Parking lot USB exercise

Contents	• There is a mix of data on the medium. There is confidential company data, such as a budget summary, presentation. There are also private files, such as photos or a guest list, containing their data, which should not fall into the wrong hands. You should not use one medium to store work and private data because it increases the risk of data leakage and potential infection.
Attacker mindset	• A hacker could use private information and photos to impersonate someone online. Company budget data could be given to a competitor for financial gain. Work schedule data could even be used to rob someone's home while they're working.
Risk analysis	• Using one data carrier for private and work purposes carries a high risk. Potential USB infection at home could result in a large data leak, encryption or serious material damage to the company. Malware could infect the entire internal network of the company. Anything could be found on such carriers. From personal data, important personal and company documents.