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: January 17, 2026	**Entry:** #1
Description	Documenting a ransomware security incident at a primary-care health clinic.
Tool(s) used	**None.**
The 5 W's	• **Who:** An organized group of unethical hackers known for targeting the healthcare and transportation industries. • **What:** A ransomware attack that encrypted critical files and medical records, resulting in the total shutdown of business operations. • **When:** Tuesday morning at approximately 9:00 a.m. • **Where:** A small health care clinic specializing in primary-care services in the United States. • **Why:** The incident occurred because hackers used targeted phishing emails to trick employees into downloading a malicious attachment, which then deployed ransomware to encrypt files for financial gain.

Additional notes	1. What protocols are in place for data backups, and can the systems be restored without paying the ransom? 2. How can the clinic improve its email filtering and employee security awareness training to prevent future phishing attempts?