



# Incident handler's journal

## Scenario

A small U.S. health care clinic specializing in delivering primary-care services experienced a security incident on a Tuesday morning, at approximately 9:00 a.m. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job. Additionally, employees also reported that a ransom note was displayed on their computers.

<b>Date:</b> 06/09/2024 Record the date of the journal entry.	<b>Entry: #1</b>
Description	Employees at a U.S. health care clinic were locked out of their files by a ransomware attack.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. <ul style="list-style-type: none"><li>• <b>Who:</b> A group of unethical hackers</li><li>• <b>What:</b> A ransomware attack</li><li>• <b>When:</b> Tuesday, June 4th at 9:00 AM</li><li>• <b>Where:</b> At a small health clinic in the U.S.</li><li>• <b>Why:</b> An employee clicked on an attachment sent by a phishing email</li></ul>
Additional notes	It would be recommended for the company to provide training for their employees to help prevent further incidents like this in the future.