q06Po7E9KNUteerMxybyN32pck9y4TR8KXuou9/B5yIVIBN qdVoVGuOO9zFZiqJhci6nx/jlIYNaD/bIbX59FFzXogQ/2pqLW/YQ1SThj2dnFOZPD5Z 2zIZVOF93fDOeN8LiTYiJS8Po+C0hVGTMEXWejo7b9Jhw13JyQ8aUMPctgeAN1PO447b XjQg==; dara=google.com
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@msnd3.com header.s=ms header.b=F6+p7Ckn; spf=pass (google.com: domain of support@fresherjobsz.com designates 45.143.132.211 as permitted sender) smtp.mailfrom=support@fresherjobsz.com; dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=fresherjobsz.com
Return-Path	<support@fresherjobsz.com>
Received-SPF	pass (google.com: domain of support@fresherjobsz.com designates 45.143.132.211 as permitted sender) client-ip=45.143.132.211;
Authentication-Results	mx.google.com; dkim=pass header.i=@msnd3.com header.s=ms header.b=F6+p7Ckn; spf=pass (google.com: domain of support@fresherjobsz.com designates 45.143.132.211 as permitted sender) smtp.mailfrom=support@fresherjobsz.com; dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=fresherjobsz.com
DKIM-Signature	v=1; a=rsa-sha256; d=msnd3.com; s=ms; c=relaxed/relaxed; q=dns/txt; t=1748272449; h=subject:to:list-unsubscribe:list-unsubscribe-post:mime-version:from: reply-to:date:content-type:content-transfer-encoding:x-csa-complaints; bh=pNgEXy/B32SLSDiDu7kP9VpmoNzxcnedguEGrCupmlA=; b=F6+p7CknjDvhcZmbJOrwunjCgteUtlSM9WoduYsAGzjg85bSJBs6UtvW2DGQWy8iNknFt1VbJB9 ycel5ssnlrr3xwlgmVCw6GYcIC1Jpu+VZXJT9OXgn6PxAuVGTJn2FbCFUFpsnPKzJ5tjkY/Dmr7sq kmh2ol8HkXwPeC0WDGc=
From	Fresher Jobs <support@fresherjobsz.com>
Date	Mon, 26 May 2025 15:14:09 +0000
Subject	👉 ZOHO: Interview Date: May 2025 - You are Selected to attend
Message-Id	<48c89e81-71f8-495e-aabf-5700295e4689_d6226053-ef50-fad8-69f4-89501d030ed8_20250526151409@fresherjobsz.com>
X-CID	48c89e81-71f8-495e-aabf-5700295e4689

