## **Parking lot USB exercise(USB baiting)**

| **Contents** | *The USB drive contains the PII of its owner Jorge, an employee at the hospital, with his personal information. Storing personal files with work files is never a good idea as it raises the risk of exploiting both categories at once* |
| --- | --- |
| **Attacker mindset** | USB can have malware that can be transferred to the system it is attached to, moreover, if it is not an attacker’s trap then Jorge PII can trouble his close one as it has information of his wedding and personal pictures which can be used against him if it goes into the wrong hands, information for shifts can lead to information about other employees which will eventually be used against him |
| **Risk analysis** | Promoting employee awareness about these types of attacksand 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. |