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: Record the date of the journal entry.	**Entry:** October 4, 2025
Description	A small U.S. healthcare clinic experienced a ransomware attack that disrupted operations and encrypted critical patient data. Employees reported being unable to access medical records and observed a ransom note on their screens. The attack appears to have originated from a phishing campaign targeting multiple employees. This journal entry documents the initial findings and analysis of the incident.
Tool(s) used	No tools used at this stage; initial information gathered from employee reports and system observations. (Future analysis may include tools such as Wireshark, Splunk, or endpoint detection and response software for investigation.)
The 5 W's	Capture the 5 W's of an incident. • Who: An organized cybercriminal group known to target healthcare and transportation industries.

	• What: A ransomware attack that encrypted files and displayed a ransom note demanding payment for decryption. • When: Tuesday morning at approximately 9:00 a.m. • Where: The clinic's internal computer network and systems across multiple employee workstations. • Why: Attackers gained access through phishing emails containing malicious attachments that installed malware, providing unauthorized network access for ransomware deployment.
Additional notes	The incident appears to be a targeted ransomware campaign against the healthcare sector. Patient data and business operations were significantly impacted, potentially violating HIPAA's data availability and confidentiality standards. Immediate steps should include isolating infected systems, preserving forensic evidence, and reporting the breach to appropriate authorities. It is essential to assess whether data backups exist and verify their integrity before attempting restoration. Staff cybersecurity awareness training should also be reinforced to prevent future phishing-related compromises.