Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: June 14, 2025	**Entry:** 1
Description	A ransomware attack disrupted operations at a small U.S. healthcare clinic. Patient records and other critical files were encrypted after attackers delivered malware through phishing emails. Employees were locked out and shown a ransom demand.
Tool(s) used	No specific tools were used at the time of the incident, but standard tools for investigation may include: ● Email security filters ● Endpoint detection & response (EDR) ● Antivirus software ● Ransomware decryptor tools
The 5 W's	● **Who caused the incident?** An organized group of unethical hackers known for targeting healthcare and transportation sectors.

	● **What happened?** A phishing attack led to ransomware installation, encrypting the clinic's files and displaying a ransom note demanding payment. ● **When did the incident occur?** Tuesday morning at approximately 9:00 a.m. ● **Where did the incident happen?** At a small U.S. based healthcare clinic specializing in primary care services. ● **Why did the incident happen?** Employees opened phishing emails with malicious attachments, which installed malware and allowed attackers to deploy ransomware.
Additional notes	This incident highlights the critical need for employee training on phishing awareness and layered email defenses. The clinic should implement multi-factor authentication (MFA), regular backups, and incident response planning. One question to investigate: **Were backups available and isolated from the attack?**