



# 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.

<b>Date:</b> July 23, 2024	<b>Entry:</b> #1
Description	Documenting a cybersecurity incident
Tool(s) used	None
The 5 W's	<ul style="list-style-type: none"><li>• <b>Who:</b> An organized group of unethical hackers</li><li>• <b>What:</b> A ransomware security incident</li><li>• <b>Where:</b> At a health care company</li><li>• <b>When:</b> Tuesday, 9:00 a.m.</li><li>• <b>Why:</b> The incident occurred because unethical hackers gained access to the company's systems through a phishing attack. Once inside, the attackers deployed ransomware, encrypting critical files. The motivation appears to be financial, as the ransom note demanded a large sum in exchange for the decryption key.</li></ul>
Additional notes	<ol style="list-style-type: none"><li>1. How could the health care company prevent a similar incident in the future?</li><li>2. Should the company pay the ransom to recover the encrypted data?</li></ol>

