

Parking lot USB exercise

Contents	<p>The device holds files containing personally identifiable information (PII), including employee work schedules and payroll budgets. It also stores sensitive work documents such as hiring letters and résumés. Keeping personal files together with work-related files is unsafe, as it increases the risk of exposing confidential information if the device is lost.</p>
Attacker mindset	<p>The information on Jorge's device could be used against him or the hospital by exposing sensitive details such as employee schedules and payment information, which could allow someone to track an employee's whereabouts over time and potentially target their home or family. This data could also be exploited to harm other employees by revealing private work-related information. Additionally, personal details about relatives could be used for social engineering or harassment. Moreover, access to sensitive documents and internal schedules could provide a gateway for unauthorized individuals to gain access to the hospital's business operations or systems.</p>
Risk analysis	<p>USB bait attacks can deliver malware such as ransomware, keyloggers, or remote access trojans that compromise security. If an infected device is discovered by an employee, it could spread malicious code throughout the network, causing data breaches or operational disruptions. Threat actors might find sensitive information like employee schedules, payroll data, and hiring documents, which could be exploited</p>

	<p>for identity theft or targeted attacks. To mitigate these risks, organizations should implement strict policies prohibiting the use of unknown USB devices, employ endpoint security solutions with malware detection, and conduct regular employee training on the dangers of USB bait attacks.</p>
--	---