Incident handler's journal

Date: 25 Aug, 2024	**Entry:** 1
Description	A ransomware attack triggered by phishing emails to a small US health care clinic's employees. Their business operation was not able to access the critical patient data due to this incident.
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 who are known to target organizations in healthcare and transportation industries. • **What** happened? Critical data files were encrypted by attackers, and attackers ask for a ransom in exchange for the decryption key. • **When** did the incident occur? On a Tuesday around 9am. • **Where** did the incident happen? A small U.S. health care clinic specializing in delivering primary-care services. • **Why** did the incident happen?The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company.
Additional notes	This organization should raise the awareness of phishing emails to their internal employees. Do not download files that are from suspicious senders which might cause other cyberattacks, i.e. DoS, mansomeware, etc.