SOC Analyst Investigative Report

Incident: Phishing Email Targeting MediSure Health Network
Analyst: Abubakar Yusuf
Date: November 2025

1. Executive Summary

On November 14, 2025, MediSure Health Network was targeted by a phishing campaign impersonating Microsoft and a medical supplier. The phishing emails contained spoofed sender domains, malicious URLs, and attempted credential harvesting. Two employees interacted with the phishing links, resulting in limited outbound connections to attacker-controlled infrastructure.

The incident posed risks to patient data, operational continuity, and financial integrity. Immediate containment and eradication actions were taken, followed by employee awareness training to strengthen the organization's resilience against future phishing attempts.

2. Business Context

MediSure Health Network is a leading healthcare provider with extensive digital infrastructure. While its systems are well-secured, phishing exploits human vulnerabilities. This incident highlighted the need for stronger defences against Business Email Compromise (BEC) and credential theft, both of which could disrupt patient care and violate HIPAA compliance.

3. Key Objectives

- **Identify Phishing Indicators:** Examine the email headers, sender information, and embedded links for signs of spoofing, domain manipulation, or suspicious payloads.
- **Validate Sender Authenticity:** Perform SPF, DKIM and DMARC checks using DNS analysis tools to confirm or reject the legitimacy of the email's origin.
- **Analyse Links and Attachments:** Use malware analysis platforms to detect hidden payloads, trojans, or credential harvesting schemes.
- **Correlate Network Logs:** Cross-check inbound and outbound network traffic using SIEM tools to identify any connections to known malicious IP addresses or domains.

- **Respond and Mitigate:** Contain the threat by blocking domains, resetting credentials, isolating affected endpoints, and updating email security filters.
- **Educate Employees:** Develop awareness material based on findings, training staff to recognize similar attacks in the future.

4. Technology Stack

The project relies on proven, cost-effective, and widely available tools that support SOC investigations:

- **MX Toolbox:** DNS and email authentication checks (SPF, DKIM, DMARC).
- **mha.azurewebsites.net:** It is a tool for parsing and analysing email message headers.
- **Virus Total:** Link and attachment malware scanning using multiple AV engines.
- **Hybrid-Analysis:** It is an online sandbox that lets you safely open and analyse suspicious files or URLs to see what they really do.
- **Splunk Cloud (Free Version):** SIEM for ingesting logs from mail servers, firewalls, and endpoint detection systems to identify anomalies.
- **AbuseIPDB:** It is a threat-intelligence platform that collects reports of malicious IPs, stores them in a public database, scores them, and makes this information easy to check through an API or website.

