



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: March 13, 2025	Entry: #1
Description	A healthcare clinic fell victim to a ransomware attack after phishing emails installed malware, encrypting crucial files and halting operations.
Tool(s) used	None.
The 5 W's	<ul style="list-style-type: none">• Who: Unethical hackers targeting health and transport sectors.• What :Phishing emails led to ransomware installation and file encryption.• When: Tuesday morning, around 9:00 AM.• Where: The healthcare clinic's internal network.• Why: Lack of email security awareness and vulnerability to phishing.
Additional notes	<ul style="list-style-type: none">• The clinic had no defense against phishing, disrupting patient care.• Security experts were contacted to restore data from backups.• Questions on improving cybersecurity to prevent future attacks were raised.