Task 2

1. Obtain a Sample phishing email

Your Microsoft Account Password Has Been Reset - Confirm Immediately

M **Microsoft Support** <security-alert@microsoft-verification-center.com>

To: you@example.com

Tue, 9 Dec 2025 18:22:14 ++0530

Hello User,

We have detected an unauthorized attempt to reset your Microsoft account password from a new device located in:

Location: Singapore
IP Address: 103.19844.67

For your protection, we have temporarily disable d account access until you verify your identity.

👉 Confirm Your Identity
https://microsoft.account-verfiy-center.com/security-check

If this action was not performed by you, please download the attached report (SecurityLog_Report.rar) and follow the instructions to secure your account.

Failure to verify within 24 hours will result in permanent account restriction.

Thank you,
Microsoft Security Team

2. Examination.

Email Spoofing is used by an attacker to show that it came from a trusted company by which they can trick the users to click their malicious link and compromise them.

Here in this email the display name `Microsoft Support` looks real and trustworthy.

The domain `microsoft-verificationcenter.com` is NOT an official Microsoft domain. Microsoft uses trusted domains like microsoft.com, outlook.com, and account.microsoft.com.

Although the display name says 'Microsoft Support', the real sender is identified by the domain after @, which is fake.

This is where spoofing became obvious

Here the attacker used a generic greeting `Hello User` instead of the user's real name.

The sender IP `207.182.142.88` does not belong to Microsoft and is associated with ENET-2 hosting, not Microsoft infrastructure.

In this email an attacker attached a file named `SecurityLog_Report.rar` while `.rar` extension is used to compress the files and are commonly used to hide malware.

Legitimate companies **never** send emails from:

- Weird long domains
- Domains with "verify/secure/account" inside
- Recently registered domains
- Domains with spelling mistakes

Phishing email uses `microsoft-verificationcenter.com` here sender domain and linked domain does-not match.

While in Confirm your identity link `verify` is spelled wrong it is written `verfiy`

Poor Formatting & Inconsistent Footer

- Not formatted like real Microsoft emails.
- Missing logos and trusted brand elements.

3. Header analysis

```
Return-Path: <security-alert@microsoft-verificationcenter.com>
Received: from mail.microsoft-verificationcenter.com (207.182.142.88)
    by mx.google.com with ESMTP id h8si192830qke.122.2025.12.09.12.52.11
    for <you@example.com>;
    Tue, 09 Dec 2025 12:52:11 -0800 (PST)
Received-SPF: fail (google.com: domain of security-alert@microsoft-verificati
oncenter.com
    does not designate 207.182.142.88 as permitted sender) client-ip=207.182.14
2.88;
Authentication-Results: mx.google.com;
    spf=fail;
    dkim=none;
    dmarc=fail;
Message-ID: <c79uiwr32.9sd8910@microsoft-verificationcenter.com>
From: Microsoft Support <security-alert@microsoft-verificationcenter.com>
To: you@example.com
Subject: Your Microsoft Account Password Has Been Reset – Confirm Immedi
ately
Date: Tue, 09 Dec 2025 18:22:14 +0530
MIME-Version: 1.0
Content-Type: text/html; charset="UTF-8"
```

Mail header analysis

Address Details

Mail From:	security-alert@microsoft-verificationcenter.com	**Mail To:**	you@example.com
Mail From Name:	Microsoft Support	**Reply To:**	

Message Details

Subject:	Your Microsoft Accoun t Password Has Been R eset – Confirm Immedi ately	**Content-Type:**	text/html charset=UTF-8
Date:	Tue, 09 Dec 2025 18:22:14 +0530	**UTC Date**	Tue Dec 9 12:52:14 2025
MessageID:	c79uiwr32.9sd8910@microsoft-verificationcenter.com		

Message Transfer Agent (MTA) - Transfer Details

Mail Server From:	mail.microsoft-verificationcenter.com	**Mail Server To:**	
Mail Server From IP:	207.182.142.88	**Mail Server To IP:**	
Mail Country From:	United States	**Mail Country To:**	Country/Code/Continent: // Longitude:/ Latitude:
AS Name From:	ENET-2	**AS Name To:**	
AS Number From:	AS10297	**AS Number To:**	
Distance (All Hops/Summary):	0/ KM	**Hops (All/Public):**	1 /
MTA Encryption	Good (*)	**Delivery Time:**	0
Your IP:	117.204.10.112	**Your GeoLoc:**	Lat:20.0024 Lon:73.7945

Daily hit counter = of

Spam Scoring Details

Score	Spam Description
1.0	RBL: ADMINISTRATOR NOTICE: The query to
0.6	HTML-only message, but there is no HTML tag
0.0	Missing DMARC policy
1.0	RBL: ADMINISTRATOR NOTICE: The
1.0	RBL: ADMINISTRATOR NOTICE: The query to
0.0	RBL: ADMINISTRATOR NOTICE: The query to DNSWL
0.0	SPF: sender does not publish an SPF Record
0.0	SPF: HELO does not publish an SPF Record
0.8	No valid author signature and domain not in DNS
1.1	Date: is 6 to 12 hours before Received: date
0.1	BODY: Message only has text/html MIME parts

Total Score (Max:5.0)	Spamassassin prediction
5.6	This Mailheader is possible Spam!

Hop Details

Hop 1/1	Public / Internal Mail Routing		
By MTA	mx.google.com	By IP	UNKNOWN (*)
From MTA	mail.microsoft-verificationcenter.com	From IP	207.182.142.88 (*)
From AS Nbr	AS10297	From AS Name	ENET-2
From Geo	Lat:39.9671 Lon:-83.0044	From Next City	(*)
Date MTA	Tue, 09 Dec 2025 12:52:11 -0800	UTC Date	Tue Dec 9 20:52:11 2025
Epoch	1765284731	For	you@example.com
MTA Encryption	Not encrypted (internal)		
RAW MESSAGE	Received: from mail.microsoft-verificationcenter.com (207.182.142.88) by mx.google.com with ESMTP id h8si192830qke.122.2025.12.09.12.52.11 for you@example.com ; Tue, 09 Dec 2025 12:52:11 -0800 (PST) Received-SPF: fail (google.com: domain of security-alert@microsoft-verificationcenter.com does not designate 207.182.142.88 as permitted sender) client-ip=207.182.142.88; Authentication-Results: mx.google.com; spf=fail; dkim=none; dmarc=fail;		

The email header analysis clearly identifies multiple signs of phishing:

- Sender domain is fake (`microsoft-verificationcenter.com`)
- Sender IP (`207.182.142.88`) is not a Microsoft-owned server
- SPF = fail
- DKIM = none

- DMARC = fail
- Message-ID contains fake domain
- Routing path does not match Microsoft mail servers
- Spam score: **5.6 / 5**, marked as possible spam
- Timestamp mismatches and no encryption
- Overall: **Email is spoofed and malicious**

All email authentication mechanisms failed, proving this email was not sent by Microsoft servers.

These indicators confirm that the email is **not from Microsoft** and is part of a **phishing attempt** impersonating account security notifications.