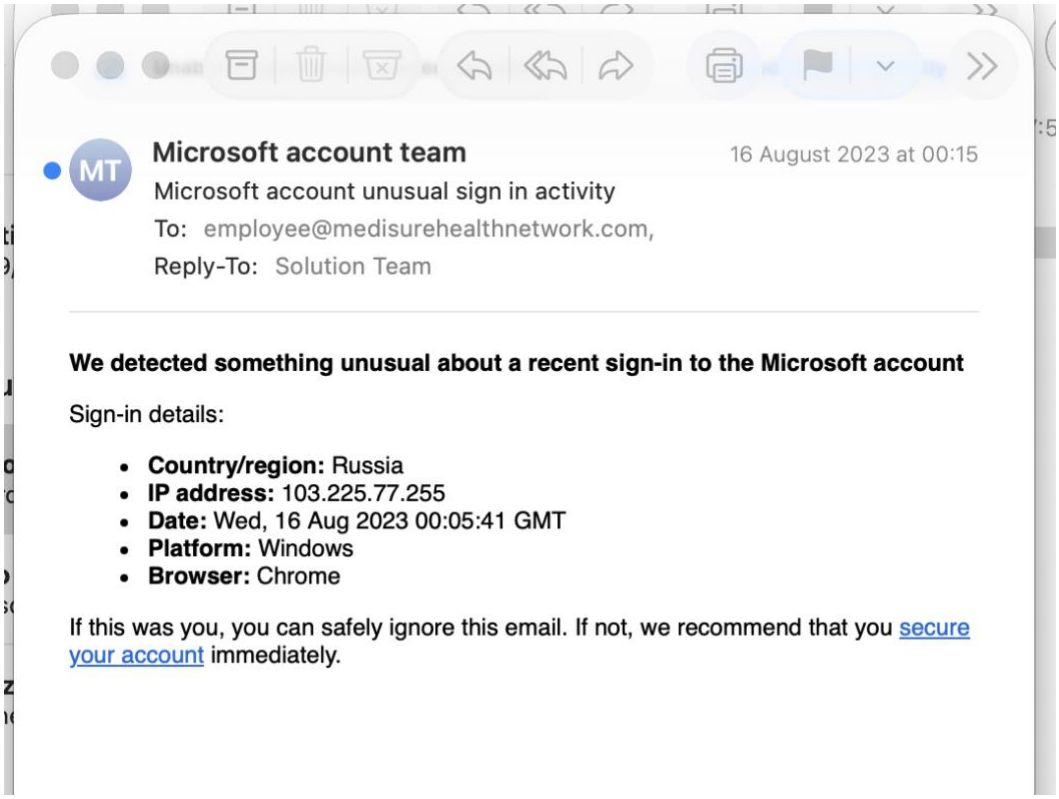
5. Incident Timeline

- **14 Nov 2025:** Suspicious phishing email received by staff.
- **16 Nov 2025:** Email header and authentication checks performed. Malicious domains and IPs identified.
- **16 Nov 2025:** SIEM (Splunk) log analysis confirmed user interaction with phishing URL and outbound traffic to attacker IPs.
- **16 Nov 2025:** Containment actions executed (blocking domains/IPs, password resets, endpoint isolation).
- **Post-Incident:** Awareness training rolled out across staff groups.

6. Technical Findings

6.1 Email Header & Email Content Analysis

- **Sender:** no-reply@access-accsecurity.com (spoofed domain, not Microsoft).
- **Reply-To:** solutionteamrecognizd03@gmail.com (inconsistent with Microsoft).
- **Indicators:** Urgent language, suspicious link (https://sign.in/), malicious IP (103.225.77.255).
- **Conclusion:** Clear spoofing and phishing attempt.

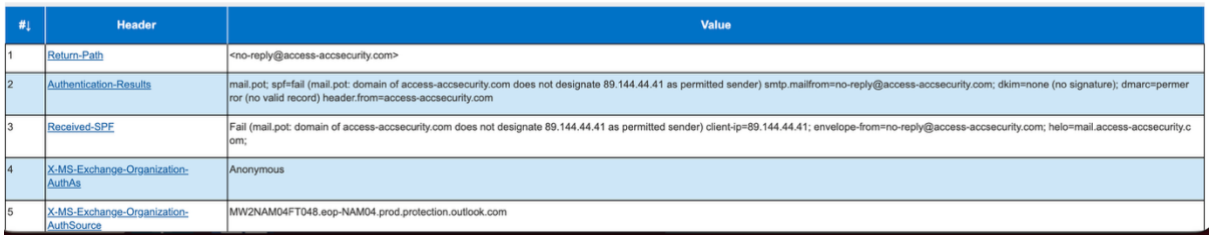


Screenshot of the initial Email review.

6.2 Authentication Checks (SPF, DKIM, DMARC)

- **SPF/DKIM/DMARC:** All failed.
- **Domain:** access-accsecurity.com lacked proper DNS authentication records.
- **IP:** 89.144.44.41 was not authorized by access-accsecurity.com and it is flagged as malicious and blacklisted.
- **Relay information:** Received delay (3840 seconds)
- **Conclusion:** Message forged, not legitimate.

Screenshot of SPF, DKIM & DMARC analysis using MX Toolbox.

