Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: Tuesday, 9:00 am	**Entry:** Entry 1
Description	A small U.S. healthcare clinic experienced a ransomware attack that prevented employees from accessing medical records and critical systems, severely impacting their healthcare operations.
Tool(s) used	• Possible tools: antivirus, antimalware, EDR (Endpoint Detection and Response), backup systems, secure email gateways (not specifically listed in the scenario).
The 5 W's	• **Who caused the incident?** An organized group of unethical hackers known for targeting the healthcare and transportation sectors. • **What happened?** A phishing email with a malicious attachment was sent to several employees. Once downloaded, ransomware was deployed, encrypting

	the clinic's critical files and demanding payment for the decryption key. • **When did the incident occur?** Tuesday at 9:00 AM. • **Where did the incident happen?** On the internal computer network of the healthcare clinic. • **Why did the incident happen?** An employee downloaded a malicious attachment from a phishing email, which allowed the attackers to gain access to the network and deploy ransomware.
Additional notes	• The organization should improve email security practices, including anti-phishing filters and ongoing employee training. • It is recommended to have an incident response plan and regularly updated offline backups. • The clinic should report the incident to the relevant authorities and consult cybersecurity professionals for mitigation and recovery.