## **Parking lot USB exercise**

| **Contents** | The information found on the USB stick contains some work files, such as the shift schedules or employee budget. These are also mixed in with personal files, including a wedding list and vacation ideas. It is not generally safe to mix work files with personal files, or use work files on a USB stick on personal devices. |
| --- | --- |
| **Attacker mindset** | The information contained in some of these files could be used maliciously against the hospital and Jorge himself. The employee budget could be discovered by employees who leak it, creating issues among other employees. Leaking the shift schedules could have other implications, such as attackers knowing when certain people are not working. Personal files could be infected with malicious code that, when used on the work network, could infect all devices connected to the network. |
| **Risk analysis** | Having policies in place that require separate USB sticks for work can help mitigate risk relating to malicious code. The possibility of the stick being stolen could also be reduced by requiring the stick to not leave the hospital if possible. |