Incident handler's journal

Karthik S – Cyber Security Analyst

Date: August 2, 2025	**Entry:** 1
Description	This journal entry documents a ransomware incident at a small U.S. healthcare clinic, where phishing emails with malicious attachments led to the encryption of critical files, severely disrupting business operations.
Tool(s) used	No specific cybersecurity tools were mentioned in the incident response. Potential tools for analysis include anti-malware software (e.g., Malwarebytes) and email filtering systems (e.g., Microsoft Defender for Office 365).
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? - An organized group of unethical hackers targeting healthcare organizations. ● **What** happened? - Phishing emails with malicious attachments installed ransomware, encrypting critical files and displaying a ransom note demanding payment for decryption. ● **When** did the incident occur? - Tuesday, 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 downloaded malicious attachments from phishing emails, allowing attackers to deploy ransomware and encrypt files.
Additional notes	The incident highlights the need for employee training on phishing awareness and robust email filtering to prevent malicious attachments. Questions remain about the clinics backup systems and whether encrypted files can be restored

	without paying the ransom.