Parking lot USB exercise (My Responses)

Contents	Write **2-3 sentences** about the types of information found on this device. *Based on the scenario and notes, the USB drive contains a mix of personal and professional files belonging to Jorge Bailey, the HR manager at Rhetorical Hospital. Some documents include personally identifiable information (PII), such as names and shift schedules of employees, while others hold personal family and pet photos. This combination of sensitive data increases the risk of both privacy breaches and targeted attacks.*
Attacker mindset	Write **2-3 sentences** about how this information could be used against Jorge or the hospital. *Based on the scenario and notes, an attacker could use the work-related PII (timesheets) to provide an attacker intel about other people in order to craft convincing phishing emails, impersonating colleagues or supervisors. The personal photos and files could help build a social engineering profile to manipulate or trick Jorge. Even if the files are not malicious themselves, the drive may have been planted intentionally to bait someone into plugging it into a secure system.*
Risk analysis	Write **3 or 4 sentences** describing technical, operational, or managerial controls that could mitigate these types of attacks: *Based on this scenario and the notes; to mitigate risks from USB baiting attacks, organizations should implement technical controls such as disabling AutoPlay and restricting USB access on company devices. Promoting employee awareness can reduce the risk of a negative incident. For instance, setting up regular antivirus scans and endpoint protection software can help detect malware early. Additionally, on the operational side, using virtualization software to analyze unknown USBs is a safe best practice. Managerial controls like security awareness training can teach employees not to plug in unknown USBs and report such incidents immediately to the IT department.*

Notes:

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

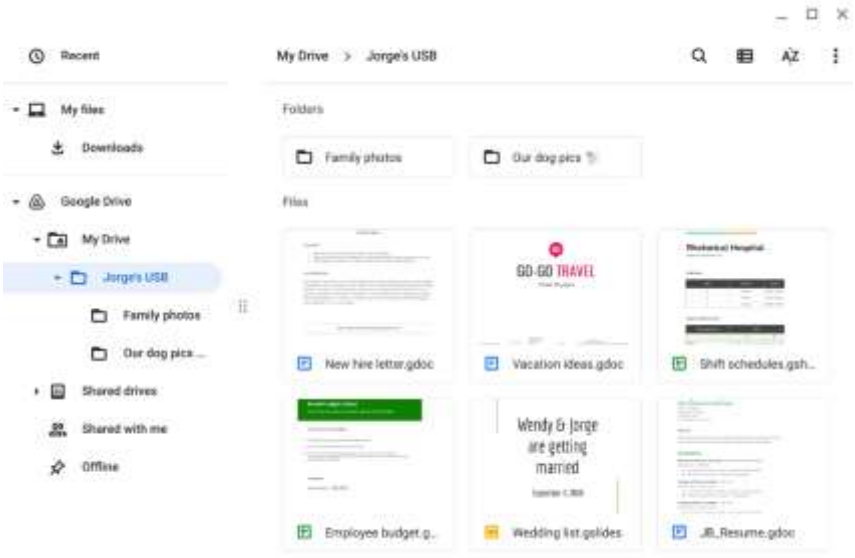
Review the following scenario. Then complete the step-by-step instructions.

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.

Step 2: Inspect the contents of the USB stick

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.

Review the types of information that Jorge has stored on this device. Then, in the **Contents** row of the activity template, write **2-3 sentences** (40-60 words) about the type of information that's stored on the USB drive.

Note: *USB drives often contain an assortment of personally identifiable information (PII). Attackers can easily use this sensitive information to target the data owner or others around them.*

Step 3: Apply an attacker mindset to the contents of the USB drive

The flash drive appears to contain a mixture of personal and work-related files. Consider how an attacker might use this information if they obtained it. Also, consider whether this whole event was staged.

For example, an attacker could have placed these files on the USB drive as a distraction. They might have targeted Jorge or someone he knows, hoping they would find the device and plug it into their workstation. In doing so, the attacker could establish a backdoor into the company's systems while the unsuspecting target browsed through the files.

In the **Attacker mindset** row of the activity template, write **2-3 sentences** (40-60 words) about how this information could be used against Jorge or the hospital.

Pro tip: *The Cybersecurity and Infrastructure Security Agency (CISA) provides some security tips on using caution with USB drives , including keeping personal and business drives separate.*

Step 4: Analyze the risks of finding a parking lot USB

You have *not* opened any of the files on the device, which is best practice.

Attackers sometimes conduct USB baiting attacks to deliver malicious code that they've crafted. However, this USB drive was still a security risk even though it did not contain malicious code. It could have easily been found by an attacker who might have used its contents to plan a variety of attacks.

Consider some of the risks associated with USB baiting 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?

In the **Risk analysis** row of the activity template, write **3 or 4 sentences** (60-80 words) describing any technical, operational, or managerial controls that could mitigate USB baiting attacks.

What to Include in Your Response

Be sure to address the following criteria in your completed activity:

- 2-3 sentences about the types of information stored on the USB drive
- 2-3 sentences about how the information could be used against the owner and/or organization
- 3-4 sentences analyzing the risks of USB baiting attacks