# Security Incident Documentation
# Ransomware Attack via Phishing, Healthcare Case Study

### Introduction

This document demonstrates incident response documentation skills through analysis of a simulated ransomware attack against a small U.S. healthcare clinic. The objective is to clearly capture incident details, identify root cause, and document business impact using structured incident response practices.

## Incident Handler's Journal Entry

### Date

February 5, 2026

### Entry

1

### Description

This journal entry documents a simulated ransomware incident affecting a healthcare clinic. The attack resulted in encrypted systems, loss of access to patient records, and operational shutdown caused by a phishing-based malware infection.

### Tool(s) Used

None
*(Scenario-based analysis and documentation exercise)*

## The 5 W's

### Who caused the incident?

The incident was caused by an organized group of unethical hackers known to target healthcare organizations using ransomware attacks.

### What happened?

Attackers sent phishing emails containing a malicious attachment. Once downloaded, the malware deployed ransomware that encrypted critical systems and displayed a ransom note demanding payment in exchange for a decryption key.

### When did the incident occur?

The incident occurred on a Tuesday at approximately 9:00 a.m., when employees reported being unable to access systems and files.

### Where did the incident happen?

The incident occurred within the internal network of a small U.S.-based healthcare clinic providing primary care services.

### Why did the incident happen?

The incident occurred due to successful phishing emails that bypassed user awareness and security controls, allowing malware execution and ransomware deployment.

### Additional Notes

- The incident caused a complete shutdown of business operations due to loss of access to patient data.
- The organization contacted external entities for technical assistance and reporting.
- Preventative controls such as phishing awareness training, email filtering, endpoint protection, and regular backups could reduce the likelihood and impact of similar incidents.
- This scenario highlights the importance of incident response preparedness in healthcare environments.

## Key Takeaways

- Phishing remains a primary ransomware delivery method.

- Healthcare organizations are high-value targets due to sensitive data.
- Proper documentation is critical during early incident response stages.
- Business impact assessment is as important as technical analysis.

Prepared by: **Sambou Kamissoko**
LinkedIn: https://www.linkedin.com/in/sambouk/