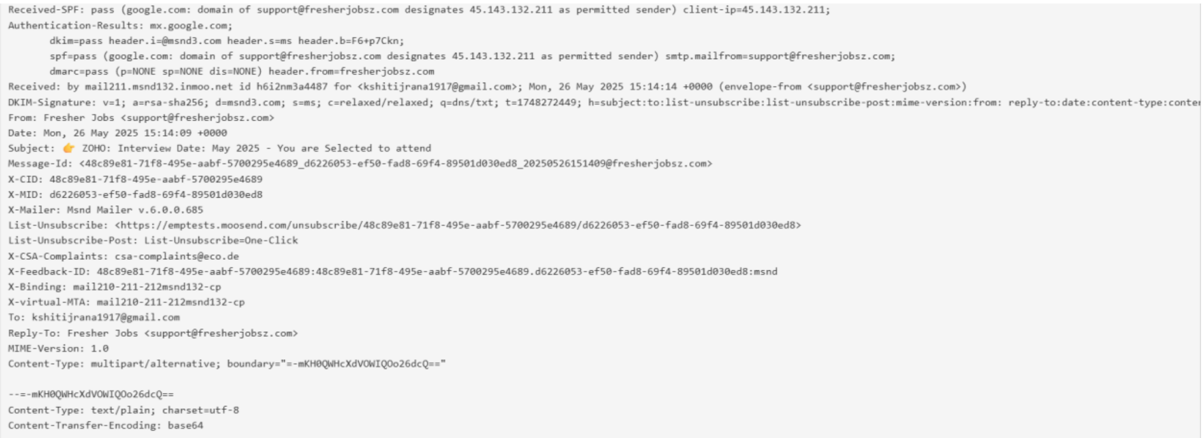


From	Fresher Jobs <support@fresherjobsz.com>
Date	Mon, 26 May 2025 15:14:09 +0000
Subject	👉 ZOHO: Interview Date: May 2025 - You are Selected to attend
Message-Id	<48c89e81-71f8-495e-aabf-5700295e4689_d6226053-ef50-fad8-69f4-89501d030ed8_20250526151409@fresherjobsz.com>
X-CID	48c89e81-71f8-495e-aabf-5700295e4689
X-MID	d6226053-ef50-fad8-69f4-89501d030ed8
X-Mailer	Msnd Mailer v.6.0.0.685
List-Unsubscribe	<https://emptests.moosend.com/unsubscribe/48c89e81-71f8-495e-aabf-5700295e4689/d6226053-ef50-fad8-69f4-89501d030ed8>
List-Unsubscribe-Post	List-Unsubscribe=One-Click
X-CSA-Complaints	csa-complaints@eco.de
X-Feedback-ID	48c89e81-71f8-495e-aabf-5700295e4689:48c89e81-71f8-495e-aabf-5700295e4689.d6226053-ef50-fad8-69f4-89501d030ed8:msnd
X-Binding	mail210-211-212msnd132-cp
X-virtual-MTA	mail210-211-212msnd132-cp
To	kshitijrana1917@gmail.com
Reply-To	Fresher Jobs <support@fresherjobsz.com>
MIME-Version	1.0
Content-Type	multipart/alternative; boundary="=-mKH0QWHcXdVOWIQOo26dcQ=="



