# Activity Exemplar: Identify the attack vectors of a USB drive

Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity.

## Completed Exemplar

To review the exemplar for this course item, click the link and select *Use Template*.

Link to exemplar: Parking lot USB exercise

OR

If you don't have a Google account, you can download the exemplar directly from the following attachment.

**Parking lot USB exercise exemplar**
DOCX File

## Assessment of Exemplar

Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course.

***Note:*** *The exemplar represents one possible way to complete the activity. Yours will likely differ in certain ways. What's important is that your activity analyzes the types of information that can be found on a USB drive, how they can be exploited by a threat actor, and the types of attacks that can be hidden on these devices.*

The completed exemplar addresses the following criteria:

- 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

Next, review the exemplar components:

**Contents:** The contents of the USB drive contain files that appear to belong to a specific person. It contains a mixture of personal and business-related information that should not be stored in the same place.

**Attacker mindset:** Any information that an attacker obtains can be used against someone. Information on a USB drive should be encrypted regardless of whether it's personal or work-related.

**Risk analysis:** It's unsafe to plug an unfamiliar USB drive into your computer because of the wide range of attacks that can be hidden on them. Promoting employee awareness of USB baiting attacks is an operational control that can reduce the risks of a negative event. Routinely scanning for viruses is an example of an operational control that can be implemented. And disabling Autoplay on all PCs is a technical precaution that can be taken.

**Mark as completed**

**Like** **Dislike** **Report an issue**