**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:** 28-Dec-2023 | **Entry:** #1 | | |
| --- | --- | --- | --- |
| Description | Document of a cybersecurity incident | | |
| Tool(s) used | None | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: An organized group of unethical hackers * **What**: A ransomware * **When**: Tuesday at 9:00 a.m. * **Where**: A small U.S. health care clinic * **Why**: The group of hackers sent a phishing email to one of the employees, containing a malicious attachment. Once downloaded, the ransomware that the group had designed before, was executed on its own and encrypted the data on the server. The attackers demanded money to decrypt the files, showing financial reasons as their motivation. | | |
| 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? | | |