Incident handler's journal Zikpi Agbemenyo Kossi

zikpiagbemenyokossi@gmail.com

Cyber Security Portfolio

Incident investigation into a Small US Healthcare Clinic.

Date: July 23, 2024	**Entry:**
Description	Documenting a cybersecurity incident
Tool(s) used	None , only Social Engineering
The 5 W's	• **Who**: An organized group of unethical hackers? • **What**: A ransomware security incident • **Where**: At a health care company • **When**: Tuesday 9:00 a.m. • **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.
Recommendations and lesson learned To avoid future similar incident	1. How could the health care company prevent an incident like this from occurring again? Training Employees about Social Engineering 2. Should the company pay the ransom to retrieve the decryption key? Even if the company pay the ransom there is no they will have the decryption key. A general and Quick assessment of the Situation must be done first.