## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | The pen drive belongs to Jorge and it contains images of his family, images of his dog, his resume and other files like employee budget sheet etc.. It has sensitive information like employee budget which isn’t supposed to be available to everyone. It is also not advisable to store both professional and personal information at the same place. |
| **Attacker mindset** | Using the budget sheet we can gain vital information about the employees, we can use the pics against their relatives and using docs like the shift schedules and hire letters we can gain access to the business as well. |
| **Risk analysis** | Promoting employee awareness about these types of attacks  and what to do when a suspicious USB drive is a managerial  control that can reduce the risk of a negative incident. Setting up routine antivirus scans is an operational control that can be  implemented. Another line of defense could be a technical  control, like disabling AutoPlay on company PCs that will prevent a computer from automatically executing malicious code when a USB drive is plugged in. |