

## 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.

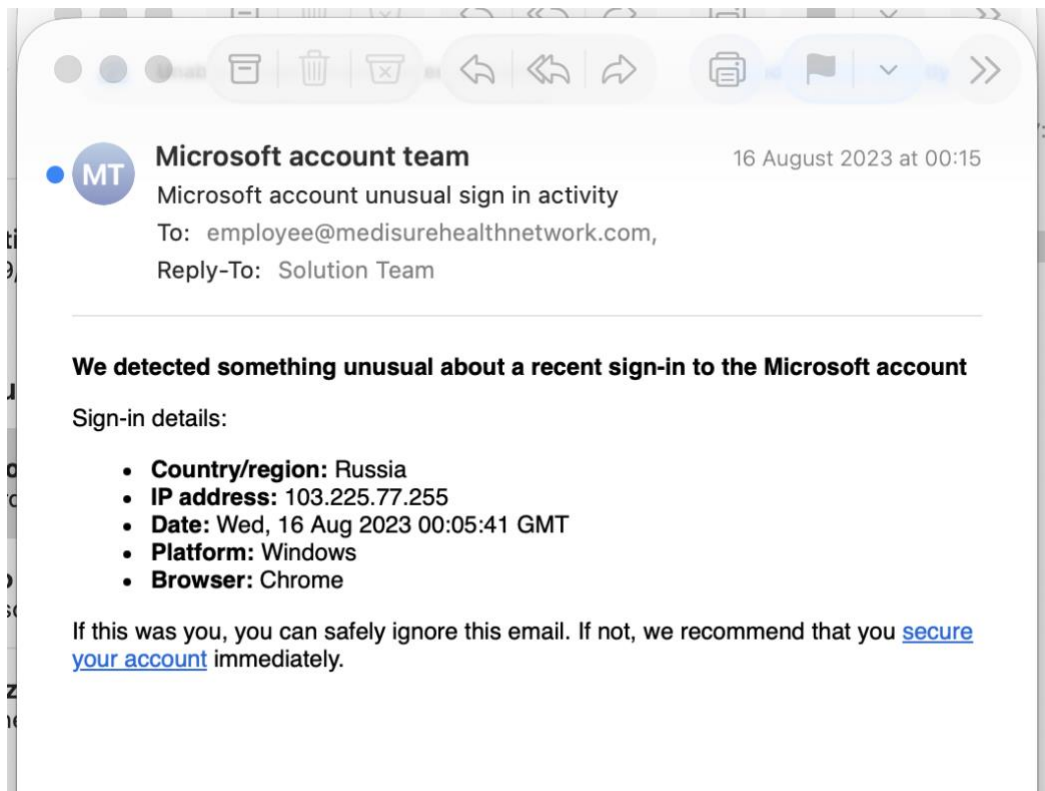
#### 5. Incident Timeline

- **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.

#### Delivery Information

DMARC Compliant (No DMARC Record Found)
SPF Alignment
SPF Authenticated
DKIM Alignment
DKIM Authenticated

#### Relay Information

Received	3840 seconds
Delay:	

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=permer ror (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.c om;
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.

https://sign.in/

1 / 98  
Community Score

1/98 security vendor flagged this URL as malicious

https://sign.in/  
sign.in

Status 200

text/html parked-domain external-resources

DETECTION DETAILS COMMUNITY

Categories

alphaMountain.ai	Business/Economy, Suspicious (alphaMountain.ai)
BitDefender	business
Dr.Web	not recommended site
Webroot	SPAM URLs
Forcepoint ThreatSeeker	business and economy

