Parking lot USB Analysis

Contents	The USB drive contains both personal files, such as family and pet photos, and work-related files, including a new hire letter and an employee shift schedule. While there are no files that explicitly contain PII, the presence of a new hire letter and an employee shift schedule suggests that it might contain sensitive work-related information. Storing personal files with work files on the same drive is generally not safe practice, as it can create a risk of exposing sensitive work-related information to personal use.
Attacker mindset	An attacker could potentially use the information on the USB drive against Jorge or the hospital in various ways. For instance, they might use the personal photos to craft convincing social engineering attacks or use the work-related files for spear-phishing. This information could also be used to impersonate Jorge or other hospital employees, potentially gaining unauthorized access to the business's systems. It's possible that the whole event was staged by an attacker who planted the USB drive to target Jorge or others.
analysis	*While the USB drive doesn't appear to contain malicious code, it still poses security risks. An attacker could hide various types of malicious software on such devices, potentially leading to the infection of the hospital's systems if it were discovered and connected to a workstation. The sensitive information on the device, particularly work-related files, could be used for impersonation, social engineering, or targeted attacks against Jorge or the hospital. To mitigate USB baiting attacks, technical controls like endpoint security solutions, operational controls such as user training and awareness, and managerial controls like strict USB usage policies should be implemented. Additionally, keeping personal and business drives separate is a good practice to reduce risks associated with USB baiting.*