Incident handler's journal

Date: 8/22/25	**Entry:** 1
Description	This entry is about documenting the incident and the events leading to it.
Tool(s) used	Logs, Databases, SIEM, Sandbox environment
The 5 W's	Capture the 5 W's of an incident. ● **Who**: Organized group of unethical hackers known to target healthcare facilities ● **What** happened? A phishing email was sent to an employee with a malicious file download. Upon downloading the file, a ransom note appeared on the screen claiming to have encrypted important files and demanding payment for the return of access. ● **When** did the incident occur? Tuesday, 9 A.M. ● **Where** did the incident happen? Small U.S. healthcare clinic ● **Why** did the incident happen? A phishing email attachment was downloaded onto an employee computer
Additional notes	Which employee? What was the history of the employee? Which organized group of unethical hackers?

Date: 8/25/25	**Entry:** 2

Description	A phishing alert has been sent based on an employee opening and downloading a password protected email file attachment.
Tool(s) used	VirusTotal, SHA256 hash
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? Threat actor sent a phishing attempt to an employee ● **What** happened? The employee downloaded and opened the password-protected attachment in the phishing email ● **When** did the incident occur? Wednesday, July 20, 2022 ● **Where** did the incident happen? On company property on an employee machine ● **Why** did the incident happen? The employee thought the email was legitimate job candidate applying for the engineering position
Additional notes	Who is the threat actor(s)? What led to the employee downloading and opening the file on their computer, could this have been prevented?