



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: 12/8/2023	Entry: #1
Description	Documenting a cybersecurity incident
Tool(s) used	None
The 5 W's	<ul style="list-style-type: none">• Who unethical hackers• What A ransomware security incident• When At a health care company• Where Tuesday 9:00 a.m.• 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	Company should do routine back ups (preferably on tape drives). The company should also invest in anti-virus software and train employees on how to spot common phishing attacks.