Parking lot USB exercise

Contents	The USB drive contains both personal and work related files, including family and pet photos, a new hire letter and an employee shift schedule. This mix of data suggests the drive belongs to Jorge Bailey from HR. Some of the files may contain sensitive personally identifiable information (PII) and confidential employee data.
Attacker mindset	An attacker could use the employee shift schedule to plan social engineering attacks, such as phishing or impersonation. The personal photos and HR files could be used to craft convincing spear-phishing emails targeting Jorge or other staff. It's also possible the USB was planted intentionally to lure a victim into plugging it in.
Risk analysis	USB baiting attacks can deliver malware such as ransomware, spyware, or remote access trojans (RATs). If infected, the device could give an attacker access to internal systems or sensitive HR data. To prevent such risks, organizations should enforce technical controls like disabling USB ports or using endpoint protection software. Operational and managerial controls like employee training and USB usage policies also help reduce the likelihood of falling for baiting attacks.