Incident handler's journal

Date: July, 1st, 2025	**Entry:** 1
Description	A small US health care clinic experienced a security insident on Tuesday 9.00 AM which severely disrupted their business operations.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An organized group of unethical hackers • **What** happened? A phishing email that contained malicious attachment. Once it was downloaded, ransomware was deployed encrypting the clinic's computer files. The clinic was demanded money in exchange for the decryption key. • **When** did the incident occur? On Tuesday, July 1st, 2025 at 9.00 AM • **Where** did the incident happen? In a small US health care clinic • **Why** did the incident happen? The incident happened because the health care clinic fell victim to a phishing attack.
Additional notes	**Human error**: An employee opened a phishing email and downloaded a malicious attachment, which is a common tactic used by cybercriminals. **Lack of awareness or training**: This suggests that the staff may not have been properly trained to recognize phishing attempts.

	Insufficient email security: Their email system likely did not have effective filtering to block or quarantine suspicious attachments. **Lack of endpoint protection**: Once the ransomware was downloaded, it was able to execute and encrypt the clinic's files—indicating a lack of strong endpoint protection or antivirus systems. In short, the incident happened due to a combination of social engineering (phishing), inadequate cybersecurity defenses, and possibly poor employee cybersecurity awareness.