

Classify the assets connected to a home network.

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

One of the most valuable assets in the world today is information. Most information is accessed over a network. There tend to be a variety of devices connected to a network and each is a potential entry point to other assets.

An inventory of network devices can be a useful asset management tool. An inventory can highlight sensitive assets that require extra protection.



You're operating a small business from your home and must create an inventory of your network devices. This will help you determine which ones contain sensitive information that require extra protection.

To do this, you will start by identifying three devices that have access to your home network. This might include devices such as:

- Desktop or laptop computers
- Smartphones
- Smart home devices
- Game consoles
- Storage devices or servers
- Video streaming devices

Then, you'll list important characteristics of each device such as its owner, location, and type. Finally, you will assign each device a level of sensitivity based on how important it is to protect.

	Asset	Network access	Owner		Location	Notes	Sensitivity
1	Network router	Continuous	Internet service provider (ISP)		On-premises	Has a 2.4 GHz and 5 GHz connection. All devices on the home network connect to the 5 GHz frequency.	Confidential
2	Desktop	Occasional	Homeowner		On-premises	Contains private information, like photos.	Restricted
3	Guest smartphone	Occasional	Friend		On and off-premises	Connects to my home network.	Internal-only
4	External hard drive	Occasional	Homeowner		On-premises	Contains music and movies.	Confidential
5	Streaming media player	Continuous	Homeowner		On-premises	Payment card information is stored for movie rentals.	Internal-only
6	Portable game console	Occasional	Friend		On and off-premises	Has a camera and microphone.	Internal-only