**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:**  6/21/2023 | **Entry:**  #1 |
| Description | security incident |
| Tool(s) used | none |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** group of hackers * **What** ransomware attack * **When** did the incident occur? 6/21/2023 at 9:00 AM * **Where** did the incident happen? At a health care company * **Why** did the incident happen? a group of hackers accessed the network with phishing attacks and installed ransomware on the company's system. the hackers demanded monetary compensation for the decryption key |
| Additional notes | Should we pay the ransom for the decryption of the files?  How can we prevent this from happening again? |

|  |
| --- |
| Reflections/Notes: Record additional notes. |

**we must prioritize training employees about phishing and how to protect ourselves from it, so that we can prevent this situation in the future**