**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:** July 23, 2024 | **Entry:** #1 |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | None. |
| The 5 W's | * **Who**: An organized group of unethical hackers * **What**: A ransomware security incident * **Where**: A small U.S. health care clinic * **When**: Tuesday morning, 9:00 a.m. * **Why**: The unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The motive seems to be money since they demanded a large sum of money for the decryption key. |
| Additional notes | 1. How can the health care company make sure to prevent an incident like this from ever occurring again? 2. Should the company pay the ransom to retrieve the decryption key? |