Incident handler's journal

Date: 10 April 2024	**Entry:#1**
Description	At 9am on Tuesday, a group of unethical hackers used phishing to deploy malware onto computers for a healthcare clinic which encrypted patient records disrupting business activities.
Tool(s) used	None
The 5 W's	• **Who -** Incident was caused by a group of unethical hackers. • **What -** Ransomware attack deployed via phishing, which encrypted patient records. • **When -** The incident occurred on the 10th of April 2024 at 9am. • **Where -** The incident occurred at the targeted healthcare clinic. • **Why -** The incident occurred because of phishing which allowed for malware to be installed. The unethical hackers demanded a ransom to decrypt the patient records data.
Additional notes	1. There is a need to review the teaching at the company against phishing attacks and update the playbooks so that a quicker response can take place and business operations are not disrupted. 2. Should the company pay the ransom ?

Date: 21 April 2024	**Entry:#2**
Description	Review of file hash loaded onto computer after spreadsheet download which led to multiple unauthorized executable files being offloaded onto the computer.
Tool(s) used	VirusTotal
The 5 W's	• **Who** - Employee downloaded spreadsheet file from malicious email • **What** - Spreadsheet file which led to encryption • **When** - 21 April 2024 at 1:11 pm • **Where** - Financial Services company • **Why** - Result of a phishing email
Additional notes	1. Employees need to be educated further on attacks and methods with which malicious actors use. 2.

Date: 23 April 2024	**Entry:#3**
Description	Continued look into entry #2 where executable files were loaded onto a personal computer after a phishing email attack was successful
Tool(s) used	VirusTotal
The 5 W's	• **Who** - Employee downloaded a malicious file and opened it on a personal computer • **What** - Executable file encrypted and locked the computer's files • **When** - 21 April 2024 • **Where** - At the office • **Why** - Successful phishing attack
Additional notes	File was verified to be malicious. The alert has been escalated to a level two SOC analyst.

Date: 06 May 2024	**Entry: #4**
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur?

	• **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.