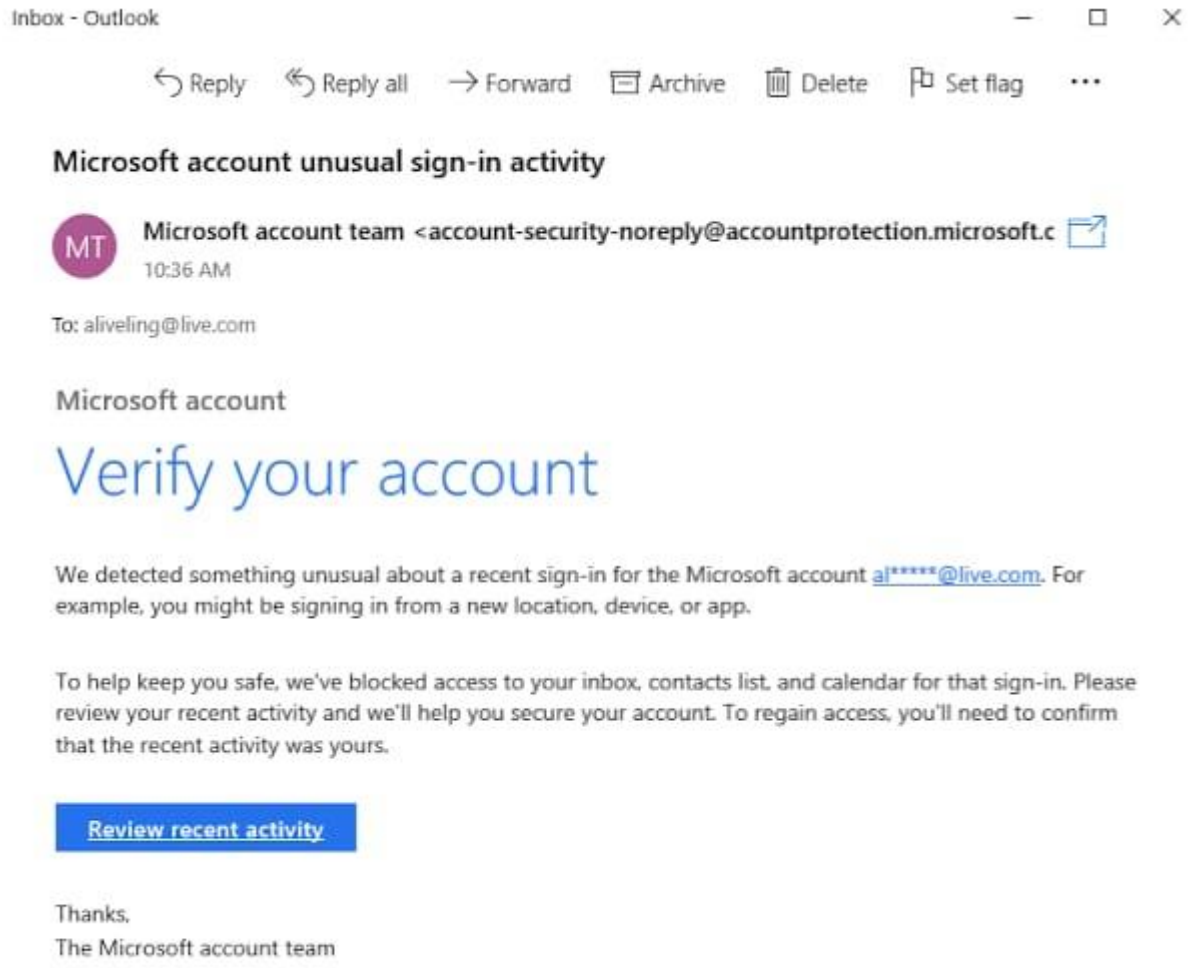
Task 2: Analyse a Phishing Email Sample.

Objective: Identify phishing characteristics in a suspicious email sample.

Sample Phishing Email: 👇👇



Phishing Email Analysis Report:

Email Summary:

- **Subject:** *Microsoft account unusual sign-in activity*
- **Sender Name**: *Microsoft account team*
- **Sender Email:** account-security-noreply@accountprotection.microsoft.c...
- **Displayed Button**: "Review recent activity"

Phishing Indicators Found:

Indicator	Details
1. Suspicious Sender Address	While it seems like a legit Microsoft domain, But it's not real Microsoft address.
2. Generic Greeting	The message is sent to *"aliveiling@live.com"*, but the content says "Verify your account" directly without greeting or no name used — which is common in phishing.
3. Urgency / Fear Tactic	"Unusual sign-in", "blocked access", "help you secure" — this creates urgency and fear, pushing the user to click.
4. Suspicious Button	The CTA is "Review recent activity", but no URL is shown. That's a red flag — hovering over it in a real email would often reveal a phishing domain.
5. Content Style Too Clean	Most real Microsoft alerts contain more structured formatting, Recent Activity Geolocation, Date and Time, security footer, and contact support links. This one lacks that, making it visually suspicious despite being clean.

Conclusion:

This email exhibits multiple phishing traits, including:

- Suspicious Sender Address
- Use of urgency
- No personalized greeting
- Suspicious CTA button
- No verifiable links shown
- No Recent login address, date or time.

That all Indicates that it's a phishing mail sent to the user to trick him to use their personal information. An user must be aware of these type of frauds.

✅ **Outcome:**

This email is highly likely to be a **credential phishing attempt** designed to harvest Microsoft account credentials by luring the victim into clicking on a malicious verification link.

🔒 **Recommendation:**

Do not interact with the email. Report and delete it. Educate users to:

- Always **hover over links** before clicking.
- Check **full sender address.**
- Be cautious of **urgency or fear tactics.**