Parking lot USB exercise

Contents	The USB drive contains a mix of personal and work-related files, including family and pet photos, an employee shift schedule, and a new hire letter. These documents contain personally identifiable information (PII) and internal organizational data. It is not safe to store personal and work files on the same device, as it increases exposure to both types of information if lost or compromised.
Attacker mindset	An attacker could use the personal images and HR documents to conduct spear phishing attacks targeting Jorge or his coworkers. The employee schedule and new hire details might help in crafting convincing emails or impersonation attempts. This data could also be used to learn more about internal hospital operations and exploit known employees.
Risk analysis	Malicious software like keyloggers, ransomware, or remote access tools could be hidden on USB drives. If an infected device were accessed by an unsuspecting employee, it could compromise the hospital's systems. Sensitive information such as employee schedules and PII could be leveraged for social engineering attacks. To mitigate these risks, organizations should enforce strict USB use policies, deploy endpoint protection, conduct employee training, and use sandboxed virtual environments for testing unknown devices.