# Incident Handler's Journal Entry

Date: June 23, 2025

Entry: 001

## Description

Documented a ransomware attack targeting a healthcare clinic. The incident resulted in critical service disruption and data encryption caused by phishing tactics.

## Tool(s) used

N/A for this entry (Scenario-based)

## The 5 W's

Who caused the incident?  
An organized group of unethical hackers known for targeting healthcare and transportation sectors.

What happened?  
The attackers sent phishing emails with malicious attachments, leading to the installation of malware and deployment of ransomware that encrypted critical business files.

When did the incident occur?  
Tuesday morning at approximately 9:00 a.m.

Where did the incident happen?  
At a small U.S. healthcare clinic specializing in primary-care services.

Why did the incident happen?  
Employees were deceived by phishing emails and unknowingly downloaded malware, which granted attackers access to the network and allowed them to deploy ransomware.

## Additional notes

This scenario highlights the importance of employee cybersecurity awareness training and phishing prevention. It also emphasizes the critical role of email security, endpoint protection, and a comprehensive incident response plan in safeguarding sensitive healthcare data.