📝 Incident Handler's Journal Entry by Jordan Butler

📅 **Date:** Tuesday, July 29, 2025
📋 **Entry #:** 001

🧠 Journal Description:

This journal entry documents a ransomware attack that occurred at a small U.S. healthcare clinic. The attack disrupted primary-care operations and prevented access to patient data and critical files. The incident has been attributed to a phishing campaign that installed malware, leading to ransomware deployment.

🧩 The 5 W's

- **Who caused the incident?**
  The incident was caused by an **organized group of unethical hackers** known for targeting the healthcare and transportation industries.
- **What happened?**
  Employees received **phishing emails** containing malicious attachments. After downloading the files, **malware was installed**, allowing attackers to deploy ransomware that **encrypted critical business and patient data**.
- **When did the incident occur?**
  The incident took place on a **Tuesday morning around 9:00 a.m.**
- **Where did the incident happen?**
  The attack occurred within the **internal network of a small U.S. healthcare clinic**.
- **Why did the incident happen?**
  The attackers exploited **human error through phishing** to gain access. The lack of adequate **email filtering and user training** likely contributed to the success of the attack.

💬 Additional Thoughts/Questions

This scenario highlights the importance of **cyber hygiene and employee awareness training**, especially in industries like healthcare where sensitive data is constantly handled. I would like to know whether the clinic had **offline backups** or an **incident response plan**, and if law enforcement was contacted. It also raises the question of whether they had **cyber insurance** to cover the costs of recovery.
