Parking lot USB exercise

Contents	The USB drive appears to contain a mix of personal and work-related files that belong to the employee. Some of the documents include personal details, such as contact information and internal notes, while others include workplace materials related to ongoing projects. Storing both types of data on the same device increases the risk of exposing sensitive information if the USB is lost or accessed by someone else.
Attacker mindset	An attacker could use the information on the USB to learn personal details about the employee and identify coworkers or departments they interact with. This knowledge could be used to craft convincing phishing emails or impersonation attempts that appear legitimate. Work-related documents could also reveal internal operations or schedules that an attacker might exploit to target the organization more effectively.
Risk analysis	USB baiting attacks carry significant risk because unknown drives can contain malware designed to automatically execute when plugged into a computer. Employees may unknowingly expose the organization if they plug in a suspicious drive out of curiosity. Technical controls such as disabling AutoRun and requiring endpoint protection can help reduce this risk. Managerial controls like employee training and awareness campaigns teach staff how to recognize and report suspicious devices. Regular antivirus scanning and strict policies on removable media usage add additional layers of defense against potential threats.