



# 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> 22 Dec,2023	<b>Entry:</b> #1
Description	Ransomware incident on a small U.S. health care clinic
Tool(s) used	N/A
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> : Ransomware attack</li><li>• <b>When</b> : on Tuesday at 9:00 a.m</li><li>• <b>Where</b> : At a U.S health care clinic</li><li>• <b>Why</b> : Attackers gained access company's network using targeted phishing emails , sent to employees. Emails contained malicious attachment that installed malware on the employee's computer once it was downloaded.Attackers gained access, deployed their ransomware, encrypted critical files</li></ul>
Additional notes	The health care clinic should hire security personnels to defend against any future similar incidents.