Phishing Email Threat Analysis Report

Cyber Security Internship – Task 2

Prepared by: Rajarshi Chakraborty

Date: [24/06/2025]

1. Executive Summary

This report provides a comprehensive analysis of a phishing email sample that masquerades as a Microsoft Office 365 security alert. The email claims that a phishing message was delivered to the recipient due to a user or tenant override, and urges the recipient to “view alert details.” Upon closer inspection, the email displays several strong indicators of phishing, including a spoofed sender domain, brand impersonation, and psychologically manipulative language.

The purpose of this analysis is to identify technical and behavioral indicators of phishing, demonstrate awareness of social engineering tactics, and document best practices for evaluating suspicious email messages in a professional setting.

2. Sample Email Overview

Subject	High-severity alert: Phish delivered due to tenant or user override
Sender Address	microsoft@email-records.com
Displayed Date	January 22, 2021
Platform Spoofed	Microsoft Office 365
Delivery Channel	Email (screenshot-based analysis)

3. Detailed Observations & Indicators

3.1 Spoofed Email Domain

The sender’s email address, microsoft@email-records.com, is misleading and crafted to look authoritative. However, it is not an official Microsoft domain. Email spoofing is a technique used by attackers to forge the 'From' field to appear as if it is from a legitimate entity.

3.2 Use of Visual Brand Impersonation

The email replicates Microsoft’s branding including logos and layout. This tactic is called brand spoofing, and it helps attackers reduce user suspicion.

3.3 Absence of Personalized or Contextual Information

No recipient-specific data is provided. Legitimate security alerts typically include user names, tenant IDs, or reference numbers.

3.4 Emotionally Manipulative Language

The email uses urgency such as 'High-severity alert' to pressure users into clicking the call-to-action without evaluating the risk.

3.5 Suspicious Call to Action (CTA)

The button labeled 'View alert details' is likely linked to a phishing or malware-hosting site.

3.6 Inconsistent Timestamp Formatting

Different times for the same event appear in the message, which indicates a lack of professional formatting.

3.7 Lack of Legitimate Contact Information

The email is signed generically as 'The Office 365 Team' without any verifiable contact details.

4. Risk Assessment

If a recipient were to interact with this email, especially by clicking the CTA button, the potential consequences could include:

- Credential Theft
- Account Compromise
- Malware Installation
- Internal Spread (via Business Email Compromise)

This phishing email poses a medium-to-high risk depending on the environment and awareness level of the recipient.

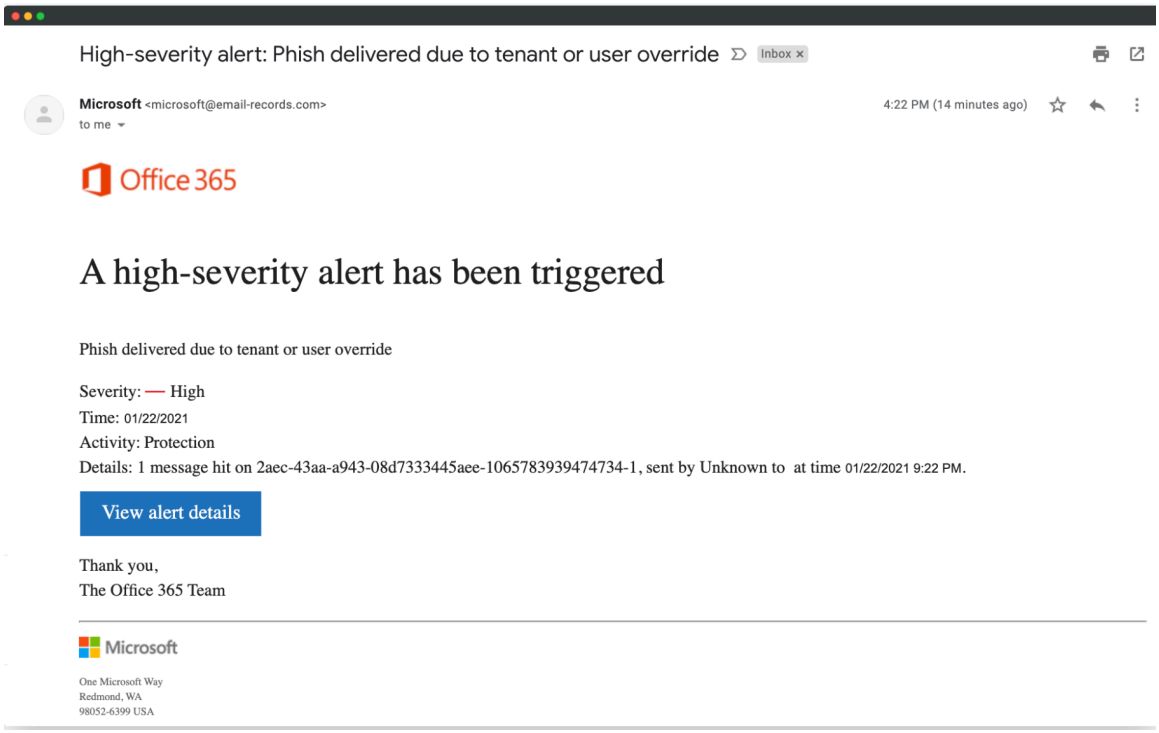
5. Conclusion

This email is a targeted phishing attempt using spoofing, impersonation, and social engineering. Its structure is designed to replicate Microsoft alerts but lacks personalization, technical authenticity, and traceability. Organizations must combine user awareness with technical email security controls to defend against such threats.

6. Attachments

- Screenshot.png – Visual sample of the phishing email
- README.md / Report.docx – Full technical analysis document

Screenshot:


High-severity alert: Phish delivered due to tenant or user override
Inbox ×
Microsoft <microsoft@email-records.com>
to me
4:22 PM (14 minutes ago)
Office 365
A high-severity alert has been triggered
Phish delivered due to tenant or user override
Severity: — High
Time: 01/22/2021
Activity: Protection
Details: 1 message hit on 2aec-43aa-a943-08d7333445aee-1065783939474734-1, sent by Unknown to at time 01/22/2021 9:22 PM.
View alert details
Thank you,
The Office 365 Team
Microsoft
One Microsoft Way
Redmond, WA
98052-6399 USA