## **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?*   ***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. |
| **Attacker mindset** | 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.  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?* |
| **Risk analysis** | 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.  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?* |