**Incident Handler's Journal**

**Date:** 28 March 2025

**Entry:** 1 (for cousera google cybersec)

**Description:** A small U.S. health care clinic experienced a ransomware attack that disrupted business operations by encrypting critical patient data. The attack originated from phishing emails containing malicious attachments. Employees downloaded the attachment, which installed malware that allowed attackers to deploy ransomware.

**Tool(s) Used:**

- Antivirus software (for detection and analysis)
- Firewall logs (to track unauthorized access)
- Email security tools (to analyze phishing emails)
- Incident response tools (for mitigation and remediation)

**The 5 W's:**

**Who caused the incident?** An organized group of unethical hackers known for targeting the healthcare and transportation industries.

**What happened?** Employees unknowingly downloaded malware from phishing emails, allowing attackers to deploy ransomware that encrypted critical business files.

**When did the incident occur?** Tuesday morning at approximately 9:00 a.m.

**Where did the incident happen?** At a small U.S. healthcare clinic, specifically affecting employee computers and patient records stored on the network.

**Why did the incident happen?** The attack occurred due to successful phishing emails that bypassed security measures, leading employees to download a malicious attachment. Once executed, the malware enabled attackers to encrypt files and demand ransom.

**Additional Notes:**

- Employees need phishing awareness training to prevent similar incidents.
- Strengthening email security and implementing endpoint protection can reduce risks.
- Conducting regular data backups with offline storage can mitigate ransomware damage.
- Multi-factor authentication (MFA) should be enforced for accessing critical systems.
- Consider a cybersecurity insurance policy for financial protection against future incidents.