**PHISHING EMAIL ATTACK INVESTIGATION REPORT**

**1. Executive Summary**

On June 24th, 2025 at 08:14 AM IST, a user-reported phishing email was triaged and found to impersonate Microsoft Security. The email included a spoofed sender, visually deceptive domain, and a credential harvesting link. The attack bypassed SPF and DKIM validation, evaded the primary mail gateway, and leveraged social engineering via urgency-based cues.

No credentials were compromised. One user clicked the link but closed it without entering data. IOC analysis revealed a domain registered <5 days prior, hosted on a VPS infrastructure commonly used for cybercrime. The incident has been contained, and response was completed within 65 minutes.

**✉️ 2. Full Phishing Email (Redacted)**

From: Microsoft Account Team <support@micr0soft-secure.com>

To: employee1@company.com

Subject: [Alert] Sign-in attempt blocked – Immediate action required

Date: Mon, 24 Jun 2025 08:12:47 +0530

Message-ID: <msgid.987654321@micr0soft-secure.com>

Content-Type: text/html; charset=UTF-8

**Email Body (HTML Rendered):**

**Microsoft Security Alert**

We’ve detected an attempt to sign in to your Microsoft account from an unrecognized location:

* **IP Address:** 192.241.220.92
* **Time:** 24 June 2025, 02:03 UTC
* **Location:** Amsterdam, Netherlands

If this wasn’t you, please verify your identity to avoid account suspension.

👉 Click here to verify your account

Failure to act within 24 hours may result in deactivation.

Thank you,  
**Microsoft Account Protection Team**

**🔬 3. Email Header & SMTP Trace Analysis**

| **Header Field** | **Description** |
| --- | --- |
| From: | Spoofed display name with visually similar domain micr0soft-secure.com |
| Return-Path: | support@micr0soft-secure.com (no SPF match) |
| Received: | via VPS mail relay at 45.76.112.50 |
| Message-ID: | Fake ID format not matching corporate pattern |
| SPF: | FAIL – sender not authorized for micr0soft-secure.com |
| DKIM: | Missing |
| DMARC: | None configured for spoofed domain |
| X-Mailer: | PHPMailer v6.7 – common in phishing kits |

📌 **SMTP Chain Observations:**

* IP reverse resolves to vultr.com, not Microsoft
* Message-ID mismatch suggests manual crafting or phishing toolkit
* SPF fail but gateway did not block (misconfiguration)

**🌐 4. Threat Infrastructure Breakdown**

**Domain Intelligence: micr0soft-security-login.com**

| **Property** | **Value** |
| --- | --- |
| Registration Date | 21 June 2025 |
| Registrar | Namecheap, Inc. |
| WHOIS Privacy | Enabled |
| DNS Records | A: 45.76.112.50, no MX, no SPF |
| SSL Cert | Self-signed, expired |
| Hosting | Vultr VPS Netherlands |
| URL Behavior | Loads fake Microsoft login page with POST to /process.php |

**IP Address: 45.76.112.50**

* ASN: 20473 (Choopa/Vultr)
* Abuse Reports: High (Spamhaus + PhishTank match)
* Open Ports: 80, 443, 22 (no rate limiting)
* TLS Fingerprinting: TLS 1.0 fallback offered (outdated)

📍 **Screenshot (Description):**  
Login page mimics Microsoft's branding, uses CSS from Microsoft's CDN (stolen), form submits credentials silently using POST to /logdata.php.

**🧠 5. MITRE ATT&CK Mapping**

| **Tactic** | **Technique ID** | **Description** |
| --- | --- | --- |
| **Initial Access** | T1566.002 | Phishing via link |
| **Credential Access** | T1110.001 | Web credential harvesting |
| **Command & Control** | T1071.001 | Exfiltration via HTTP POST |

**🧪 6. Indicators of Compromise (IOC Table)**

| **Type** | **Value** | **Risk** | **Action Taken** |
| --- | --- | --- | --- |
| URL | http://micr0soft-security-login.com/verify | High | Blocked on DNS & proxy |
| IP Address | 45.76.112.50 | High | Added to FW denylist |
| Domain | micr0soft-security-login.com | High | Sinkholed internally |
| Email Sender | support@micr0soft-secure.com | Medium | Banned via content rule |

IOC entries submitted to: AbuseIPDB, VirusTotal, OpenPhish.

**📊 7. SIEM Correlation & Endpoint Review**

* **Tool:** Splunk + EDR (SentinelOne)
* **Query:**

ini

CopyEdit

index=email\_logs sender="support@micr0soft-secure.com" OR uri="micr0soft-security-login.com"

* **Hits:** 3 users received the email
* **EDR Alerts:** None
* **One user clicked the link** – browser telemetry shows **no data entered**, tab closed in <10 seconds

**📆 8. Incident Response Timeline**

| **Time** | **Action** | **Tool** |
| --- | --- | --- |
| 08:12 | Email received | O365 Gateway |
| 08:18 | Reported by user | PhishAlert Button |
| 08:25 | Header analysis complete | Splunk |
| 08:32 | URL sandboxed | Any.Run |
| 08:40 | SIEM IOC search complete | Splunk |
| 08:45 | Email quarantined | Exchange Admin Center |
| 08:50 | IOC added to DNS/EDR/FW | CrowdStrike, Cisco Umbrella |
| 09:00 | Awareness email sent | Internal comms |

**🔧 9. Root Cause & Gaps**

| **Gap** | **Recommendation** |
| --- | --- |
| SPF failed but allowed | Enforce hard fail policy (-all) |
| No DMARC reporting | Deploy DMARC with policy p=quarantine |
| User clicked phishing link | Phishing training refresh + simulation |
| No URL rewriting | Enable link detonation in gateway |

**📘 10. Recommendations**

**🧰 Technical:**

* Enforce SPF, DKIM, and DMARC with reject/quarantine policies
* Block newly registered domains <30 days old
* Enable URL link rewriting and detonation (Microsoft Defender / Proofpoint)
* Implement inline sandboxing

**👥 Awareness:**

* Conduct monthly phishing simulation
* Update training with real examples
* Test user reactions and measure click rate

**🏛️ Policy:**

* Update IR Playbook with phishing SOP
* Require passwordless/MFA authentication on email accounts
* Review 3rd party DMARC monitoring services (Valimail, dmarcian)

**✅ 11. Conclusion**

The phishing email was sophisticated in appearance but lacked technical sophistication (missing DKIM, invalid SPF). The spoofed domain used visually deceptive characters and a fake login page hosted offshore. Quick action by the SOC and user vigilance prevented any breach. Continued investment in email security layers, awareness, and automated IOC detection is essential.