Incident handler's journal - U.S. health care

A small U.S. health care clinic experienced a security incident on Tuesday at 9:00 a.m. which severely disrupted their business operations. The cause of the security incident was a phishing email that contained a malicious attachment. Through the download, ransomware was deployed and encrypted the organization's computer files.

Date: May 29, 2024	**Entry:** #1
Description	Documenting a cybersecurity incident
Tool(s) used	SIEM: Chronicle Malware Analysis: CrowdStrike Mail Analysis: Mimecast Recovery: Acronis for restoring the backups
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.
Additional notes	1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key? 3. What employee downloaded and opened the file? 4. How can we make our emails safer? 5. Who sent the email?