Email phishing analysis
Daniel Cruz
6/26

This project analyzes a phishing email impersonating Microsoft Outlook Support. The email was obtained from a public .eml repository and examined using forensic tools to assess its metadata, delivery path, social engineering tactics, and potential indicators of compromise (IOCs). The goal was to identify how the email bypassed authentication and what threat indicators a Tier 1 SOC analyst would use for triage and escalation.

Tools used

github for finding .eml
Thunderbird To safely open and inspect raw email headers and metadata
virus total to detect viruses from attachments
MXToolbox To analyze SPF, DKIM, and DMARC results from raw headers
Google Header Analyzer To trace email routing, delivery path, and delays

Header analysis

Subject: Your account has been flagged for unusual activity
A common phishing tactic to generate fear and urgency.

From: Outlook Support Team <social201712152@social.helwan.edu.eg>
The display name is impersonating Microsoft Outlook. The actual sender address is from a suspicious .edu.eg domain, unrelated to Microsoft.

Return-Path: <social201712152@social.helwan.edu.eg>
The domain helwan.edu.eg is an Egyptian university, not related to Microsoft. Official Outlook support emails would originate from a Microsoft-owned domain like outlook.com or microsoft.com.

Sending IP: 40.107.241.55 — Microsoft Corporation (Austria)
This is a Microsoft-owned cloud IP. Attackers often abuse Microsoft infrastructure (Office 365, Outlook) to send phishing emails from seemingly legitimate servers.

SPF Authenticated Passed
The IP is allowed to be sent on behalf of the `helwan.edu.eg` domain.
SPF Alignment Passed
The `From:` domain and SPF-authenticated domain match.
DKIM Authenticate failed
The DKIM signature was invalid or missing. This may mean the message was altered or forged.

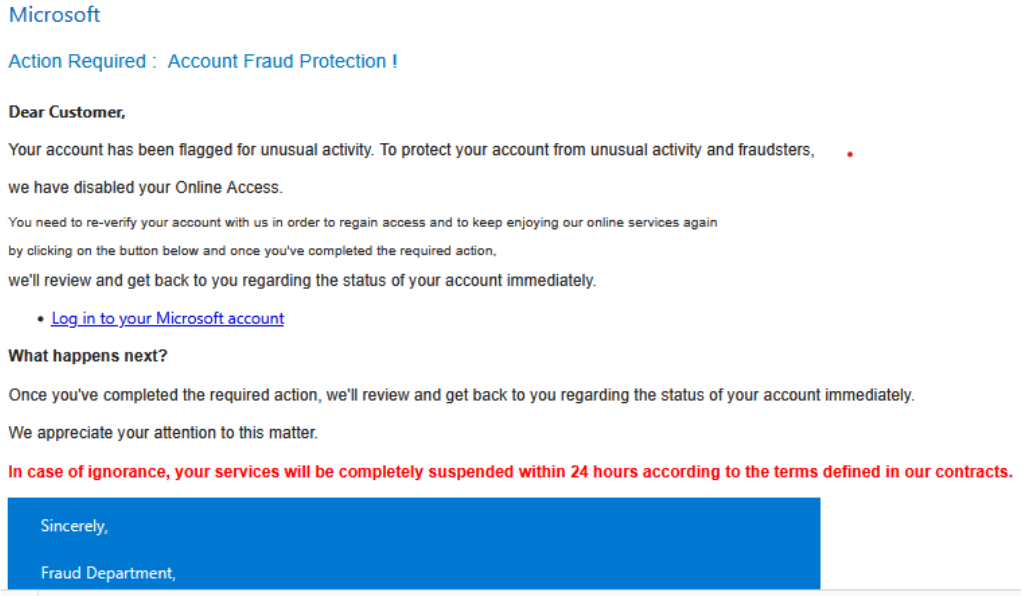
DKIM Alignment failed

The domain used to sign the email (DKIM) did not align with the From domain.

DMARC Compliant failed

Because DKIM failed and SPF alone is insufficient without DKIM or alignment, this email failed DMARC. Indicates potential spoofing.

Body Analysis



Microsoft

Action Required : Account Fraud Protection !

Dear Customer,

Your account has been flagged for unusual activity. To protect your account from unusual activity and fraudsters,

we have disabled your Online Access.

You need to re-verify your account with us in order to regain access and to keep enjoying our online services again

by clicking on the button below and once you've completed the required action,

we'll review and get back to you regarding the status of your account immediately.

- Log in to your Microsoft account

What happens next?

Once you've completed the required action, we'll review and get back to you regarding the status of your account immediately.

We appreciate your attention to this matter.

In case of ignorance, your services will be completely suspended within 24 hours according to the terms defined in our contracts.

Sincerely,

Fraud Department,

Generic Greeting: “Dear Customer” No personalization, a very big sign of phishing attempts .

Urgency and Threats: Mentions account suspension within 24 hours, pressuring the victim to act without thinking.

Fear Language: Words like “fraudsters,” “suspended,” “unusual activity,” and “immediately” are used to invoke panic.

Call to Action: The email urges the recipient to click a button to log in to their Microsoft account.

Malicious Link:
https://share.polymail.io/...

This is a legitimate domain used by Polymail for email tracking and sharing. However, attackers abuse trusted platforms like Polymail to: Host phishing pages Distribute malicious files Appear more credible and bypass domain-based filters Despite being hosted on a legitimate service, the context and the link’s use in a spoofed email suggest it is being weaponized for credential theft or malware delivery.

What to Do: Block sender domain and related URLs at the email gateway.
Add the email address, IP, and link to IOC watchlists in the SIEM. Create correlation rules for: From: domains impersonating Microsoft that fail DMARCSubject lines including “flagged for unusual activity” or “account suspended” Submit the phishing page for sandbox analysis. Notify affected users and security awareness teams.

Final Notes
This project demonstrates foundational skills for a Tier 1 SOC analyst, including:
Email threat triage
IOC extraction
Header and authentication analysis
Social engineering awareness
Communication of threat intelligence