Incident Report – Phishing Case

1. Case Information

Case ID: 1

Status: Open / In Progress / Closed

Priority: Low / Medium / High / Critical

Category: Email Security / Phishing

Subcategory: Suspicious Email Reported

Assigned To: Michelle Flores

Date/Time Created: 7:00AM

Date/Time Closed:

2. Reporter Details

Reported By: Michelle Flores

Method of Report: Email / Phone / Phishing Button / Other

Contact Info: michelle@example.com

3. Incident Details

Summary: Phishing Attempt

Description of Event: On August 8, 2025, I received a suspicious phishing email claiming to be Microsoft Support. The email contained a spoofed sender domain, an urgent request to verify the account, and a malicious link to a non-Microsoft domain. The email appears to be a part of a credential-harvesting phishing attempt and it is misspelled.

Time of Occurrence: 02:12PM

Attachments:

4. Analysis

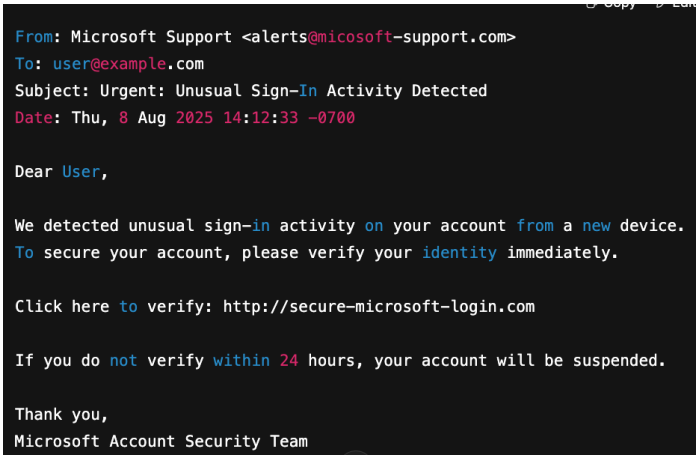
Sender Email: alerts@micosoft-support.com

Display Name: Microsoft Support

Subject Line: Urgent: Unusual Sign-In Activity Detected

Link(s) in Email: http://secure-microsoft-login.com

Attachment(s): eml file:



```
From: Microsoft Support <alerts@micosoft-support.com>
To: user@example.com
Subject: Urgent: Unusual Sign-In Activity Detected
Date: Thu, 8 Aug 2025 14:12:33 -0700

Dear User,

We detected unusual sign-in activity on your account from a new device.
To secure your account, please verify your identity immediately.

Click here to verify: http://secure-microsoft-login.com

If you do not verify within 24 hours, your account will be suspended.

Thank you,
Microsoft Account Security Team
```

Indicators of Compromise (IOCs): Linguistic anomalies, urgency, generic greeting(Dear Customer), Sender domain, suspicious links

Threat Analysis: This email is a credential-harvesting phishing attempt. The attacker is impersonating Microsoft to trick me into clicking a malicious link and entering login credentials on a fake login page. The misspelled sender domain, generic greeting, urgency, and non-Microsoft URL are consistent with common phishing tactics used to bypass security filters and exploit human behavior.

5. Impact

Targeted User(s): Self(simulation) and organization

Potential Impact: If successful, the attacker could have harvested Microsoft account credentials, potentially leading to unauthorized access to corporate systems, data theft, or further phishing attacks within the organization.

Scope: Single targeted user

6. Containment Actions

Email quarantined: Yes

Malicious link blocked in proxy/firewall: Yes

Sender domain blocked: Yes

Account reset: Yes

7. Eradication & Recovery

Steps taken to remove malicious content from the environment: The reported phishing email was quarantined in the email security gateway to prevent further delivery. The malicious link was added to the proxy/firewall blocklist, and the sender domain was

blocked at the email filter level to prevent future attempts. The targeted account password was reset as a precaution.

Verification that affected accounts are secure: Confirmed the targeted account password change was successful and that multi-factor authentication remained active. No signs of unauthorized login attempts were detected in account logs.

Post-incident scanning results: A post-incident scan of the affected systems revealed no signs of malware or persistence mechanisms. No further indicators of compromise were detected.

8. Lessons Learned

Root Cause: The attacker likely obtained the email address from a previous data breach or public source, then sent a generic phishing campaign targeting multiple organizations.

Gaps Identified: Existing email security controls did not block the phishing message before delivery, indicating a possible gap in filtering rules or threat intelligence updates. Additionally, the absence of an advanced email security tool capable of restricting access to suspicious emails allowed the user to view and interact with the message.

Recommended Improvements: Implement enhanced email security controls with advanced phishing detection capabilities to more effectively block malicious messages before delivery. Require an organization-wide password reset following the incident to mitigate potential credential exposure. Establish a policy discouraging the use of corporate email addresses for non-business purposes to reduce the risk of addresses being exposed in external data breaches.