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: November 25,2025	**Entry:** #1
Description	Documentation of security incident.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. ● **Who:** Unethical hackers ● **What:** Deployment of ransomware. ● **When**: Tuesday at 9:00 a.m. ● **Where**: Health care company. ● **Why**: Using targeted phishing emails, the attacker was able to gain access through malware once downloaded. Once malware was downloaded, ransomware was deployed encrypting critical files. Motivation appears to be financial due to ransom that was demanded in exchange for the encryption key.
Additional notes	1. Should the company pay the ransom during these scenarios? 2. How can we prevent this from happening again?