Activity Overview

In this activity, you will assess the attack vectors of a USB drive. You will consider a scenario of finding a USB drive in a parking lot from both the perspective of an attacker and a target.

USBs, or flash drives, are commonly used for storing and transporting data. However, some characteristics of these small, convenient devices can also introduce security risks. Threat actors frequently use USBs to deliver malicious software, damage other hardware, or even take control of devices. **USB baiting** is an attack in which a threat actor strategically leaves a malware USB stick for an employee to find and install to unknowingly infect a network. It relies on curious people to plug in an unfamiliar flash drive that they find.

Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

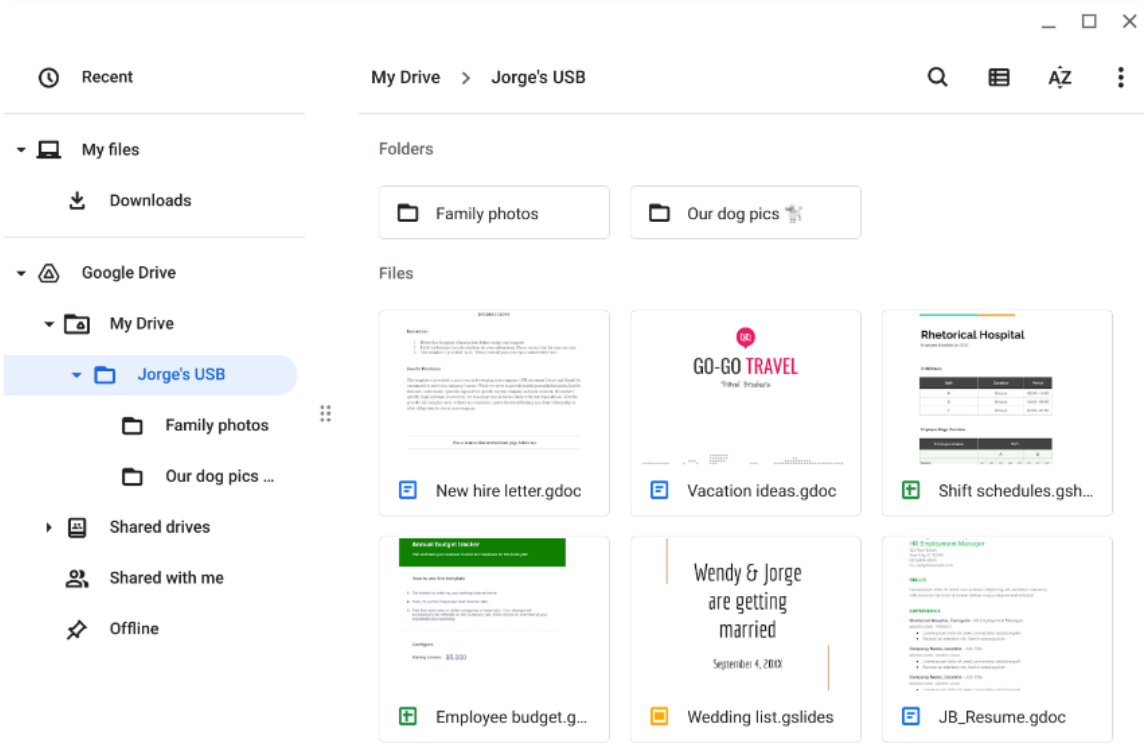
Scenario

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.

You create a virtual environment and plug the USB drive into the workstation. The contents of the device appear to belong to Jorge Bailey, the human resource manager at Rhetorical Hospital.



Jorge's drive contains a mix of personal and work-related files. For example, it contains folders that appear to store family and pet photos. There is also a new hire letter and an employee shift schedule.

Parking lot USB exercise

Contents	Write **2-3 sentences** about the types of information found on this device. *There are some files containing PII such as Family photos file and dog pics file. There are also sensitive work files in the USB stick such as employee budget and shift schedules. Storing personal files and work files together is risky because it might exploit by unauthorized user.*
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. *The information in USB stick could be used against other employees which attacker can utilize employee shift schedule.* *Jorge could be deceived by leveraging either professional or personal details. For instance, a deceptive email might seem to originate from a colleague or family member.*
Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: *There might be viruses or spyware hidden in the USB stick. Viruses can replicate themselves and infect other files on the computer once infected USB is inserted while spyware is designed to gather information without user's consent. Threat actor could find a lot of sensitive information as example time sheet, budget allocation and user personal information. This information can be used to granting access towards system or phishing individual.*