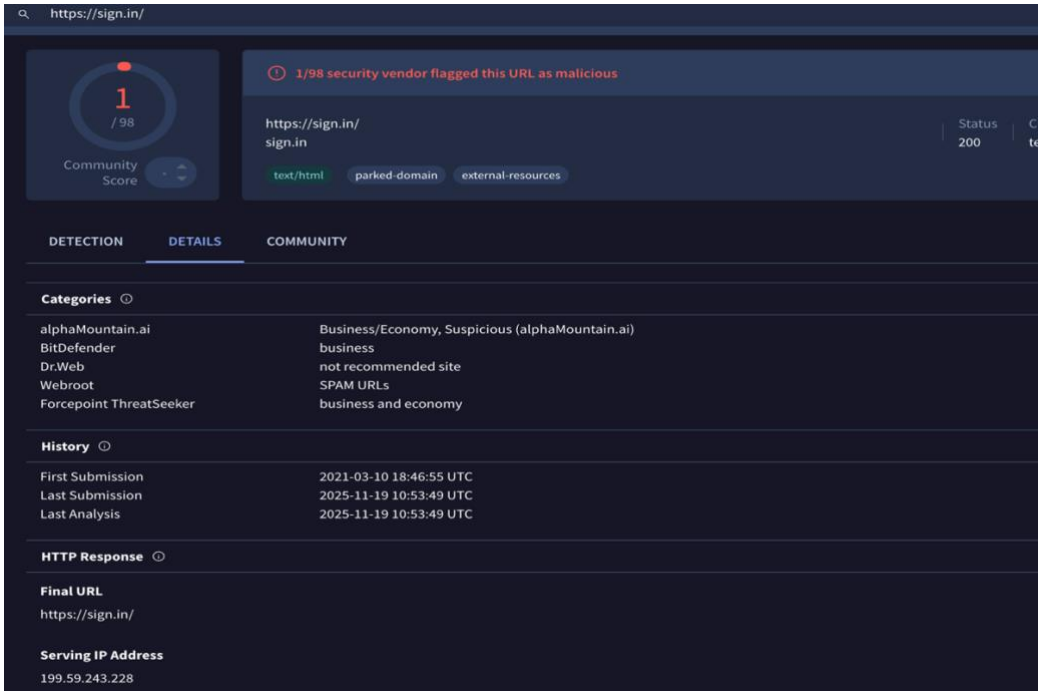


#↓	Header	Value
1	Return-Path	<no-reply@access-accsecurity.com>
2	Authentication-Results	mail.pot; spf=fail (mail.pot: domain of access-accsecurity.com does not designate 89.144.44.41 as permitted sender) smtp.mailfrom=no-reply@access-accsecurity.com; dkim=none (no signature); dmarc=permerror (no valid record) header.from=access-accsecurity.com
3	Received-SPF	Fail (mail.pot: domain of access-accsecurity.com does not designate 89.144.44.41 as permitted sender) client-ip=89.144.44.41; envelope-from=no-reply@access-accsecurity.com; helo=mail.access-accsecurity.com;
4	X-MS-Exchange-Organization-AuthAs	Anonymous
5	X-MS-Exchange-Organization-AuthSource	MW2NAM04FT048.eop-NAM04.prod.protection.outlook.com

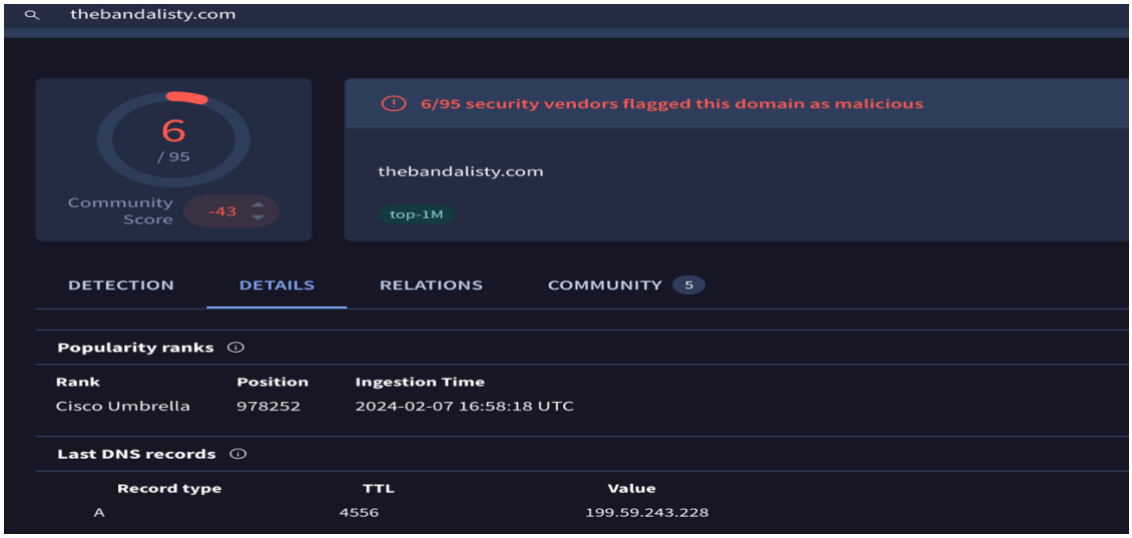
Screenshot of email header analysis using mha.azurewebsites.net.

6.3 URL & Domain Analysis

- **URL:** https://sign.in/ flagged as suspicious/malicious (data exfiltration behaviour).
- **Domain:** thebandalisty.com linked to same IP (199.59.243.228), flagged by multiple vendors.
- **Recommendation:** Block both domains and IPs.



