



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: 06/09/25	Entry: Journal Entry 1
Description	Provide a brief description about the journal entry. A health care clinic experienced a security incident on Tuesday at 9:00 a.m. which severely disrupted their business operations.
Tool(s) used	List any cybersecurity tools that were used. There were no cybersecurity tools used to prevent this attack.
The 5 W's	Capture the 5 W's of an incident. <ul style="list-style-type: none">• Who caused the incident? A group of Unethical hackers• What happened? The group sent a mass phishing email that turned into a ransomware attack.• When did the incident occur? On Tuesday at 9am.• Where did the incident happen? A U.S. Healthcare Clinic• Why did the incident happen? The incident happened because the group of unethical hackers were targeting the clinic and employees gave access to the hackers by clicking on the phishing email.
Additional notes	Include any additional thoughts, questions, or findings. There were no security measures put in place to prevent the attack.