**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 8, 2023 | **Entry:**  1 |
| Description | The journal is about an incident which took place at a small health care clinic in the US. |
| Tool(s) used | - |
| The 5 W's | Capture the 5 W's of an incident.   * A group of Hackers caused the event through a social engineering technique * A ransomware encrypted the data * The incident happened on Tuesday at 9:00 a.m. * The incident happened in a small health care clinic in USA * The incident happened because an employee opened a phishing email which contained a malicious file. |
| Additional notes | 1. How could the health care company prevent an incident like this from  occurring again?  2. Should the company pay the ransom to retrieve the decryption key? |