Incident handler's journal

Date: 12/11/2025	**Entry:** 1
Description	Document a cibersecurity incident to a small U.S. health care clinic specializing in delivering primary-care services
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **WHO: The incident was cause by a group of unethical Hackers** • **WHAT: The group of unethical Hackers send gmail´s to the workers of the U.S health care clinic, when the workers click on the link, a form of ransomware** • **WHEN: The incident ocurr on Tuesday morning, at approximately 9:00 a.m** • **WHERE: In the U.S health care clinic** • **WHY: The incident occurred because a group of unethical hackers sent a phishing email to employees. Opening the email infected the system with ransomware. The ransomware encrypted the files and prevented access until a ransom was paid. The motive appears to be financial.**
Additional notes	Should the company pay the hackers? Should the company provide cybersecurity training and services to its employees?

Date: 12/21/2025	**Entry:** 2
Description	Document an incident that occurred related to a file containing malware, analyzed using the virustotal tool
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● **Who** : unknown by gmail ● **What** :I received an alert about a suspicious file being downloaded on an employee's computer (financial services company). We discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer. ● **When: 1:11 p.m.** ● **Where** In the financial services company workspace ● **Why** The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer
Additional notes	It's important to never trust anything or anyone, especially not a file sent via Gmail. Using sandboxes and tools like VirusTotal, you can observe and analyze whether the contents of that file are malicious or not.

Date: 12/22/2025	**Entry:** 3
Description	Continuing with the problem that occurred yesterday related with the email and the

	harsh file
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● **Who** Clyde West ● **What** A possible phissing attack ● **When** **1:11 p.m.** ● **Where** In the financial services company workspace ● **Why** The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer
Additional notes	Include any additional thoughts, questions, or findings.

Date: 12/23/2025	**Entry:** 4
Description	Major security incident involving a data breach of over one million users.(Recently, the company experienced a major security incident involving a data breach of over one million users. Because this was a recent and major security incident, my team is working to prevent incidents like this from happening again)
Tool(s) used	none
The 5 W's	Capture the 5 W's of an incident. ● **Who** :A anonymous individual ● **What** : An individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information ● **When** : on December 28, 2022, at 7:20 p.m., PT ● **Where** :In a Gmail of a costumer

	• **Why** :The root cause of the incident was identified as a vulnerability in the e-commerce web application. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. This vulnerability allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated.
Additional notes	Part of the job of cybersecurity is prevent and ensure that the security of the people is always the first priority. This scenarios generate frustration but also makes us more aware about new ways that problems can occur.

Reflections/Notes: