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: 24 May 2025	**Entry:** 1
Description	Summary of cybersecurity incident
Tool(s) used	None
The 5 W's	**Who**: Organized group of unethical hackers who are known to target organizations in healthcare and transportation industries. **What**: Employees were unable to access the files and software needed to do their job due to ransomware **When**: Tuesday morning, at approximately 9:00 a.m **Where**: At health care company **Why**: Hackers were able to gain access into the company's network by using targeted phishing emails which were sent to several employees. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded. Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The hackers demanded a large sum of money in exchange for the decryption key, motivation seems to be for financial gain.
Additional notes	Employees required additional training to avoid phishing attacks.

	The company needs to decide if they should pay ransom.