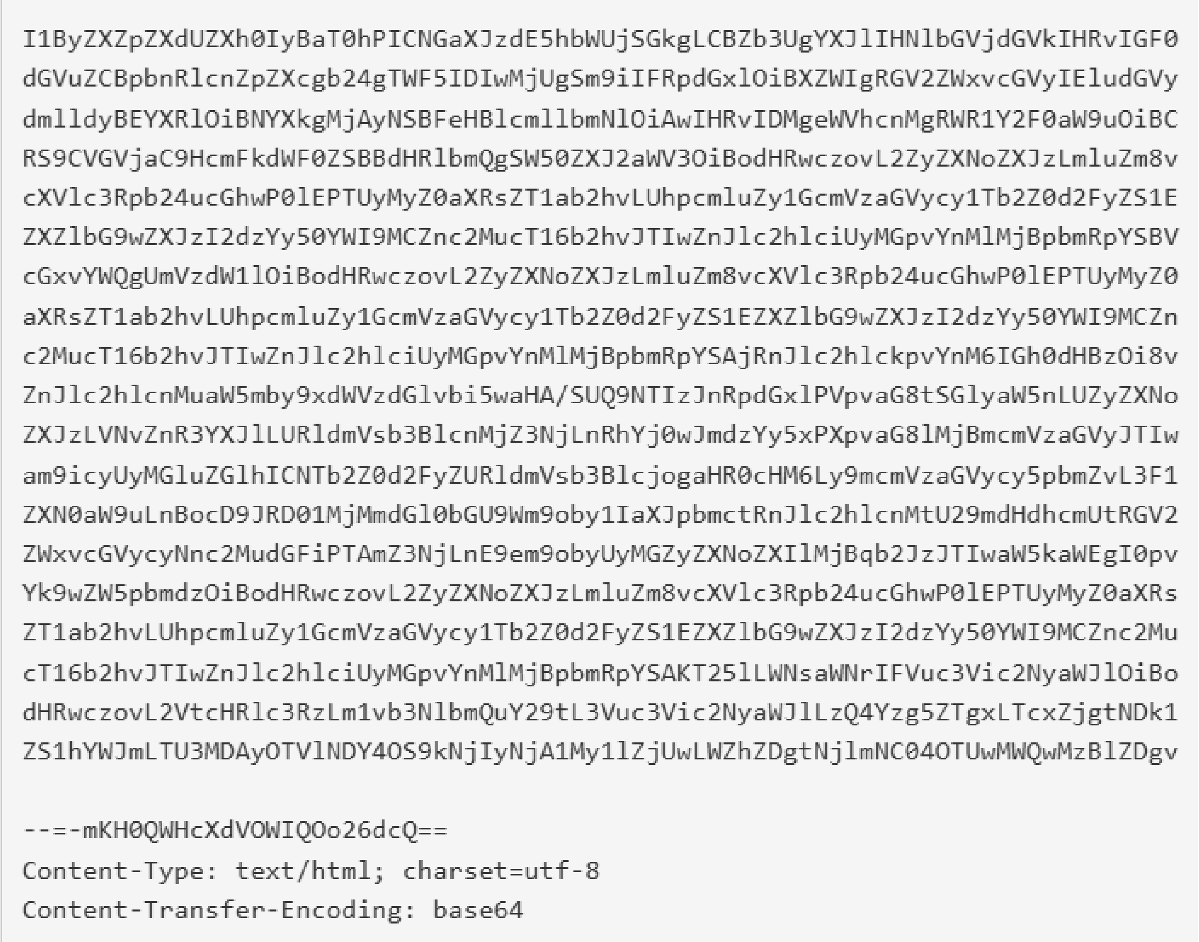
Received Header

```
Delivered-To: kshitijrana1917@gmail.com
Received: by 2002:a05:7022:423:b0:9e:729d:e638 with SMTP id 35csp4269723dlf;
        Mon, 26 May 2025 08:15:07 -0700 (PDT)
X-Google-Smtp-Source: AGHT+IHcUss2wx+f6ekvKdxTI20GSoYR8/lWun1PylJWuhfc/EtgXfno4U0Pki6xBIzarRyU1Arg
X-Received: by 2002:a05:600c:4ed2:b0:441:d438:159d with SMTP id 5b1f17b1804b1-44c91511fb7mr78223915e9.6.1748272507506;
        Mon, 26 May 2025 08:15:07 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1748272507; cv=none;
        d=google.com; s=arc-20240605;
        b=NIxcaXp5o6U6p1nBLO1sd+BK1WCtDjYvbe6+q+6S4Md9rveUS3cBQ1BOdGx3gOoHSX
         R/OubBFV6pkDq48QzBKPjub+Vn6GZ7WMzl9zMhBvqiXS6oYGvfgymNGMrVuu1nCcoSLV
         doLejV7dXg6k2P9JGZklVIcoXt1eUy8JD8ka19Fw41TcNpinPngNeo1tC247WPQiIBLw
         n+NtztUeAtG4vUfgfu0ImIK7nsI/Rech4+5sG2yWhNSR3oXMljtlE7cFnR8J9pxkzUB7
         gs4yj6ud+3JggYcTZoOx4cezxFAsmf7iZWu15Wpfy8GFsQsbDS/XkbqsXvHwmGqN2c0q
         tF0g==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605;
        h=mime-version:reply-to:to:list-unsubscribe-post:list-unsubscribe
         :message-id:subject:date:from:dkim-signature;
        bh=pNgEXy/B32SLSDiDu7kP9VpmoNzxcnedguEGrCupmlA=;
        fh=G6/7XcU5z1pSc/G9aEsYTeQuA1KAy3o+uYzWhSofz8A=;
        b=DsHanMu0kwpOQHmmJDmySSRDvs4Xea4D7ZGG/meVdm5IQXY3swHp4LCcOhdIQMQmM0
         aqOm8oKHeujUCRaqRM/4vvtQTnc1ZM8ecFXJy80AUFmJFU3tZRdNPW0kbRtmSHmkDo8U
         4yrI3i4LWNfsEYh88YHB6Q06Po7E9KNUteerMxybyN32pck9y4TR8KXuou9/B5yIVIBN
         qdVoVGuOO9zFZiqJhci6nx/jlIYNaD/bIbX59FFzXogQ/2pqLW/YQ1SThj2dnFOZPD5Z
         2zIZVOF93fDOeN8LiTYiJS8Po+C0hVGTMEXWejo7b9Jhw13JyQ8aUMPctgeAN1PO447b
         XjQg==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@msnd3.com header.s=ms header.b=F6+p7Ckn;
       spf=pass (google.com: domain of support@fresherjobsz.com designates 45.143.132.211 as permitted sender) smtp.mailfrom=support@fresherjobsz.com;
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=fresherjobsz.com
Return-Path: <support@fresherjobsz.com>
Received: from mail211.msnd132.inmoo.net (mail211.msnd132.inmoo.net. [45.143.132.211])
        by mx.google.com with ESMTPS id 5b1f17b1804b1-4483713180fsi119940845e9.29.2025.05.26.08.15.07
        for <kshitijrana1917@gmail.com>
```



```
Received-SPF: pass (google.com: domain of support@fresherjobsz.com designates 45.143.132.211 as permitted sender) client-ip=45.143.132.211;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@msnd3.com header.s=ms header.b=F6+p7Ckn;
       spf=pass (google.com: domain of support@fresherjobsz.com designates 45.143.132.211 as permitted sender) smtp.mailfrom=support@fresherjobsz.com;
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=fresherjobsz.com
Received: by mail211.msnd132.inmoo.net id h6i2nm3a4487 for <kshitijrana1917@gmail.com>; Mon, 26 May 2025 15:14:14 +0000 (envelope-from <support@fresherjobsz.com>)
