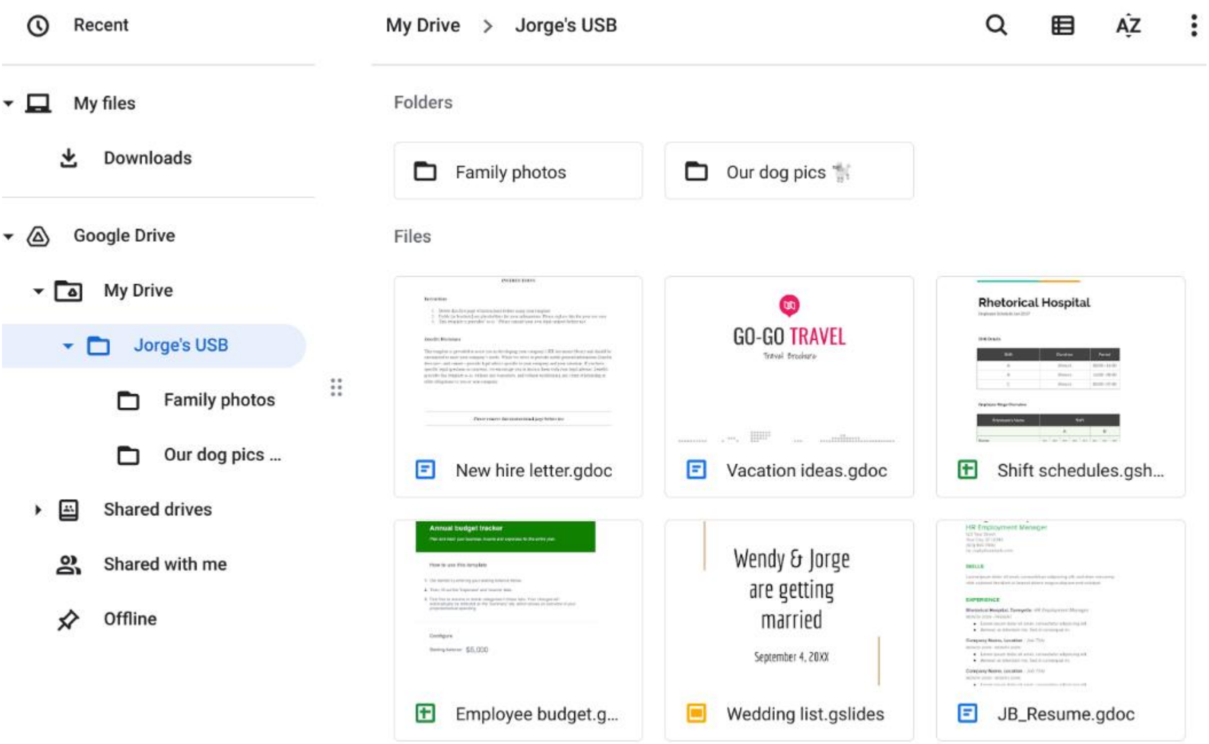
Parking lot USB exercise

Contents	Write 2-3 sentences about the types of information found on this device. • *Are there files that can contain PII?* • *Are there sensitive work files?* • *Is it safe to store personal files with work files?*
	The USB drive contains a mixture of personal and work-related files, including family and pet photos, a new hire letter, and an employee shift schedule. These files contain personally identifiable information (PII) such as full names, addresses, dates, employee information, and company budgets. It is not safe to store personal files alongside work files, as it increases the risk of exposing sensitive corporate data and creates vulnerabilities for both the individual and the organization.
Attacker mindset	Write 2-3 sentences about how this information could be used against Jorge or the hospital. • *Could the information be used against other employees?* • *Could the information be used against relatives?* • *Could the information provide access to the business?*
	An attacker could use Jorge's personal information to conduct targeted phishing or social engineering attacks, using details about his family and personal life to appear credible. The shift schedule and new hire letter could be exploited to identify other employees, understand the hospital's organizational structure, and plan attacks during shifts with fewer staff members. Additionally, knowing Jorge's role in human resources and having access to sensitive documents such as budgets and employee information, an attacker could impersonate him to gain unauthorized access to the hospital's systems or conduct further attacks against other staff members.
Risk analysis	Write 3 or 4 sentences describing technical, operational, or managerial controls that could mitigate these types of attacks: • *What types of malicious software could be hidden on these devices? What could have happened if the device were infected and discovered by another employee?* • *What sensitive information could a threat actor find on a device like this?* • *How might that information be used against an individual or an organization?*

	To mitigate USB baiting attacks, the hospital should implement technical controls such as disabling unauthorized USB ports, using updated antivirus software, and intrusion detection systems that automatically scan all external devices. Operational controls should include a strict "do not plug in unknown devices" policy, regular employee training on cybersecurity risks, and mandatory use of virtualized environments to inspect any suspicious devices before connecting them to the corporate network. Managerial controls must include clear policies on separating personal and work files, reporting procedures for suspicious devices found on company premises, and periodic audits to verify compliance with security policies. If the device had been infected, it could contain malware such as keyloggers, ransomware, or trojans that could compromise the entire hospital network, steal sensitive patient data, or install backdoors for future unauthorized access.


Recent
My files
Downloads
Google Drive
My Drive
Jorge's USB
Family photos
Our dog pics ...
Shared drives
Shared with me
Offline
My Drive > Jorge's USB
Folders
Family photos
Our dog pics
Files
New hire letter.gdoc
GO-GO TRAVEL
Vacation ideas.gdoc
Rhetorical Hospital
Shift schedules.gsh...
Annual budget tracker
Employee budget.g...
Wendy & Jorge are getting married
September 4, 20XX
Wedding list.gslides
JB_Resume.gdoc