Incident handler's journal

Date: 27th april 2025	**Entry:** 1
Description	This journal entry documents a ransomware attack on a small U.S. healthcare clinic caused by a phishing email. The attack encrypted critical files, disrupted operations, and demanded a ransom for decryption.
Tool(s) used	• **Email Security Tools** (for phishing detection) • **Endpoint Detection & Response (EDR)** (to identify malware) • **Backup & Recovery Solutions** (if available for restoring files)
The 5 W's	● **Who caused the incident?** ○ An organized group of unethical hackers targeting healthcare and transportation industries. ● **What happened?** ○ Employees received phishing emails with malicious attachments, leading to ransomware deployment. Files were encrypted, and a ransom note demanded 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?** ○ Attackers exploited weak email security and employee awareness, tricking users into downloading malicious attachments.
Additional notes	• **Response Actions Taken:** ○ Systems were shut down to prevent further spread. ○ Incident was reported to authorities (e.g., FBI, HHS for healthcare breaches). • **Preventive Measures Needed:** ○ Employee training on phishing awareness. ○ Stronger email filtering and endpoint protection. ○ Regular backups tested for ransomware resilience.