History

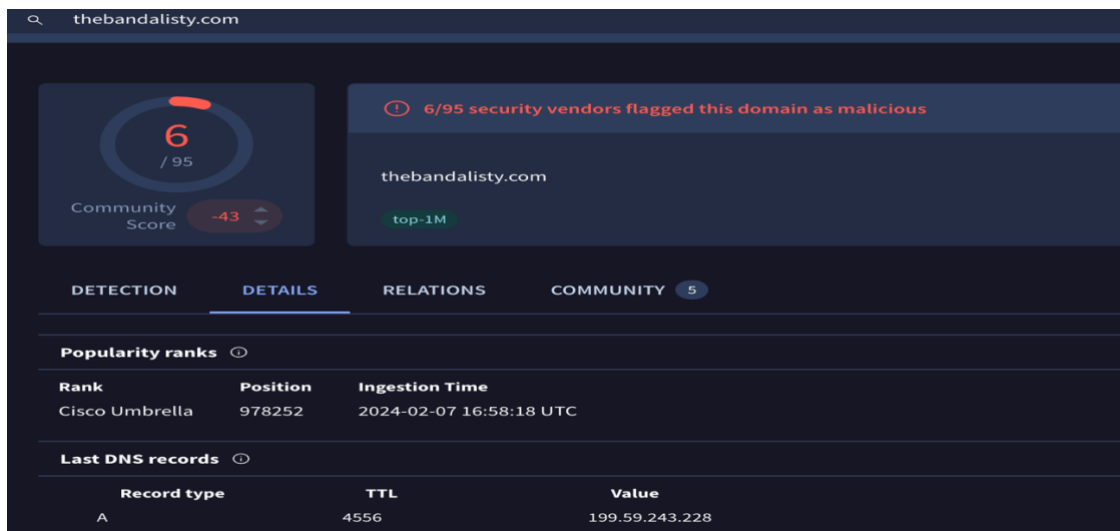
First Submission	2021-03-10 18:46:55 UTC
Last Submission	2025-11-19 10:53:49 UTC
Last Analysis	2025-11-19 10:53:49 UTC

HTTP Response

Final URL  
https://sign.in/

Serving IP Address  
199.59.243.228

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.

splunk cloud Apps Messages Settings Activity Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search Save As Create Table View Close

source=medisure\_phishing\_combined\_logs.csv log\_type=proxy url\_domain=sign.in OR url\_domain=access-accsecurity.com | stats count by user, src\_ip, url\_domain Time range: All time

✓ 4 events (before 19/11/2025 14:18:21.000) No Event Sampling Job Policy-Based Pool Smart Mode

Events Patterns Statistics (4) Visualization

Show: 20 Per Page Format Preview: On

user	src_ip	url_domain	count
alice@medisurehealthnetwork.com	10.1.5.23	access-accsecurity.com	1
alice@medisurehealthnetwork.com	10.1.5.23	sign.in	1
bob@medisurehealthnetwork.com	10.1.5.45	access-accsecurity.com	1
bob@medisurehealthnetwork.com	10.1.5.45	sign.in	1

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

New Search

source="medisure\_phishing\_combined\_logs.csv" log\_type=firewall  
(dest\_ip="89.144.44.41" OR dest\_ip="103.225.77.255")  
| stats count by src\_ip, dest\_ip

Time range: All time

3 events (before 19/11/2025 14:33:43.000) No Event Sampling

Events Patterns Statistics (2) Visualization

Show: 20 Per Page Format Preview: On

src_ip	dest_ip	count
10.1.5.23	89.144.44.41	1
10.1.5.89	89.144.44.41	2

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

New Search

source="medisure\_phishing\_combined\_logs.csv" log\_type=auth  
location="Russia"  
| stats count by user, result, location

Time range: All time

1 event (before 19/11/2025 14:45:18.000) No Event Sampling

Events Patterns Statistics (1) Visualization

Show: 20 Per Page Format Preview: On

user	result	location	count
bob@medisurehealthnetwork.com	Failure	Russia	1

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

**89.144.44.41** was found in our database!

This IP was reported **20** times. Confidence of Abuse is **0%**: ?

0%

ISP	GHOSTNET GmbH
Usage Type	Data Center/Web Hosting/Transit
ASN	<a href="#">AS58212</a>
Hostname(s)	41.0-255.44.144.89.in-addr.arpa
Domain Name	ghostnet.de
Country	Germany
City	Frankfurt am Main, Hesse

IP info including ISP, Usage Type, and Location provided by [IPInfo](#). Updated biweekly.

