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: July 23, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	None.
The 5 W's	• **Who**: An organized group of unethical hackers • **What**: A ransomware security incident • **Where**: At a health care company • **When**: Tuesday 9:00 a.m. • **Why**: The incident occurred because a group of unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' intent appears to be financial demand because the ransom note they left requested a large sum of money in exchange for the decryption key.
Additional notes	1. How could the health care company prevent an incident like this from reoccurrence? 2. If the ransom is paid by the company, what is the assurance of receiving the decryption key in exchange from the hackers ?