Incident handler's journal

Date: October 17, 2024	**Entry: #1**
Description	A small U.S. healthcare clinic specializing in primary-care services experienced a ransomware attack on a Tuesday morning, around 9:00 a.m. Employees reported being unable to access critical files, including medical records, which caused a full shutdown of business operations. A ransom note appeared on their computers, demanding a large sum of money for a decryption key to unlock the encrypted files.
Tool(s) used	None.
The 5 W's	• **Who**: an organized group of unethical hackers • **What**: a ransomware attack caused by phishing emails, encrypting critical medical files and demanding ransom for decryption. • **When**: Tuesday at approximately 9:00 a.m. • **Where**: a small U.S. healthcare clinic's internal network and computer systems. • **Why**: The hackers aimed to exploit the clinic's vulnerability in employee awareness and email security, targeting healthcare organizations for financial gain.
Additional notes	1. Investigate if any known decryption tools can be used to avoid paying the ransom. 2. Review data backup strategies to ensure the clinic can restore operations quickly in the future without relying on decryption from attackers. 3. Use stronger email filters or employee training on phishing awareness to prevent this incident from happening again