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: 7/26/25	**Entry: 1**
Description	Documenting a ransomware incident that targeted a healthcare clinic.
Tool(s) used	

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ An organized group of hackers known to target healthcare and transportation organizations with ransomware.
	• **What** happened?
	  ○ Hackers gained access to the organization's system using phishing emails containing malicious attachments. Once they were in the system they deployed ransomware and encrypted critical data, leaving a ransom note for employees to see.
	• **When** did the incident occur?
	  ○ Tuesday at 9:00am
	• **Where** did the incident happen?
	  ○ On the healthcare company's systems and their databases containing critical patient data.
	• **Why** did the incident happen?

	○ The hackers were trying to extort the business for money in exchange for decrypting their information. They were successful in deploying a phishing attack which gave them access to the system and the ability to encrypt sensitive data.
Additional notes	While the immediate focus must be on trying to recover the encrypted data and contacting authorities to investigate this group, the company must make a stronger commitment in the future to educating their employees about the dangers of phishing and implementing other security controls to prevent it. This will help prevent another event like this in the future.