



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: Record the date of the journal entry.	Entry: #1
Description	Documenting a cybersecurity incident
Tool(s) used	-
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none">• Who: An organized group of unethical hackers who are known to target organizations in healthcare and transportation industries.• What: A ransomware attack.• When: Tuesday 9:00 AM.• Where At the healthcare company.• Why: The incident happened because of group of hackers that used phishing to gain access to organization's data. The workers were victims of phishing emails. The hackers wanted a large sum of money for unlocking data. We can assume that they had financial motivation.
Additional notes	Should the company pay the ransom for unlocking encrypted data?