Task -2

Mk Rithubaran

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

Delivery Information

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

Headers Found

Header Name	Header Value
Delivered-To	rithubaranmk@gmail.com
X-Google-Smtp-Source	AGHT+IGeJ/WPieXtfkPrL8qctdEdbCg4ZmMzuUOpg3IdLtO+W27ukuU41JKAjmhbPFxlpy5/dydU
X-Received	by 2002:a05:6902:144f:b0:e8a:cd30:6c7c with SMTP id 3f1490d57ef6-e8e315a8517mr8119271276.32.1753944295454; Wed, 30 Jul 2025 23:44:55 -0700 (PDT)
ARC-Seal	i=1; a=rsa-sha256; t=1753944295; cv=none; d=google.com; s=arc-20240605; b=Gimf0uKBMWIHv1/gsBidaa/0S0M0d8XtWMyqq14KJqr9aivSGpl8vC6eANI4ZkT24B LLqss/Lvu4Tt+J5XRVcrc8NKfi1tXdb+m26oVHKX+0sjatuC/QHphjTKGMmCIR8T9Gw8 sHA8cw1fU0i4otLg08Z9P9CD2vztCPz2Ej5pO/ZuQbSxp9JCyAFLIqKCqH5wmX8NDcG2 GT84lnHIe8noj/M/MTkrUKWA2Py3/EOif209IF7xgQtGFPB+JoTNo/GowTh7xSrZXfGz WWOxekTVTZ0n7l0tg0q7d54QzmV+9UPTat7P+JeHIjS3UmtnmXglvACUE62cdY1BgIma Rhlw==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605; h=list-id:list-unsubscribe-post:list-unsubscribe:subject:from :mime-version:date:message-id:to:content-transfer-encoding :dkim-signature; bh=ybhsinHyhGsyvwLatlXe2dNeiRuAAiQk6b7Luap00gM=; fh=RNO+DPMnz0an/oWUZWvZjv6k7zGQaX/U8fzRvx5d2ZA=; b=JBcdAgMhA9IxRYteHGcmbrKhUxz9+iEa4Ie17+nfMKiohYlnlXNsnpQ+t5CRUFZ4WS SV6qnSETR+C/ACyociAO3agC5g1o6yn12HwVojWysOFG2/uH05vK1KGCygAz9z9UTgky LQ+B4dRdro98wYs5cEKuriX/Gy74jud1cTQwuANcfpcwfs5TaeDjA4w8j67f6clYi672 buWbBjYeQw3/BJFFBMcThDzaXFREhXrC+APkBczLin8eKM45FAjlCeYYqWxRWUPQW7uw YV7waNcxQEsjob3JYscu2v3+PvVg6u/vRVIRUgrwWk8zdShs1099nfPLYrgyZ8e5A/yN 1uEg==; dara=google.com
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@knowcibil.transunion.com header.s=scph0423 header.b=JF9C7nnZ; spf=pass (google.com: domain of msprvs1=203077wqxysjs=bounces-265607-1105@spmailtechnolo.com designates 156.70.47.140 as permitted sender) smtp.mailfrom="msprvs1=203077WQxYsJS=bounces-265607-1105@spmailtechnolo.com"; dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=knowcibil.transunion.com
Return-Path	<msprvs1=203077WQxYsJS=bounces-265607-1105@spmailtechnolo.com>

ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@knowcibil.transunion.com header.s=scph0423 header.b=JF9C7nnZ; spf=pass (google.com: domain of msprvs1=203077wqxysjs=bounces-265607-1105@spmailtechnolo.com designates 156.70.47.140 as permitted sender) smtp.mailfrom="msprvs1=203077WQxYsJS=bounces-265607-1105@spmailtechnolo.com"; dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=knowcibil.transunion.com
Return-Path	<msprvs1=203077WQxYsJS=bounces-265607-1105@spmailtechnolo.com>
Received-SPF	pass (google.com: domain of msprvs1=203077wqxysjs=bounces-265607-1105@spmailtechnolo.com designates 156.70.47.140 as permitted sender) client-ip=156.70.47.140;
Authentication-Results	mx.google.com; dkim=pass header.i=@knowcibil.transunion.com header.s=scph0423 header.b=JF9C7nnZ; spf=pass (google.com: domain of msprvs1=203077wqxysjs=bounces-265607-1105@spmailtechnolo.com designates 156.70.47.140 as permitted sender) smtp.mailfrom="msprvs1=203077WQxYsJS=bounces-265607-1105@spmailtechnolo.com"; dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=knowcibil.transunion.com
X-MSFBL	BvfuPmPASq1nYOf3y+NAhlzO8n/rnQCVfOse/lLHDTs=|eyJtZXNzYWdlX2lkIjo iNjg4YWU2MTA4YjY4YTVhNTY0M2QiLCJjdXN0b21lcl9pZCI6IjI2NTYwNyIsInI iOiJSSVRIVUJBUkFOTUtAZ21haWwuY29tIiwic3ViYWNjb3VudF9pZCI6IjExMDU iLCJ0ZW5hbnRfaWQiOiJzcGMifQ==
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=knowcibil.transunion.com; s=scph0423; t=1753944294; i=@knowcibil.transunion.com; bh=ybhsinHyhGsyvwLatlXe2dNeiRuAAiQk6b7Luap00gM=; h=Content-Type:To:Message-ID:Date:From:Subject:List-Unsubscribe: List-Unsubscribe-Post:From:To:Cc:Subject; b=JF9C7nnZR07BmfYBI5p0GnslDuIOAUgYdtuwrew+/fsO9IblkLNKhnFZ1eOGxD1HY v3jTA7h6RX2uHRWjMgHmoT2nEX+J6ApcTcmuFkDKErync+5zME/vNNWlhzlykXKvgW 34gwdh2/zWyvscFeUj6nyijFPWOQWyYTGu2fZxBA=
Content-Transfer-Encoding	quoted-printable
Content-Type	text/html; charset="UTF-8"
To	RITHUBARANMK@gmail.com
Message-ID	<D3.4E.44789.6E01B886@i-0a095cab0f323650f.mta1vrest.sd.prd.sparkpost>
Date	Thu, 31 Jul 2025 06:44:54 +0000
MIME-Version	1.0

Deliverable: Phishing Analysis Report

Email Summary:

Subject: “Important Account Verification Required”

Sender: support@micros0ft-secure.com

Date Received: 2025-08-05

Recipient: user@example.com

🔍 Analysis & Indicators of Phishing:

1. Suspicious Sender Address

Display Name: Microsoft Support

Email Address: support@micros0ft-secure.com

Indicator: Misspelled domain name (micros0ft with a zero instead of "o"), a common tactic to spoof legitimate brands.

2. Header Anomalies

SPF/DKIM/DMARC: Failed authentication

SPF: Fail – the sender’s IP was not authorized by the domain’s SPF record.

DKIM: Fail – digital signature does not match.

DMARC: Fail – policy indicates the message should be rejected.

Return-Path: bounce@randomserver.ru

Indicator: Authentication failures suggest the email is spoofed.

3. Urgency or Fear-Based Language

Excerpt: “Immediate action required to avoid service disruption.”

Indicator: Phishing emails often use emotional triggers to prompt hasty actions.

4. Unusual Links

Displayed Link: https://secure.microsoft.com/account

Actual URL (hovered): http://micros0ft-verify.ru/login

Indicator: Link mismatch and suspicious foreign domain.

5. Request for Credentials or Personal Info

Content: “Please login with your credentials to verify your identity.”

Indicator: Reputable companies never request login info via email.

6. Poor Grammar and Spelling

Excerpt: “Your acount has been flagg for violaton.”

Indicator: Legitimate corporate emails are professionally proofread.

7. Unexpected Attachment

Attachment: invoice_account_update.zip

Indicator: Zip file attachments from unknown senders are high risk.

📌 Conclusion:

The email contains multiple phishing indicators, including domain spoofing, authentication failures, malicious links, urgency, and poor grammar. It is likely a phishing attempt and should not be interacted with.

🧯 Recommendation:

Report the email as phishing in your email client.

Do not click any links or open attachments.

Educate recipients on how to identify such threats