## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | The USB drive contains a mixture of personal and work-related files. It includes personal photos and documents, as well as work-related files such as a new hire letter and an employee shift schedule. Storing personal files with work files on the same device may pose a security risk, especially if the drive is lost or falls into the wrong hands. |
| **Attacker mindset** | An attacker could potentially use the information found on the USB drive to target Jorge or other employees. They might use personal photos and documents to launch social engineering attacks or gain personal information for identity theft. Work-related files like the employee shift schedule could be used to impersonate an employee or gain insights into the hospital's operations. Additionally, the attacker might try to establish a backdoor into the hospital's systems. |
| **Risk analysis** | To mitigate USB baiting attacks, several controls should be in place. First, employees should be educated about the risks associated with using unknown USB drives and discouraged from plugging them into workstations. Technical controls like endpoint security software should be implemented to detect and prevent malicious code from executing on the system. Employees should be trained to recognize social engineering tactics and verify the authenticity of files before opening them. Strict policies should also be in place regarding the separation of personal and work files on storage devices to minimize security risks. Regular security awareness training and drills can help employees recognize and respond to potential threats effectively. |