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: October 1, 2024	**Entry:** 1
Description	Mass phishing attack happened at a health care clinic. The phishing led to a ransomware attack.
Tool(s) used	No tools were used
The 5 W's	● **Who** caused the incident? ○ The threat actors ● **What** happened? ○ They sent out a email with a malicious file that encrypted the uses files if downloaded ● **When** did the incident occur? ○ Tuesday at 9am ● **Where** did the incident happen? ○ U.S. health care clinic ● **Why** did the incident happen? ○ Because a lack of training of the employees
Additional notes	The employees should be trained in cyber security protocols. Will the company pay the ransom, if not what will happen?