## **Parking lot USB exercise**

| **Contents** | This USB drive appears to be a personal device belonging to Jorge Bailey. It’s a mixed use device and there are files that contain PII such as family photos and resumes as well as potentially sensitive work related information in the shift schedules and the employee budget files. Work and personal files should always be stored separately as it reduces the attack surface if somebody were to obtain this information. |
| --- | --- |
| **Attacker mindset** | Jorge’s personal information on the USB can be used against him as people would know his phone number and address from the resume, and the faces of all of his family and relatives through the family photos. The information found on the employee budget and shift schedules could be maliciously used to disrupt business operations at the hospital. |
| **Risk analysis** | This USB could have contained malware which could infect the computer and track all of the activity of that computer, including sensitive payment information or business information. If a threat actor found this device, they could do harm to Jorge personally through identity theft or physical harm by knowing his family and address. Or, they could harm the organization by accessing the employee budget and spreading the information. We can reduce risk through employee awareness training, and installing anti virus to prevent malicious code being executed. |