Phishing Email Investigation Report

Analyst: Samuel Jemal
Date of Investigation: 28 October 2025
Incident Type: Phishing (Credential Harvesting)
Severity Level: Medium
Status: Closed

1. Executive Summary

On October 25, 2025, a suspicious email was reported by an employee claiming to be from Microsoft Account Security. The email requested the recipient to verify their credentials due to “unusual sign-in activity.” Upon investigation, it was determined that the email originated from a spoofed domain and contained a malicious phishing link designed to capture user login credentials. The malicious domain was taken down, and no users were compromised.

2. Tools Used

• MXToolbox – Header and SPF/DKIM validation
• VirusTotal – URL and domain scanning
• URLScan.io – Website behavior and screenshot
• AbuseIPDB – IP reputation analysis
• MITRE ATT&CK; Framework – Technique mapping

3. Investigation Process

• Header Analysis: Sender address appeared as security@microsoftsupport.com, but return-path pointed to micros0ft-auth-login.net (SPF failed).
• URL Extraction: Link redirected to hxxps://micros0ft-auth-login[.]net/secure (domain registered recently).
• Threat Verification: URL flagged as malicious on VirusTotal and confirmed by URLScan.io as a fake Microsoft login page.
• IP Analysis: IP 185.165.123.22 had multiple phishing abuse reports.
• Containment: Blocked domain/IP and issued internal advisory.

4. Findings

Indicator Type	Value	Description
Sender Address	security@microsoftsupport.com	Spoofed sender
Return-Path	micros0ft-auth-login.net	Fake domain
URL	hxxps://micros0ft-auth-login[.]net/secure	Phishing page
IP Address	185.165.123.22	Host of malicious domain
MITRE Technique	T1566.002	Phishing: Spearphishing Link

5. MITRE ATT&CK; Mapping

Phase	Technique ID	Technique Name
Initial Access	T1566.002	Phishing: Spearphishing Link
Credential Access	T1056.003	Input Capture (Credential Harvesting)
Command & Control	T1071	Application Layer Protocol

6. Containment & Remediation

• Blocked malicious domain and IP on firewall.
• Updated spam filters to detect similar emails.
• Implemented DMARC and DKIM verification for inbound mail.
• Conducted phishing awareness training for all users.

7. Lessons Learned

• Always verify sender domains carefully, even if they look legitimate.
• Newly registered domains often indicate phishing attempts.
• Early user reporting prevents escalation.
• Continuous awareness training is essential.

8. Analyst Signature

Name: Samuel Jemal
Role: SOC Analyst (Intern)
Date: 28 October 2025