## **Parking lot USB exercise**

|  |  |
| --- | --- |
| **Contents** | The USB stick contains a mix of personal and work-related files. The work-related documents, such as the "New hire letter" and "Shift schedules," may contain personally identifiable information (PII), including employee names, contact details, and possibly sensitive work-related data. Additionally, there are personal folders like "Family photos" and "Our dog pics," indicating a mix of personal and work information stored together. |
| **Attacker mindset** | An attacker could use the personal and work-related files found on the USB drive to target Jorge or his colleagues. For instance, sensitive work documents like the new hire letter and shift schedules could provide insight into the hospital’s operations, allowing the attacker to craft targeted phishing attacks. The personal files, such as family and dog photos, could be leveraged for social engineering attacks, making it easier to deceive Jorge or his family members. Additionally, the attacker might use the USB to gain unauthorized access to the hospital’s network, potentially establishing a backdoor to steal confidential information. |
| **Risk analysis** | USB baiting attacks can deliver various types of malicious software, such as keyloggers, ransomware, or spyware, potentially compromising the entire network. If another employee had plugged the USB into a non-virtualized system, malware could spread across the organization's devices, leading to data breaches or financial losses. Sensitive information on the device, such as employee records or operational files, could be used for identity theft or to exploit weaknesses in the organization’s security. Implementing strict policies, such as disabling USB ports, using encryption, and training employees on USB safety, can mitigate these risks. |