Phishing Incident Analysis Report
Incident: Spoofed Microsoft Account Security Alert

SOC Analyst
`Tier 2 - Incident Response`

October 30, 2025

Abstract

This report details the analysis of a high-priority phishing attempt targeting end-users through a spoofed Microsoft security alert. Triage confirmed this was a malicious attempt to steal credentials, leveraging social engineering tactics (**urgency** and **false branding**). Technical analysis revealed critical Indicators of Compromise (IOCs), including failed email authentication checks (SPF/DKIM) and the origination IP address belonging to a high-risk, historically abusive web hosting provider. Immediate mitigation steps are recommended to prevent potential breaches.

---

1 Executive Summary

The identified incident is a **High-Confidence Phishing Attack** detected in the inbound mail stream. The primary threat vector is email spoofing aimed at harvesting user credentials via a malicious link disguised as a security action button ("Report the user").

- **Classification:** Phishing/Credential Harvesting.
- **Severity:** **CRITICAL**. Direct risk of account compromise.
- **Key Findings:** Failed SPF/DKIM authentication confirms spoofing. The originating **IP** (hosted by GHOSTNET GmbH) has a significant history of abuse reports, confirming its use as malicious infrastructure.
- **Status:** Analysis Complete. Transitioning to Mitigation and Containment Phase.

2 Incident Details and Scope

The objective of this analysis was to methodically triage the suspicious email, reverse-engineer its origination using technical headers, and produce actionable Indicators of Compromise (IOCs) for immediate mitigation.

- ▷ **Initial Trigger:** End-user reporting a suspicious "Unusual Sign-in Activity" notification.
- ▷ **Skills Demonstrated:** Email Header Analysis, Email Authentication Validation, Threat Intelligence integration, and Formal Incident Documentation.

3 Technical Analysis and Findings

3.1 Social Engineering and Content Review

The email content was professionally crafted to maximize user anxiety and compliance.

- **False Branding:** The email uses Microsoft branding, including logo and formatting, to create a false sense of trust.
- **Urgency/Fear Tactic:** The subject line and body communicate an 'unusual sign-in activity' which compels the end-user to act without critical thought.
- **Call to Action (CTA):** The user is instructed to click a button to "report the user," which, upon inspection, is a malicious URL designed for credential harvesting.

3.2 Raw Email Source and Sender Consistency

Inspection of the raw email source immediately revealed inconsistencies indicating a spoofing attempt.

- **Display Name Spoofing:** The sender address is displayed as a legitimate-looking Microsoft account team address: `no-reply@access-accsecurity.com`.
- **Return Path Mismatch:** The technical return path is `bounce@thcultarfdes.co.uk`, which completely contradicts the sender's display domain, confirming a high likelihood of spoofing.

3.3 Email Authentication Verification

An email header analyzer (MXToolbox) was used to systematically check standard authentication records (SPF, DKIM).

- **SPF Status: NONE**. The absence of an SPF record for the sending domain is highly alarming, as legitimate corporate domains almost always configure this record.
- **DKIM Status: FAIL**. This result conclusively proves the sender was unauthorized to use the domain and that the message content was either forged or improperly signed.
- **Conclusion:** Failed authentication checks confirm the email originated from an unauthorized external source masquerading as a trusted entity.

3.4 Origin IP Intelligence (AbuseIPDB)

The true sending IP address was extracted from the `Received` headers and analyzed using threat intelligence services.

- **IP Address:** [Extracted Sending IP Address - placeholder]
- **Hosting Misalignment:** The IP is hosted by a generic Data Center/Web Hosting provider (`GHOSTNET GmbH`). Legitimate corporate emails do not typically originate from this type of shared infrastructure, strongly suggesting malicious staging.
- **Historical Abuse:** The IP record shows it has been reported **30**× by 10 different sources for abusive or questionable activities, which elevates its inherent risk profile.
- **Threat Intelligence Note:** The coincident association with the ISP name `GHOSTNET` (even if unrelated to the historical APT) immediately triggers high vigilance and scrutiny from security analysts.

4 Indicators of Compromise (IOCs)

The following high-confidence IOCs have been generated for immediate implementation into security controls (Firewalls, Proxies, Mail Filters).

IOC Type	Indicator	Action Priority
Sending IP	[Extracted Sending IP Address - placeholder]	Block/Quarantine
Return-Path Domain	`thcultarfdes.co.uk`	Block/Filter
Sender Display Domain	`access-accsecurity.com`	Block/Flag
Malicious URL Target	[Malicious URL from Button - placeholder]	Block/Sinkhole

5 Mitigation and Containment

The following steps are recommended for immediate containment and long-term security posture improvement:

Immediate Containment

C1. Apply all listed IOCs (Sending IP, domains, and extracted URL) to network firewalls, web proxies, and email filtering solutions.

C2. Perform a global log sweep for the malicious IP and domain to identify if any other users received the email or, critically, if they clicked the link.

C3. Issue an immediate internal security alert to all users, providing screenshots of the malicious email and re-iterating phishing awareness procedures.

Long-Term Remediation

R1. Review existing email security gateway policies to enforce stricter DMARC policies (e.g., quarantine or reject based on failed DKIM/SPF).

R2. Conduct a focused security awareness training module on ”Urgency and Branding Spoofing” based on the analysis of this specific incident.