“From: Microsoft Security <no-reply@micros0ft-support.com>
To: employee@company.com
Subject: Urgent: Unusual Sign-In Activity Detected

Dear User,

We detected an unusual sign-in attempt on your Microsoft account from an unknown device.

If this was not you, please verify your identity immediately to prevent account suspension.

Verify Now: https://login-microsoft-security[.]com/verify

Failure to verify within 24 hours may result in limited account access.

Regards,
Microsoft Security Team”

Incident Summary
A phishing email impersonating Microsoft Security was identified and analyzed.

Detection Method
User reported suspicious email.

Indicators of Compromise (IOCs)
- **Sender email: no-reply@micros0ft-support.com (0 instead of O)**
- **Malicious URL: login-microsoft-security[.]com/verify (unusual “[.]”)**
- **IP Address: N/A (email-based attack)**

Attack Stage
Initial Access (Phishing)

MITRE ATT&CK Mapping
- **T1566.001 – Phishing: Spearphishing Link**

Impact Assessment
Potential credential compromise if link was accessed.

Containment & Remediation
- **Blocked sender domain**
- **Blocked malicious URL**
- **User advised to reset password**
- **Security awareness reminder issued**

Lessons Learned
Phishing emails continue to rely on urgency and brand impersonation.