Incident handler's journal - #1

Lab Description:

In this lab, I analyzed a ransomware attack that hit a small healthcare clinic. The attack caused employees to lose access to patient records and medical software. A ransom note appeared on all computers, demanding payment in exchange for a decryption key. The attackers used phishing emails with a malicious attachment to infect the network and encrypt files.

Date: Record the date of the journal entry.	**Entry:** #1
Description	A small healthcare clinic was hit by a ransomware attack that locked employees out of their computers and medical records. The attackers demanded money in exchange for the decryption key.
Tool(s) used	Email security filters, antivirus software, and incident response reporting tools.
The 5 W's	Capture the 5 W's of an incident. ● **Who**: A known group of cybercriminals that targets healthcare and transportation companies. ● **What:** Ransomware attack that encrypted all company files and shut down access to medical records. ● **When:** Tuesday morning around 9:00 a.m. ● **Where:** The clinic's internal network and employee computers. ● **Why**: The attackers used phishing emails with malicious attachments to infect the network and demand ransom money.
Additional notes	The incident forced the clinic to shut down operations and contact law

	enforcement and cybersecurity experts for help. This shows how dangerous phishing emails can be and why employees need better training to recognize them.