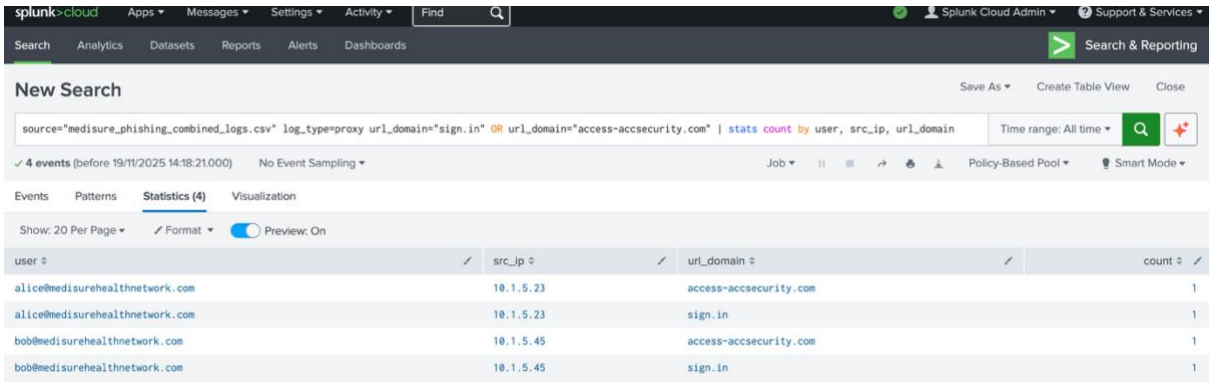
Screenshot of the virus total report of the phishing link (https://sign.in/)



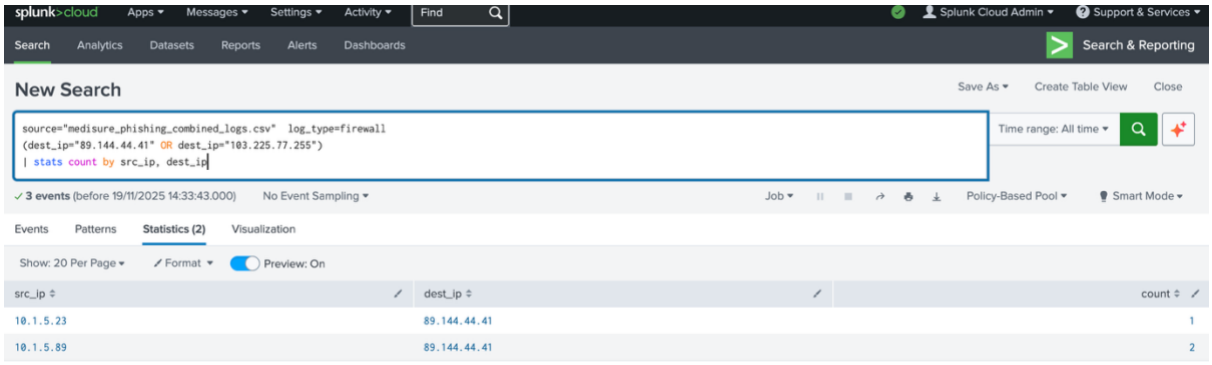
Screenshot of the virus total report on the malicious domain (thebandalisty.com)

6.4 SIEM Log Analysis (Splunk)

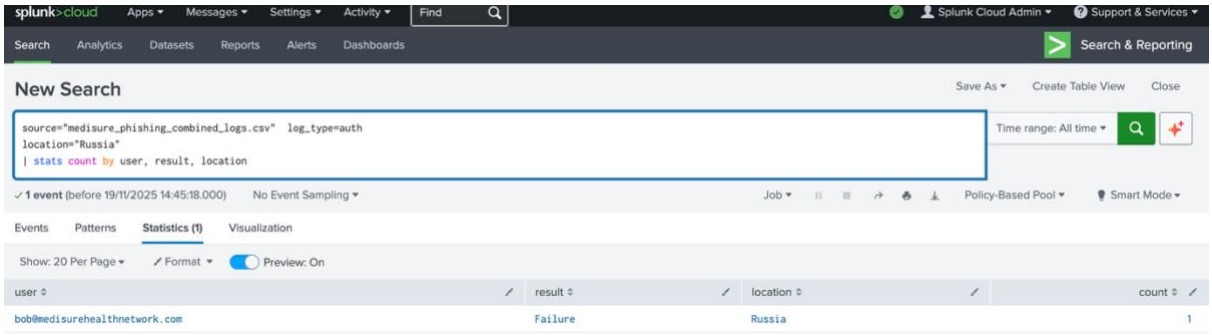
- **Employees Impacted:** Alice (10.1.5.23) and Bob (10.1.5.45).
- **Events:**
    1. The proxy log indicates the employees that clicked phishing link (sign.in, access-accsecurity.com).
    2. The Firewall log indicate the outbound connections to attacker IP (89.144.44.41).
    3. The Authentication log showed the failed login attempt from Russia targeting Bob's account.
- **Total Events:** 5 phishing-related events across proxy, firewall, and authentication logs.



