Portfolio Project 2 – Phishing Email Triage Walk-through – Login Theft Attempt

Introduction

This project simulates the triage and investigation of a phishing email reported by a user.
It follows a typical SOC workflow including email header analysis, link investigation, user activity review, and final decision-making.

This project demonstrates practical SOC skills for identifying phishing attempts, assessing user risk, and documenting findings clearly.

Alert:

Alert Name: Reported Suspicious Email – Possible Phishing
Source: User-reported (via Outlook Report Phishing button)
Severity: High
Timestamp: July 6, 2025 – 09:11 AM

Description:
User s.parker@acmeinc.com reported an unexpected email with the subject:

"[ACTION REQUIRED] Password Expiration Notice – Click to Keep Access"

The email contained a link to a login page impersonating Microsoft.
The email passed SPF but failed DKIM validation.
Initial review suggests a credential harvesting attempt.

Triage Process:

1. Acknowledge and Assign Alert

- User s.parker@acmeinc.com submitted the email via phishing report button
- SOC analyst assigned and begins investigation

2. Review Email Metadata and Headers

- Subject: [ACTION REQUIRED] Password Expiration Notice – Click to Keep Access
- Sender: security-alerts@micr0soft-support.com
- Return-Path domain doesn't match display name
- SPF: Pass

- DKIM: **Fail**
- DMARC: **Fail**
- Reply-To differs from sender address = suspicious

3. Analyze Link or Attachment

- Hovered link: http://microsoft-signin-auth.helpdesksecurity.ru/login
- URL submitted to VirusTotal and URLscan.io
- Results:
    - Phishing flagged by 6 engines (VirusTotal)
    - Hosted on free subdomain host
    - Impersonates Microsoft login

4. Investigate User Behaviour

- Check EDR and browser logs
- User clicked the link – redirected to phishing site
- No form submission or credential entry detected
- No unusual behaviour post-click

5. Scan for Lateral Spread or Other Targets

- Check email logs for recipients
- 3 other users received similar emails
- 2 additional users clicked the link, no further impact

6. Contain and Prevent

- Block domain in web proxy and firewall
- Add domain to phishing blocklist
- Notify affected users to reset passwords
- Review endpoints for IOCs — clean

Findings Summary

- Email was a phishing attempt impersonating Microsoft
- Sender domain and reply-to address mismatched legitimate sources
- SPF passed, but DKIM and DMARC failed
- Link directed to a credential harvesting site flagged by multiple engines
- User clicked link but did not enter credentials
- 2 additional users clicked similar emails, no compromise detected
- No malware or lateral movement observed post-click

Analyst Decision

This was a **confirmed phishing campaign** targeting user credentials. Impact was limited due to fast user reporting and SOC response. No indicators of compromise found in affected user sessions.

Action Taken

- Reported email and domain blocked at firewall and proxy level
- IOC shared with email filtering provider for rule updates
- Affected users prompted to reset passwords as a precaution
- Awareness reminder sent to all staff about phishing indicators

Final Summary

This project simulates a Tier 1 SOC phishing email triage scenario, based on a real-world login theft attempt.
It demonstrates my ability to:

- Analyse email headers (SPF, DKIM, DMARC, sender validation)
- Investigate malicious links using tools like VirusTotal and URLscan.io
- Review user behaviour and endpoint activity
- Take action to contain phishing threats and notify affected users
- Document findings clearly and follow SOC escalation protocols

Tools and platforms referenced in this simulation are modelled after those used in real-world SOC environments.