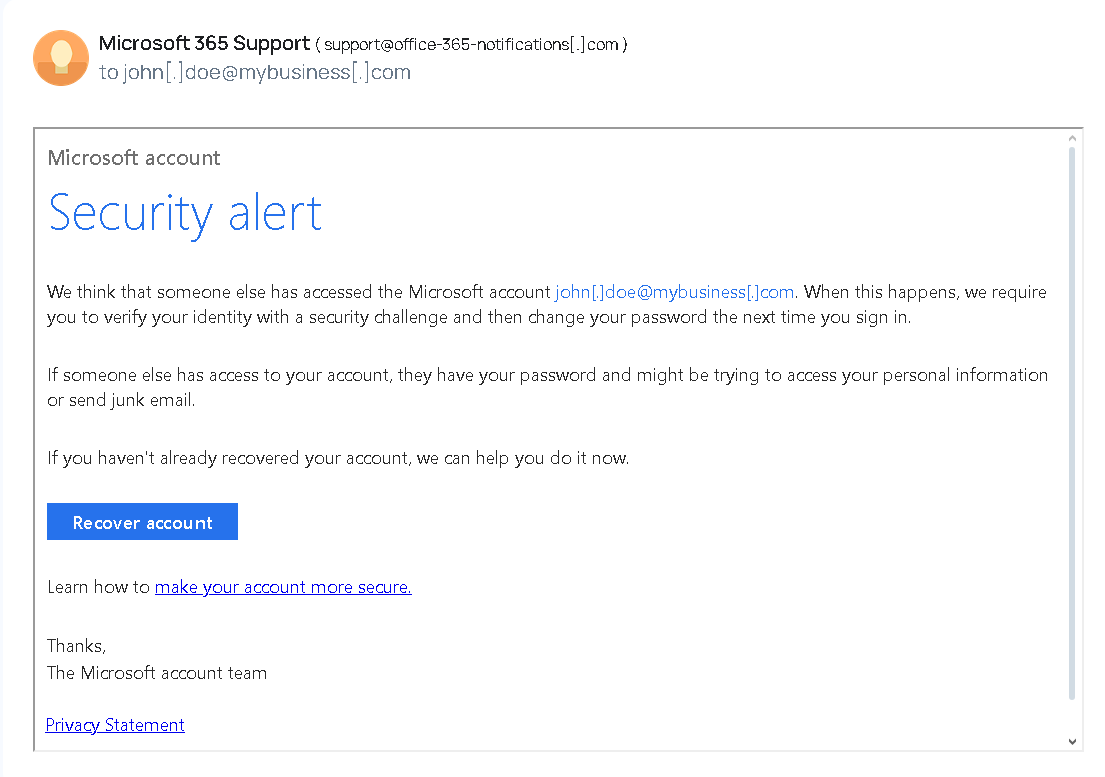
# Phishing Email Analysis Report

Analyst: Nivas

Date: 2025-10-21

## 1.Sample Email (provided)



## 2. Summary Findings

- Sender address: support@office-365-notifications.com (not an official Microsoft domain)

- Urgency / Tone: Creates fear and urges immediate action (account recovery).

- Links: Contains a 'Recover account' call-to-action — destination URL not provided in sample (likely malicious).

- Attachments: None in the provided sample.

- Spelling / Grammar: No obvious spelling errors; professional-looking copy (common in advanced phishing).

- Header analysis: Not available in the provided sample text. If headers are retrieved, check SPF/DKIM/DMARC and Received chain for inconsistencies.

## 3. Social Engineering Techniques Observed

- Exploits fear of account compromise to force quick action.

- Impersonates a trusted brand (Microsoft) to gain user trust.

- Uses a single clear call-to-action (Recover account) to capture credentials.

## 4. Recommendations / Next Steps

- Do NOT click the 'Recover account' link. Do not reply.

- If this targets a real account you own, go directly to the official Microsoft website (https://account.microsoft.com) and check account activity / change password.

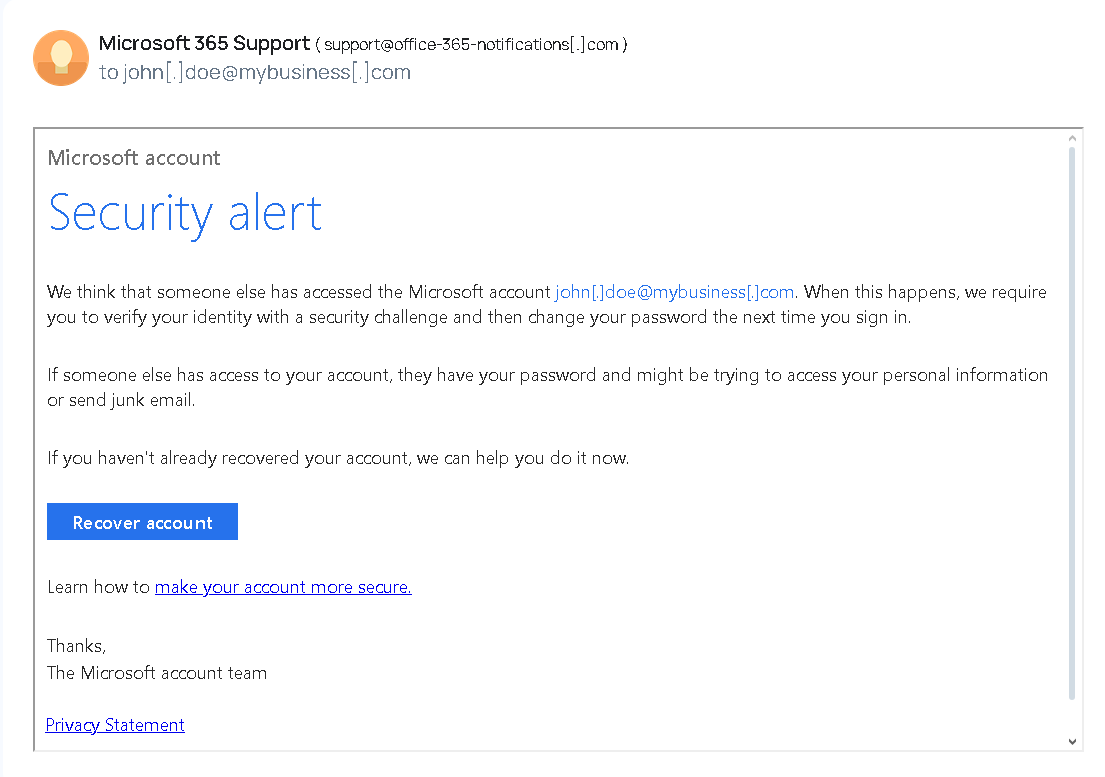
- Report the email to your email provider (e.g., Gmail: Report phishing) or to your organization's IT/Security team.

- If possible, obtain the full email headers and analyze them with an online header analyzer (MXToolbox).

- Enable multi-factor authentication (MFA) on important accounts.

- Block the sender and delete the email after reporting.

## 5. Evidence / Screenshots



## 6. Conclusion

Based on the sender domain and social engineering cues, this email is classified as a phishing attempt trying to harvest account credentials via a fake 'Recover account' link.