Incident handler's journal

Date: May 10, 2023,	**Entry:** #001
Description	Incident log of the ransomware attack on the healthcare clinic.
Tool(s) used	CERT (Computer Emergency Response Team)
The 5 W's	• **Who** caused the incident? An unethical group of hackers was responsible for the ransomware attack on the healthcare clinic. • **What** happened? The hackers used a phishing email with a malicious attachment to install ransomware on the clinic's systems and encrypt their files. • **When** did the incident occur? The incident took place on Tuesday at 9:00 a.m., severely disrupting business operations. • **Where** did the incident happen? The incident occurred at the healthcare clinic, where the ransomware affected their systems and files. • **Why** did the incident happen? The incident occurred because the hackers employed phishing emails to deceive employees and gain access to the clinic's systems, with the intention of obtaining a ransom payment in exchange for the decryption key.
Additional notes	It is important to investigate how the hackers managed to send the phishing emails to multiple employees of the clinic and whether there were any vulnerabilities in the organization's security systems that facilitated unauthorized access.

Reflections/Notes: Additionally, it is crucial to consider the necessary prevention and recovery measures to prevent future similar attacks and protect sensitive patient data.