Incident handler's journal

Date: Tuesday, July 8th 2025	**Entry:** #000000000 **Incident Responder:** Trevor Stahl **EmployeeID:** 1234567890-tcs
Description	Documenting a cybersecurity incident, ransomware attack.
Tool(s) used	None
The 5 W's	**5Ws:** • **Who:** Organized group of hackers • **What:** Ransomware attack • **When:** Tuesday, July 8th 2025 @ 9AM central time • **Where:** At hypothetical healthcare company • **Why**: Attackers initially launched a phishing campaign. After this allowed access to critical file systems and databases, the attackers used ransomware software to encrypt our critical data and left a message requesting payment in exchange for the decryption keys to our compromised data.
Additional notes	1- How did this phishing attack bypass the email spam and malware filters? 2- When and what was the last cybersecurity awareness training and phishing prevention education for the employees targeted in the phishing attack? 3-