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: Nov 21st ,2025	**Entry:** #1
Description	This journal entry describes a ransomware attack that seriously disrupted activities at a tiny healthcare practice. The event was caused by a phishing email, which resulted in file encryption and system shutdown.
Tool(s) used	No tools were used during this documentation activity.
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? An organized group of unethical hackers carried out the attack after employees fell for targeted phishing emails. ● **What** happened? The problem occurred on Tuesday about 9:00 a.m., when personnel lost access to their systems and patient records. ● **When** did the incident occur? The problem occurred on Tuesday about 9:00 a.m., when personnel lost access to their systems and patient records. ● **Where** did the incident happen? The attack occurred at a modest U.S. healthcare facility that provides primary care. ● **Why** did the incident happen? The incident happened when staff downloaded a fraudulent email attachment, allowing attackers to penetrate the network and install ransomware.

Additional notes	This event highlights the need for robust email filtering systems and frequent personnel cybersecurity training. The assault also underlines the importance of dependable data backups and an adequate incident response strategy in order to preserve continuity of care and minimize operational interruption.