Screenshot of the proxy log indicating that some employees (Alice & Bob) clicked on the phishing link and accessed the malicious domain.



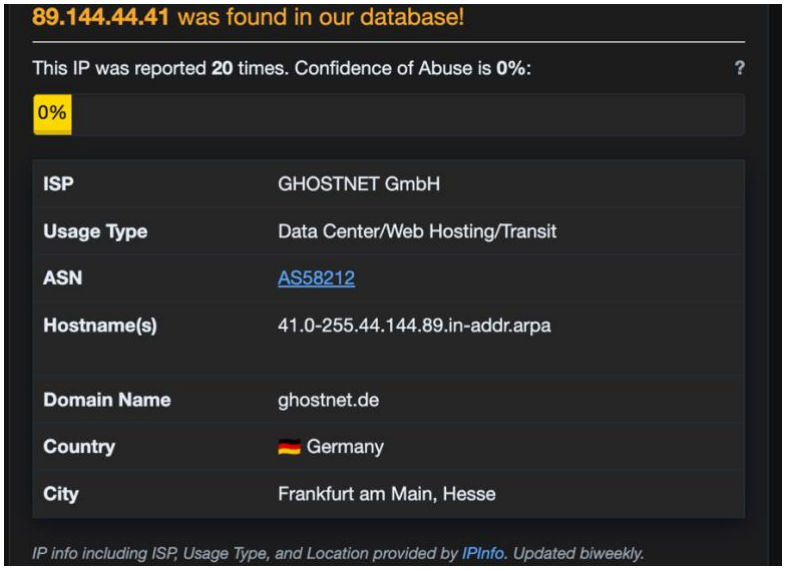
Screenshot of the firewall log indicating outbound connection to attacker infrastructure (89.144.44.41).



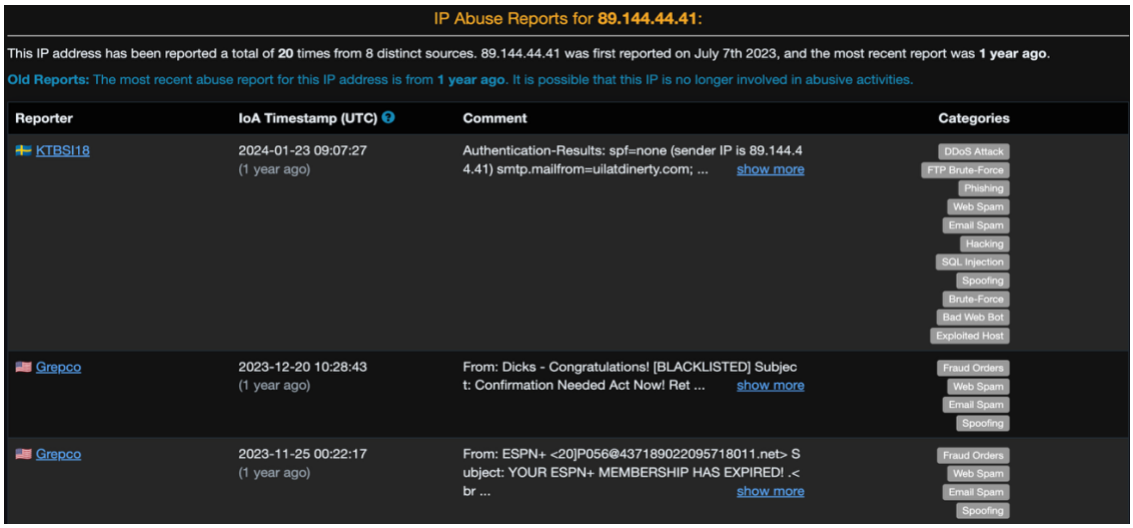
Screenshot of the Authentication log indicating credential attempt on Bob account.

