## **Parking lot USB exercise**

| **Contents** | The USB drive contains a mix of personal and work files as well as some personal photos. Some of these files appear to contain some sensitive information and PII. The work files in particular include a resume, hire letter, and employees scheduling and budget likely all containing sensitive information. It is best practice to keep work and personal files stored separately. |
| --- | --- |
| **Attacker mindset** | The information on this drive could be used against employees, relatives or Jorge himself. The employee budget and schedule likely have personal information that could be used by an attacker against employees of the Hospital. There is also a personal wedding list which would contain names and possibly addresses of Jorge’s family and friends. Lastly it is possible this USB drive is a trap that was intentionally left for someone to use on their device which may allow a threat actor to gain backdoor access to the business or install malware. |
| **Risk analysis** | If this was a USB baiting attack a threat actor could have gained unauthorized access to a system or infected that device and system with malicious code. They could also gain access to sensitive information like financial data or username/passwords and possibly use that to gain authorization to personal or business systems or even use the information for identity theft. |