DKIM-Signature: v=1; a=rsa-sha256; d=msnd3.com; s=ms; c=relaxed/relaxed; q=dns/txt; t=1748272449; h=subject:to:list-unsubscribe:list-unsubscribe-post:mime-version:from: reply-to:date:content-type:conte
From: Fresher Jobs <support@fresherjobsz.com>
Date: Mon, 26 May 2025 15:14:09 +0000
Subject: 👉 ZOHO: Interview Date: May 2025 - You are Selected to attend
Message-Id: <48c89e81-71f8-495e-aabf-5700295e4689_d6226053-ef50-fad8-69f4-89501d030ed8_20250526151409@fresherjobsz.com>
X-CID: 48c89e81-71f8-495e-aabf-5700295e4689
X-MID: d6226053-ef50-fad8-69f4-89501d030ed8
X-Mailer: Msnd Mailer v.6.0.0.685
List-Unsubscribe: <https://emptests.moosend.com/unsubscribe/48c89e81-71f8-495e-aabf-5700295e4689/d6226053-ef50-fad8-69f4-89501d030ed8>
List-Unsubscribe-Post: List-Unsubscribe=One-Click
X-CSA-Complaints: csa-complaints@eco.de
X-Feedback-ID: 48c89e81-71f8-495e-aabf-5700295e4689:48c89e81-71f8-495e-aabf-5700295e4689.d6226053-ef50-fad8-69f4-89501d030ed8:msnd
X-Binding: mail210-211-212msnd132-cp
X-virtual-MTA: mail210-211-212msnd132-cp
To: kshitijrana1917@gmail.com
Reply-To: Fresher Jobs <support@fresherjobsz.com>
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="=-mKH0QWHcXdVOWIQOo26dcQ=="

--=-mKH0QWHcXdVOWIQOo26dcQ==
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: base64
```



```
I1ByZXZpZXdUZXh0IyBaT0hPICNGaXJzdE5hbWUjSGkgLCBZb3UgYXJlIHNlbGVjdGVkIHRvIGF0
dGVuZCBpbnRlcnZpZXcgb24gTWF5IDIwMjUgSm9iIFRpdGxlOiBXZWIgRGV2ZWxvcGVyIEludGVy
dmlldyBEYXRlOiBNYXkgMjAyNSBFeHBlcmllbmNlOiAwIHRvIDMgeWVhcnMgRWR1Y2F0aW9uOiBC
RS9CVGVjaC9HcmFkdWF0ZSBBdHRlbmQgSW50ZXJ2aWV3OiBodHRwczovL2ZyZXNoZXJzLmluZm8v
cXVlc3Rpb24ucGhwP0lEPTUyMyZ0aXRsZT1ab2hvLUhpcmluZy1GcmVzaGVycy1Tb2Z0d2FyZS1E
ZXZlbG9wZXJzI2dzYy50YWI9MCZnc2MucT16b2hvJTIwZnJlc2hlciUyMGpvYnMlMjBpbmRpYSBV
cGxvYWQgUmVzdW1lOiBodHRwczovL2ZyZXNoZXJzLmluZm8vcXVlc3Rpb24ucGhwP0lEPTUyMyZ0
aXRsZT1ab2hvLUhpcmluZy1GcmVzaGVycy1Tb2Z0d2FyZS1EZXZlbG9wZXJzI2dzYy50YWI9MCZn
c2MucT16b2hvJTIwZnJlc2hlciUyMGpvYnMlMjBpbmRpYSAjRnJlc2hlckpvYnM6IGh0dHBzOi8v
ZnJlc2hlcnMuaW5mby9xdWVzdGlvbi5waHA/SUQ9NTIzJnRpdGxlPVpvaG8tSGlyaW5nLUZyZXNo
ZXJzLVNvZnR3YXJlLURldmVsb3BlcnMjZ3NjLnRhYj0wJmdzYy5xPXpvaG8lMjBmcmVzaGVyJTIw
am9icyUyMGluZGlhICNTb2Z0d2FyZURldmVsb3BlcjogaHR0cHM6Ly9mcmVzaGVycy5pbmZvL3F1
ZXN0aW9uLnBocD9JRD01MjMmdGl0bGU9Wm9oby1IaXJpbmctRnJlc2hlcnMtU29mdHdhcmUtRGV2
ZWxvcGVycyNnc2MudGFiPTAmZ3NjLnE9em9obyUyMGZyZXNoZXIlMjBqb2JzJTIwaW5kaWEgI0pv
Yk9wZW5pbmdzOiBodHRwczovL2ZyZXNoZXJzLmluZm8vcXVlc3Rpb24ucGhwP0lEPTUyMyZ0aXRs
ZT1ab2hvLUhpcmluZy1GcmVzaGVycy1Tb2Z0d2FyZS1EZXZlbG9wZXJzI2dzYy50YWI9MCZnc2Mu
cT16b2hvJTIwZnJlc2hlciUyMGpvYnMlMjBpbmRpYSAKT25lLWNsaWNrIFVuc3Vic2NyaWJlOiBo
dHRwczovL2VtcHRlc3RzLm1vb3NlbmQuY29tL3Vuc3Vic2NyaWJlLzQ4Yzg5ZTgxLTcxZjgtNDk1
ZS1hYWJmLTU3MDAyOTVlNDY4OS9kNjIyNjA1My1lZjUwLWZhZDgtNjlmNC04OTUwMWQwMzBlZDgv
```

```
--=-mKH0QWHcXdVOWIQOo26dcQ==
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: base64
```

