## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | The USB drive contains a mix of personal and work-related files. It includes folders with family and pet photos, a new hire letter, and an employee shift schedule. While the photos may not contain sensitive information, work-related files like the new hire letter and shift schedule could potentially include personally identifiable information (PII) and sensitive business data. |
| **Attacker mindset** | This information could be used against Jorge or the hospital in various ways. An attacker could leverage the work-related files to impersonate Jorge or gain insight into the hospital's operations. If an attacker staged the USB drive, they might have targeted Jorge or someone he knows, exploiting their curiosity to introduce malware into the hospital's network. |
| **Risk analysis** | To mitigate USB-baiting attacks, technical controls such as endpoint security solutions capable of detecting and blocking malicious files on USB drives can be implemented. Operational controls like security awareness training for employees to recognize and avoid suspicious USB drives and enforcing policies prohibiting using personal USB drives for work-related tasks can also mitigate risks. Furthermore, implementing strict access controls and encryption for sensitive files can reduce the impact of unauthorized access to data. |