# England National Health Centre (ENHC)

## Phishing Investigation – Executive Summary

### Phishing-Led Endpoint & Credential Compromise Simulation

**Organisation**: England National Health Centre (ENHC)
**Sector:** Healthcare / Public Health Services
**Cybersecurity Function**: Blue Team (SOC)
**Lead Analyst**: Joseph Christopher
**Date**: January 2026

---

## Organisational Overview

### Organisation Name:

England National Health Centre (ENHC)

### Industry:

Healthcare & Public Health Services

### Organisation Size:

Medium-sized healthcare organisation (clinical, administrative, and IT staff)

### Business Context

England National Health Centre (ENHC) delivers critical healthcare and patient services and relies heavily on internal email systems, clinical workstations, and web-based applications. These systems routinely process sensitive patient data, internal operational information, and staff credentials.

Due to the healthcare sector's high value to threat actors, ENHC is a prime target for phishing campaigns, credential harvesting, and follow-on abuse of user access.

Protecting endpoints, email infrastructure, and network communications is therefore a critical priority for the ENHC Security Operations Centre (SOC).

---

## 2. Introduction

This document presents the **final executive summary** of a **phishing-led security incident simulation** conducted within the England National Health Centre (ENHC) internal environment.

The objective was to:

- Simulate a realistic phishing and credential harvesting attack
- Validate detection and response capabilities
- Demonstrate **end-to-end SOC investigation workflows** using **evidence-based correlation**

No alert was treated in isolation. All findings were validated across **multiple telemetry sources** to ensure accuracy and reduce false positives.

---

## 3. Scope of Investigation

### In Scope

- Internal email delivery and user interaction
- Phishing link access and credential submission activity
- Endpoint telemetry and host-based events
- Network traffic monitoring and DNS activity

- SOC investigation, response, and validation

**Out of Scope**

- Cloud infrastructure
- Mobile devices
- Email gateway security platforms
- Third-party SaaS applications
- Full disk or memory forensics

---

## 4. Tools & Telemetry Sources

The investigation relied on multiple, corroborating telemetry sources:

- **GoPhish** – Phishing campaign delivery and user interaction tracking
- **hMailServer** – Internal email services and mail log evidence
- **Microsoft Defender for Endpoint (XDR)** – Endpoint protection, alerting, and automated investigation
- **Windows Endpoint Telemetry (Sysmon)** – Process creation, network connections, and host activity
- **Splunk Enterprise** – Centralised log ingestion, correlation, and investigation
- **pfSense Firewall** – Perimeter traffic visibility

- **Suricata IDS** – Network intrusion detection and HTTP/DNS inspection

---

## 5. Investigation Methodology

The investigation followed a structured **Security Operations Centre (SOC)** lifecycle:

**Detection → Triage → Correlation → Investigation → Response → Review**

Email telemetry identified phishing delivery, which was correlated with user interaction data from GoPhish. Endpoint and network telemetry were analysed within defined time windows to confirm malicious activity and rule out false positives.

Manual investigation techniques were used to mirror real-world SOC operations, with all workflows designed to be automation-ready for future SOAR integration.

---

## 6. Detection & Analysis Approach

An **evidence-based correlation model** was applied:

- DNS queries reviewed for suspicious domain resolution
- Source and destination IPs validated against campaign timelines
- Port and protocol analysis performed (e.g., DNS 53, HTTPS 443)
- Email delivery events correlated with user actions
- Endpoint telemetry reviewed for execution, persistence, or payload delivery

Time-bounded analysis ensured findings were accurate and contextualised within the incident window.

---

## 7. Artifacts & Evidence

### Indicators of Compromise (IOCs) & Forensic Artifacts

The following artifacts were reviewed and cross-validated:

- Phishing URLs accessed by ENHC users (Suricata HTTP & DNS logs)
- Source and destination IP addresses associated with outbound connections
- Ports and protocols indicating encrypted external communication
- Email sender identity and internal mailbox activity (hMailServer logs)
- Endpoint telemetry confirming user interaction without payload execution

All artifacts were correlated in **Splunk** to ensure **no reliance on single-source alerts**.

---

## 8. MITRE ATT&CK Mapping

Observed activity was mapped to the **MITRE ATT&CK** framework:

- **T1566 – Phishing**
- **T1071.004 – Application Layer Protocol (HTTPS)**

No evidence of:

- Execution

- Persistence
- Privilege escalation
- Lateral movement

was identified during the investigation.

---

## 9. Response & Containment Actions

Upon confirmation of credential harvesting activity, the following actions were taken:

- Impacted user credentials secured and reset
- Active sessions revoked to prevent further access
- Email activity reviewed for mailbox rules or abuse
- Endpoint telemetry reviewed to confirm no payload execution
- Continued monitoring enabled for affected users and IP addresses
- Phishing awareness reinforcement for staff

No post-exploitation activity or lateral movement was observed.

---

## 10. Mitigation & Hardening Measures

Post-incident actions focused on reducing future risk:

- Enforcement of **Multi-Factor Authentication (MFA)** using conditional access

- Improved visibility through tighter correlation of email, endpoint, and network logs
- Validation of endpoint integrity and credential exposure
- Refinement of SOC detection dashboards
- Reinforcement of internal phishing awareness controls

---

## 11. Playbooks, Process & Operations

The investigation adhered to a repeatable SOC playbook:

**Detection → Triage → Correlation → Investigation → Response → Review**

Although manual correlation was used, the workflow aligns with industry-standard SOC processes and is suitable for future automation and scaling.

---

## 12. MTTR & SOC Performance Metrics

- **Mean Time to Detect (MTTD):** Minutes after user interaction
- **Mean Time to Investigate (MTTI):** ~40 minutes
- **Mean Time to Respond (MTTR):** Within the same operational window

---

## 13. Lessons Learned

Aligned with **NIST CSF** principles:

- **Identify:** Comprehensive telemetry coverage is essential
- **Protect:** MFA significantly reduces credential abuse impact
- **Detect:** Cross-source correlation increases confidence
- **Respond:** Rapid containment prevents escalation
- **Recover:** Continuous monitoring and process improvement close the loop

---

## 14. Recommendations & Future Improvements

- Implement enterprise email authentication (SPF, DKIM, DMARC)
- Expand conditional access policies for healthcare users
- Formalise SOC incident response playbooks and escalation paths
- Introduce automated alert correlation to further reduce MTTR
- Enhance user reporting workflows for suspected phishing

---

## 15. Final Summary

This project demonstrates **England National Health Centre (ENHC)** SOC capability to **detect, investigate, and respond** to phishing-led threats using industry-standard tools and professional methodologies.

The investigation was **evidence-driven, structured, and aligned with real-world SOC best practices**, reflecting mature Blue Team operations suitable for healthcare environments.

---

## Architecture Overview

The architecture diagram illustrates the full telemetry and investigation flow across:

- Email delivery
- User interaction
- Endpoint visibility
- Network monitoring
- Centralised SOC investigation and response