Screenshot showing information about 89.144.44.41

**IP Abuse Reports for 89.144.44.41:**

This IP address has been reported a total of **20** times from 8 distinct sources. 89.144.44.41 was first reported on July 7th 2023, and the most recent report was **1 year ago**.

**Old Reports:** The most recent abuse report for this IP address is from **1 year ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp (UTC) ?	Comment	Categories
<a href="#">KTBSI18</a>	2024-01-23 09:07:27 (1 year ago)	Authentication-Results: spf=none (sender IP is 89.144.44.41) smtp.mailfrom=ullatdinerty.com; ... <a href="#">show more</a>	<a href="#">DDoS Attack</a> <a href="#">FTP Brute-Force</a> <a href="#">Phishing</a> <a href="#">Web Spam</a> <a href="#">Email Spam</a> <a href="#">Hacking</a> <a href="#">SQL Injection</a> <a href="#">Spoofing</a> <a href="#">Brute-Force</a> <a href="#">Bad Web Bot</a> <a href="#">Exploited Host</a>
<a href="#">Grepco</a>	2023-12-20 10:28:43 (1 year ago)	From: Dicks - Congratulations! [BLACKLISTED] Subject: Confirmation Needed Act Now! Ret ... <a href="#">show more</a>	<a href="#">Fraud Orders</a> <a href="#">Web Spam</a> <a href="#">Email Spam</a> <a href="#">Spoofing</a>
<a href="#">Grepco</a>	2023-11-25 00:22:17 (1 year ago)	From: ESPN+ <20JP056@437189022095718011.net> Subject: YOUR ESPN+ MEMBERSHIP HAS EXPIRED! .<br ... <a href="#">show more</a>	<a href="#">Fraud Orders</a> <a href="#">Web Spam</a> <a href="#">Email Spam</a> <a href="#">Spoofing</a>

Screenshot showing reports and comments about 89.144.44.41

**103.225.77.255** was found in our database!

This IP was reported **42** times. Confidence of Abuse is **0%**: ?

0%

ISP	Adsizzler Media Pvt Ltd
Usage Type	Unknown
ASN	Unknown
Domain Name	adsizzler.com
Country	India
City	Mumbai, Maharashtra

IP info including ISP, Usage Type, and Location provided by [IPInfo](#). Updated biweekly.

Screenshot showing information about 103.225.77.255

IP Abuse Reports for 103.225.77.255:			
This IP address has been reported a total of 42 times from 18 distinct sources. 103.225.77.255 was first reported on March 11th 2022, and the most recent report was 1 year Old Reports: The most recent abuse report for this IP address is from 1 year ago. It is possible that this IP is no longer involved in abusive activities.			
Reporter	IoA Timestamp (UTC)	Comment	Categories
✓ Anonymous	2024-04-22 08:52:00 (1 year ago)	Got Email with telling try to access from Russia and this was from India. Some companies use this ip address for training purpose. <a href="#">show less</a>	Web Spam Email Spam
🇺🇸 Red Lee	2023-10-24 03:17:52 (2 years ago)	Every day they try to get into my Microsoft account.	Hacking
🇺🇸 anrento	2023-10-20 23:31:03 (2 years ago)	spam	Web Spam Email Spam
🇺🇸 Grepco	2023-10-15 18:17:39 (2 years ago)	Same as everyone else. Received fraudulent MS email meant to scare. Ignore. Junk SPAM.	Email Spam Spoofing
✓ Anonymous	2023-10-08 17:35:09 (2 years ago)	Spoofing Microsoft account team.	Email Spam Spoofing
🇺🇸 Red Lee	2023-09-18 01:40:40 (2 years ago)	Reported by Microsoft, this IP invades my account day after day...and nothing is done to stop it.	Hacking
✓ Anonymous	2023-09-01 16:11:10	PART OF AN ELABORATE SCAM TO MAKE YOU THINK	

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.