6.5 Indicators of Compromise (IOCs)

Type	IOC	Source	Findings
Malicious IP	89.144.44.41	AbuseIPDB	Blacklisted, spoofing/hacking
Malicious IP	103.225.77.255	AbuseIPDB	Phishing, brute-force, exploited host
Malicious Domain	access-accsecurity.com	Virus Total	Associated with phishing emails
Malicious Domain	thebandalisty.com	Virus Total	Low reputation, flagged malicious
Malicious URL	https://sign.in/	Virus Total / Hybrid Analysis	Data exfiltration behaviour

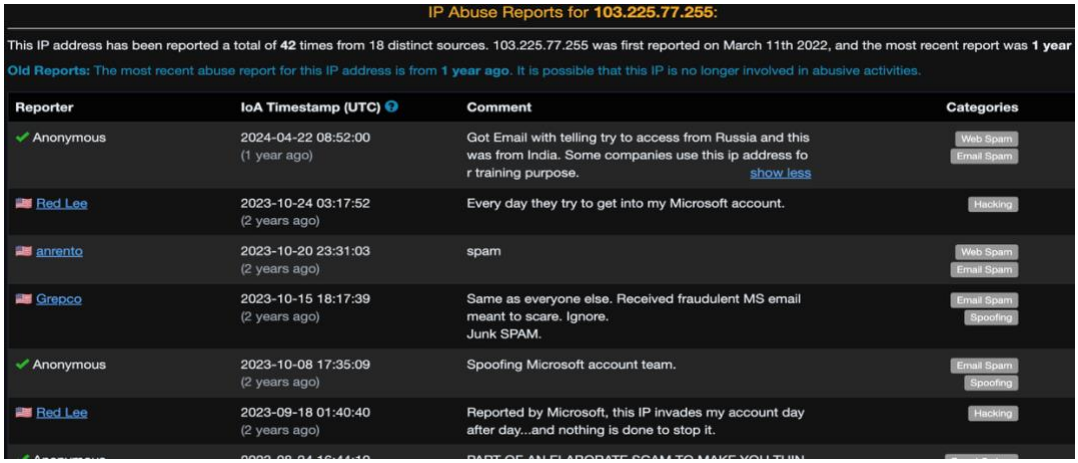


Screenshot showing information about 89.144.44.41



Screenshot showing reports and comments about 89.144.44.41

Screenshot showing information about 103.225.77.255



Screenshot showing reports and comments about 103.225.77.255

7. Incident Response Actions

Containment

- Blocked malicious domains & URL (sign.in, thebandalisty.com, access-accsecurity.com).
- Blocked malicious IPs (89.144.44.41, 103.225.77.255).
- Isolated affected endpoints (10.1.5.23, 10.1.5.89).
- Disabled accounts for Alice & Bob; enforced password resets.

Eradication

- Full malware scans on affected endpoints.
- Cleared browser cache and sessions.
- Removed phishing emails from mailboxes.

Recovery

- Reconnect cleaned devices.
- Enforced MFA and geolocation login restrictions.
- Monitored for 72 hours for further activity.

Post-Incident

- Updated SIEM detection rules with new IOCs.
- Documented incident timeline.
- Enhanced phishing awareness training for Medisure employees.

8. Awareness & Training

Employees were trained to recognize phishing attempts using five key signs:

1. Suspicious sender addresses.
2. Urgent or threatening language.
3. Unexpected attachments or links.
4. Requests for credentials or patient data.
5. Poor grammar and odd formatting.

This initiative turned staff into the first line of defence, reducing future risk.

9. Outcome

- Phishing attempt contained with no successful compromise of accounts or patient data.
- Immediate risks reduced through blocking, isolation, and password resets.
- Long-term resilience improved via updated detection rules and staff training.
- HIPAA compliance maintained, patient trust preserved, and financial fraud prevented.

10. Recommendations

- Continue phishing simulations and awareness campaigns.
- Strengthen email gateway filtering with advanced threat intelligence feeds.
- Enforce strict SPF, DKIM, and DMARC policies across all domains.
- Maintain SIEM correlation rules for geolocation anomalies and IOC detection.
- Regularly review firewall/proxy logs for suspicious outbound traffic.

Final Note: This incident demonstrated that while technical defences are strong, human awareness remains critical. By combining technical controls with employee vigilance, MediSure Health Network can better protect patient data, ensure operational continuity, and safeguard its reputation.