# Cybersecurity

## Project 1.2.5: It’s a Trap

Copy and paste screenshots and/or answer questions from the activity.

#8 **Plan of Action**

1. Firewall Rules: *How will you disable Windows file sharing? Are there other services/ports you need to disable?*
2. Suspicious files: *How can you identify suspicious files?*
3. Downloaded files: *How will you know where to look for files downloaded from the internet?*
4. Lost/deleted user files: *Where will you find your friend’s “deleted” files?*
5. Suspicious processes:*How will you determine suspicious processes and what will you do with them?*

#11 **Implement Your Plan of Action**

* Thoroughly document how you found and how you fixed each problem. Take screenshots for each of the step of your action plan (a through e) to help you explain what you did. Another team should be able to read your notes and perform the same tasks you did to secure the computer. **(BETTER TO HAVE TOO MUCH THAN TOO LITTLE)**
* Next to each “fix” that you documented, note which Cybersecurity Lifecycle activity you performed. Some fixes or tasks may fall into more than one category.

#13 **Present**

* Be engaging and appealing and something you would use to educate your classmates or workmates.
* Use a format such as a checklist, a “How-to”, or “helpful hints” so that other teams can use it to help them collaborate.
* Describe the protection measure you addressed when fixing each problem or weakness.

#16 **Reflect**

1. Describe what each team member contributed.
2. Describe how the diverse composition of your team helped with problem-solving.
3. Describe one moment during teamwork when your team:
   1. Worked well together.
   2. Could improve on collaboration.