

Incident handler's journal

Date: Record the date of the journal entry.	Entry: 5/28/25
Description	Documenting a cybersecurity incident
Tool(s) used	None
The 5 W's	<ul style="list-style-type: none">● Who: An organized group of unethical hackers● What: A ransomware security incident● Where: A healthcare company● When: Tuesday 9:00 a.m.● Why: The incident occurred because a group of unethical hackers gained access to the company's systems by performing a phishing attack. After gaining access, the attackers launched ransomware on the company's systems which encrypted critical files. The attackers' motivation appears to be financial because they left a ransom note demanding a large sum of money in exchange for the decryption key.
Additional notes	<ol style="list-style-type: none">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?