**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:**  24th July, 2025. | **Entry:**  Entry 1 | | |
| --- | --- | --- | --- |
| Description | At 9:00 a.m. on a Tuesday, a U.S. healthcare clinic was hit by a ransomware attack. Phishing emails with malware let attackers access the network, encrypt patient data, and shut down operations. A ransom note demanded payment to restore the files. | | |
| Tool(s) used | None were mentioned in the scenario | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? A group of organized attackers known for targeting healthcare and transportation industries. * **What** happened? A ransomware attack disrupted operations and encrypted sensitive files. * **When** did the incident occur? Around 9:00 a.m. on a Tuesday. * **Where** did the incident happen? At a small U.S. healthcare clinic. * **Why** did the incident happen? Due to insufficient email filtering, lack of security monitoring, and likely absence of antivirus defenses, which allowed phishing emails to succeed and malware to execute. | | |
| Additional notes | This case shows how one phishing email can disrupt an entire clinic. Strong employee training, antivirus tools, and backup systems are essential. It raised questions for me about incident response readiness and whether SIEM tools or MFA could’ve helped prevent the damage. | | |