Incident handler's journal

Date: February 1, 2024	**Entry: #1**
Description	Documenting a cybersecurity incident
Tool(s) used	No tools were used in this incident
The 5 W's	Capture the 5 W's of an incident. ● **Who**: Organized group of unethical hackers ● **What**: A ransomware security incident ● **When**: Tuesday at 9:00 am ● **Where**: A small U.S. health clinic ● **Why**: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key.
Additional notes	Seems proper training for employees needs to be implemented to help spot suspicious emails.

Date: February 2, 2024	**Entry: # 2**
Description	Document a cybersecurity event
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. ● **Who**: An employee of a financial service company ● **What**: malware was downloaded from an email attachment ● **When**: 1:11 pm ● **Where**: Employees workstation ● **Why**: The incident occurred because an employee downloaded an attachment from an email that had malware attached to it.
Additional notes	Over 50 vendors reported the file as malicious. A Sha256 hash value was used to capture the file for it to be decrypted by VirusTotal. The file is a known malware Flagpro that has been commonly used by advanced threat actor BlackTech.

Date: 2/3/2024	**Entry: #3**
Description	Document a cybersecurity event
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. ● **Who**: A vulnerability in the companies web-application allowed for the attack to occur ● **What**: An attacker was able to gain unauthorized access to customer PII and financial information ● **When**: December 28, 2022 at 7:20 p.m. PT ● **Where**: Occurred onsite at a company facility ● **Why:** a vulnerability in the e-commerce web application allowed an 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.
Additional notes	Due to a vulnerability in the web-application customer data was able to be stolen. This included PII and financial information. Some preventative tactics that were put in place post-incident were performing routine vulnerability scans and penetration testing. Also implementing the following access control mechanism: implementing allowlisting to allow access to specified set of URLs and automatically block all requests outside of this URL range; ensure that only authenticated users are authorized access to content.