Task 2: Phishing Email Analysis Report

Phishing Email Sample:

From: Microsoft Account Team <support@microsoft-alertverify.com>
To: user@example.com
Subject: [Action Required] Unusual sign-in activity detected

Dear User,

We noticed an unusual sign-in attempt from an unknown device. For your safety, we have temporarily locked your Microsoft account.

👉 To restore access, please verify your identity by clicking the link below:

[Verify Now](http://microsoft.support-loginalert.com/verify)

If no action is taken within the next 24 hours, your account will be permanently disabled.

Thank you for your immediate attention,
Microsoft Account Team

Phishing Indicator:

1. **Spoofed Email Address:**The sender email address is **support@microsoft-alertverify.com**, which is **not an official Microsoft domain**. It attempts to spoof Microsoft by including "microsoft" in the domain name, but it is actually a fake domain. This is a clear sign of phishing.

2. **Suspicious Link:**The link text says "Verify Now," which appears trustworthy. However, when hovering over the link (or viewing the source), the actual URL is:

`http://microsoft.support-loginalert.com/verify`

This is a **fake domain** designed to look like Microsoft. Real Microsoft links would start with `https://login.microsoftonline.com` or `https://account.microsoft.com`.

3. **Urgent or Threatening Language:**The email uses threatening language such as “your account will be permanently disabled” and creates urgency by stating a 24-hour deadline.
This is a common phishing tactic to make the victim act without thinking.
Legitimate companies rarely use such pressure-based wording.

4. **Grammar and Language Style:**The email uses a **generic greeting** (“Dear User”) and the tone is unnatural and robotic.While there may not be obvious spelling mistakes, the wording is unprofessional and overly aggressive. This lack of personalization and poor tone is typical in phishing emails.

Summary of Phishing Indicators

Based on the above indicators, this email is clearly a **phishing attempt**.
It tries to trick the user into clicking a malicious link and giving away personal credentials.

Conclusion

This email demonstrates multiple phishing traits designed to trick the user into clicking a malicious link and giving away sensitive information. It is important to recognize such signs early and avoid responding or clicking on any suspicious links.