**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:**  02/23/24 | **Entry:**  1 | | |
| --- | --- | --- | --- |
| Description | A small U.S. health care clinic experienced a ransomware attack | | |
| Tool(s) used | To my knowledge none were used | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? A group of unethical hackers * **What** happened? Ransomware was installed onto company computers causing medical records and important files to be held hostage through encryption * **When** did the incident occur? Tuesday morning 9:00 am * **Where** did the incident happen? A small U.S. health care clinic * **Why** did the incident happen? Employees unknowingly downloaded malware from an email phishing scam | | |
| Additional notes | How did the email appear from the employees perspective? Did they feel it was an important work document? We need to find this information out so we can prevent something of this nature happening again. | | |