## **Parking lot USB exercise**

### **Contents**

The USB drive contains both personal and work-related files, including a new hire letter, an employee shift schedule, and a budget tracker, along with personal items like vacation ideas and wedding plans. Some of these files may contain personally identifiable information (PII) such as employee names, schedules, or financial details. Storing personal and work files together increases the risk of exposure, especially if the drive is lost or compromised.

### **Attacker Mindset**

An attacker who gains access to this USB drive could exploit the work-related files to launch phishing attacks against the hospital or its employees. Employee schedules could help attackers plan social engineering attacks, while hiring documents may contain sensitive HR information. Additionally, personal files could be used to target Jorge or his relatives, either through identity theft or personalized scams.

### **Risk Analysis**

USB baiting attacks can introduce various types of malware, including keyloggers, ransomware, or remote access trojans (RATs), which could compromise the hospital's network if an unsuspecting employee plugs it in. Even if the USB contains no malware, an attacker could use the information within the files to plan further attacks, such as spear phishing or business email compromise (BEC). To mitigate these risks, organizations should enforce strict USB policies, including disabling USB ports on workstations, using endpoint protection software, and educating employees about the dangers of unknown USB devices. Additionally, personal and work files should be stored separately to reduce exposure risks.