Incident handler's journal

By: cammi.sec

Date: July 7, 2025	**Entry: 001**
Description	A small U.S. health care clinic received a ransomware attack on Tuesday at approximately 9am, where they had all the company's files encrypted by an organized group of unethical hackers, asking for a large amount of money to provide the decryption key. Business operations shut down because employees were unable to access the files and software needed to do their job.
Tool(s) used	n/a
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? An organized group of unethical hackers ● **What** happened? Phishing emails were sent to several employees with a malicous attachment. After gaining access, the group encrypted all the company's files. ● **When** did the incident occur? On Tuesday morning, around 9am. ● **Where** did the incident happen? At a small health care clinic in the U.S. ● **Why** did the incident happen? The cause of the security incident was a phishing email that contained a malicious attachment. It happened due to lack of employee experience in recognizing malicious and fake emails. Also, if an IDS was implemented, it could have been avoided.
Additional notes	To avoid future breaches, it's important to provide proper cybersecurity training for all employees, and implement tools to help identify and block suspicious emails.