Incident handler's journal

Date: 2nd July 2025	**Entry:** 1
Description	Documenting a phishing and ransomware incident.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. • **Who:** a group of unethical hackers. • **What:** A ransomware incident • **When:** on Tuesday at 9:00 am • **Where:** a health care company in the US • **Why:** The hackers got access to their computers after sending phishing emails. They prevented employees from accessing files on their computers.
Additional notes	1. Should the ransom be paid? 2. How can the health care company prevent an incident of this form from happening again.

Date: 8th July 2025	**Entry:** 2
Description	Documenting a phishing attack

Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. ● **Who**: a phishing attacker. ● **What**: a file was been downloaded on an employee's computer ● **When**: Wednesday, July 20, 2022 09:30:14 AM ● **Where**: on an employee's computer at a financial company ● **Why**: the employee received a phishing email form the hacker.
Additional notes	Include any additional thoughts, questions, or findings.

Date: 10th July 2025	**Entry:** 3
Description	An individual (hacker or attacker) got access to customer data due to a vulnerability of the e-commerce we application. When the attacker got access to the data, he mailed an employee of the company on December 22, 2022 at approximately 3:13 p.m., claiming he has access to customer data and requested $25,000 cryptocurrency payment. But the employee assumed the email to be a spam and deleted it. On the December 28, 2022, the same employee received another email from the same sender claiming that he has access to customer data, but this time he added a sample of the stolen customer data while requesting for $50,000.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. ● **Who**: an individual (hacker) ● **What**: the attacker threatened an employee to pay $50,000 cryptocurrency or else customer data will be released to the public.

	● **When**: December 28, 2022 at 7:20p.m ● **Where**: an employee's computer ● **Why**: due to a vulnerability in the e-commerce web application.
Additional notes	To prevent future recurrences, we are taking the following actions: ● Perform routine vulnerability scans and penetration testing. ● Implement the following access control mechanisms: ▪ Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range. ▪ Ensure that only authenticated users are authorized access to content.

Date: 12th July 2025	**Entry:** 4
Description	It's a website traffic investigation
Tool(s) used	wireshark
The 5 W's	Capture the 5 W's of an incident. ● **Who**: not stated ● **What**: not stated ● **When**: not stated ● **Where** not stated ● **Why**: not stated
Additional notes	Include any additional thoughts, questions, or findings.

Date: 12th July 2025	**Entry:** 5
Description	A suspicious malicious file was being downloaded on an employee's computer. So it had to be investigated and solved
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● **Who**: phishing attacker ● **What**: a phishing email was sent to an employee ● **When**: not stated ● **Where**: on an employee's computer ● **Why**: the employee downloaded a file from the phishing email.
Additional notes	The employees of that company should be educated on phishing emails and it's effects and preventions.