

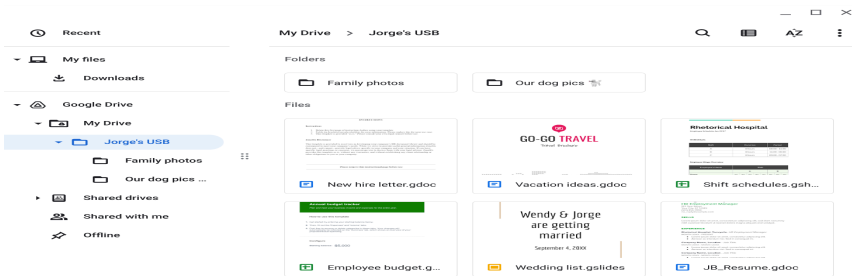
Parking lot USB exercise

Scenario

Review the following scenario. Then complete the step-by-step instructions.

You are part of the security team at Rhetorical Hospital and arrive to work one morning. On the ground of the parking lot, you find a USB stick with the hospital's logo printed on it. There's no one else around who might have dropped it, so you decide to pick it up out of curiosity.

You bring the USB drive back to your office where the team has virtualization software installed on a workstation. Virtualization software can be used for this very purpose because it's one of the only ways to safely investigate an unfamiliar USB stick. The software works by running a simulated instance of the computer on the same workstation. This simulation isn't connected to other files or networks, so the USB drive can't affect other systems if it happens to be infected with malicious software.

Contents	<div>The screenshot shows a Google Drive window titled 'My Drive > Jorge's USB'. On the left is a sidebar with navigation options: Recent, My files, Downloads, Google Drive, My Drive (selected), Shared drives, Shared with me, and Offline. Under 'My Drive', 'Jorge's USB' is expanded, showing sub-folders 'Family photos' and 'Our dog pics ...'. The main area displays a grid of files: 'Family photos' folder, 'Our dog pics' folder, 'New hire letter.gdoc', 'Vacation ideas.gdoc', 'Employee budget.g...', 'Wendy & Jorge are getting married' (with date September 4, 2000), 'Wedding list.gslides', 'Rhetorical Hospital' folder, 'Shift schedules.gsh...', and 'JB_Resume.gdoc'.</div> <p>The contents do contain PII: name of employee, home address, job location, resume containing a lot of information about Jorge, his pictures and family pictures.</p> <p>There are files containing sensitive information about hospitals: the employee budgets, the hospital shifts.</p> <p>Looks like Jorge was careless to use the same USB for work and personal use.</p>
Attacker mindset	<p>An attacker could use the sensitive personal and work-related files to impersonate Jorge, target his family, or access internal hospital systems. Information like budget files and shift rosters could be leveraged to exploit the organization. SPII, such as health or HR records, may also be used to gain unauthorized access or extort victims.</p>

Risk analysis

If this USB contained malware such as keyloggers or ransomware, plugging it into an unsuspecting employee's machine could lead to infection of the local system or even spread across the network. A threat actor could extract confidential files and use personally identifiable information (PII) to impersonate individuals, access internal systems, or launch further attacks on the organization.

To mitigate these risks, organizations should implement the following controls:

- Install and regularly update "antivirus" and "anti-malware" software on all company devices.
- Disable the "autorun" feature for USB drives to prevent automatic execution of potentially malicious code.
- Encrypt USB drives and require password protection to prevent unauthorized access to stored data.
- Train employees to never plug in "unknown" or "lost" USB devices into their workstations.
- Establish a policy that mandates any "found USB device" must be handed to the security team for analysis in an "isolated environment" (such as a virtual machine or sandbox).