



Incident handler's journal

Date: February 1, 2024	Entry: #1
Description	Documenting a cybersecurity incident
Tool(s) used	No tools were used in this incident
The 5 W's	<p>Capture the 5 W's of an incident.</p> <ul style="list-style-type: none">• Who: Organized group of unethical hackers• What: A ransomware security incident• When: Tuesday at 9:00 am• Where: A small U.S. health clinic• Why: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	Seems proper training for employees needs to be implemented to help spot suspicious emails.