Parking lot USB exercise

## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | Some documents contain personal information that Jorge would prefer to keep private. Additionally, the work files include the PII of others and sensitive details about the hospital's operations. |
| **Attacker mindset** | Timesheets can give an attacker valuable insight into Jorge's colleagues. Both work-related and personal information could be exploited to deceive him. For instance, a malicious email could be crafted to appear as if it were sent by a coworker or relative. |
| **Risk analysis** | Raising employee awareness about these types of attacks and instructing them on how to handle suspicious USB drives is a managerial control that helps reduce the risk of security incidents. Implementing routine antivirus scans serves as an operational control to detect and mitigate potential threats. Additionally, a technical control, such as disabling AutoPlay on company PCs, can prevent malicious code from executing automatically when a USB drive is inserted, adding another layer of defense. |