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: May 21, 2024	**Entry:** #1
Description	Cybersecurity incident
Tool(s) used	None
The 5 W's	• **Who**: An organised group of unethical hackers • **What**: Ransomware • **Where**: Health care clinic • **When**: Tuesday 9:00 a.m. • **Why**: Unethical hackers gained access to the company's systems through a phishing attack. After infiltrating the systems, they deployed ransomware, encrypting critical files. The attackers were likely motivated by financial gain, as evidenced by the ransom note demanding a large sum of money for the decryption key.
Additional notes	It is necessary to find out whether there are any ways of decrypting the data other than paying the ransom. In addition, it is necessary to plan for the next steps to prevent ransomware attacks in the future.