5. Summary of Phishing Indicators Identified

Indicator Type	**Details**
Sender Email	it-support@securelogin-account.com – spoofed, illegitimate domain
Subject Line	"Important: Immediate Account Verification Required" – urgency tactic
Domain Analysis	Recently registered, privacy-protected, no verifiable ownership info
File Attachment	SecureLogin.html – flagged by VirusTotal (8/65 engines detected malware)
Embedded Link	Redirects to a fake Microsoft 365 login – listed in phishing databases
Email Header Check	SPF failed, DKIM not aligned, DMARC check failed
Language Used	Generic salutation, spelling/grammar issues, no personalized content

6. Key Learnings

- **Phishing relies heavily on human manipulation**, emphasizing the need for user education alongside technical controls.
- **Email headers are valuable tools** for tracing spoofed messages and identifying forged senders.
- **Sandboxing and threat intelligence platforms** such as VirusTotal are essential for detecting malware-laden files or URLs.
- **Domain investigation techniques** can reveal patterns commonly used in phishing campaigns (e.g., recent registration, anonymity).
- **Thorough documentation of IOCs** is crucial for reporting incidents and improving organizational security postures.

---

7. Conclusion

This phishing investigation task provided practical exposure to one of the most common cyber threats faced by individuals and organizations today. By following a systematic approach and leveraging cybersecurity tools, I was able to detect and analyze key indicators of a phishing attack. This experience improved my technical skills, critical thinking, and awareness of the evolving tactics used by threat actors. It reinforced the importance of vigilance, layered defense strategies, and prompt response in the field of cybersecurity.