Incident Handler's Journal

Date: May 22, 2025	**Entry:** 1
Description	Documenting 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 caused this incident. • **What?** A ransomware security incident. • **When?** Tuesday, May 20, 2025 at 9:00 AM. • **Where?** A small healthcare clinic in Chicago, IL. • **Why?** The hackers gained access to the company's systems through phishing emails. After gaining access, they launched their ransomware attack. Their motivation is financial; they left a ransom note demanding a large sum of money in exchange for the decryption key.
Additional notes	1. Does the company conduct routine cybersecurity training? 2. Should they pay the ransom to receive the decryption key?

Date: June 10, 2025	**Entry:** 2
Description	Investigating a suspicious file hash
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. • **What**? An employee downloaded a malicious attachment from an email • **When**? Wednesday, July 20, 2022 • **Where**? Organization workplace
Additional notes	

Date: June 11, 2025	**Entry:** 3
Description	Investigating and responding to a phishing incident
Tool(s) used	Phishing playbook
The 5 W's	Capture the 5 W's of an incident. • **Who**? Malicious threat actor using the email: 76tguyhh6tgftrt7tg.su • **What**? Employee downloaded a malicious attachment from a phishing email • **When**? Wednesday, July 20, 2022 • **Where**? Organization workplace • **Why**? Employee missed signs of phishing and downloaded a malware file
Additional notes	Attachment was verified as malicious; medium severity.