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: 8/10/23	**Entry: 1**
Description	Provide a brief description about the journal entry. Small US health clinics had their business compromised on Tuesday at 9 AM via a phishing email. The hackers are using ransomware to halt operations until they receive payment.
Tool(s) used	List any cybersecurity tools that were used. none
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Malicious hackers target healthcare and transportation services • **What** happened? Business operations were halted by ransomware • **When** did the incident occur? Tuesday at 9AM • **Where** did the incident happen? A small US health clinic • **Why** did the incident happen? Staff was not educated about phishing emails and to not access unknown attachments
Additional notes	Include any additional thoughts, questions, or findings. How do we prevent this from happening again?

	Should the company pay the ransomware?

Date: 8/17/23	**Entry: 2**
Description	Provide a brief description about the journal entry. Employee received and downloaded an email attachment that contained a password for the attachment within the email. Upon entering the password, a malicious payload was executed on their computer.
Tool(s) used	List any cybersecurity tools that were used. SHA256 hash of the file VirusTotal
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Malicious hacker, “Clyde West” targeted the HR department • **What** happened? Employee downloaded and executed a malicious file onto their computer • **When** did the incident occur? 1:11 PM • **Where** did the incident happen? Financial service company • **Why** did the incident happen? Staff was not educated about phishing emails and to not access unknown attachments
Additional notes	Include any additional thoughts, questions, or findings. Legitimate phishing email. • Sender’s email is not from a known/trusted domain • Improper grammar used in the body of the email • Resume files would not need to be password protected