# Incident handler's journal

| | |
|---|---|
| **Date:**<br>09/01/2023 | **Entry: #1 - Small Business in Lima, Peru** |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | None |
| The 5 W's | • **Who**: An organized group of unethical hackers<br>• **What**: A social engineering incident using Vishing and Whaling method<br>• **When**: At a small convenient store - Small Business<br>• **Where**: Sunday 11:30 pm<br>• **Why**: The incident happened when the owner of the convenience store answered her business phone during off business hours to the criminals who attempted to psychologically manipulate her in exchange for 1 million of dollars in a wire transfer. The attackers rushed the owner to act quickly to protect herself from an arrest using an accusation of releasing child pornography under her name. The attackers' motivation appears to be financial because of manipulating her to comply in their vishing and whaling attack for money. |
| Additional notes | 1. How could the owner and business prevent an incident like this from occurring again?<br>2. Should they restrict phone calls out of business hours?<br>3. What are their physical and cyber security measures?<br>4. Educate business owners and employees for this incident and how to prevent them, especially on Vishing and Whaling. |