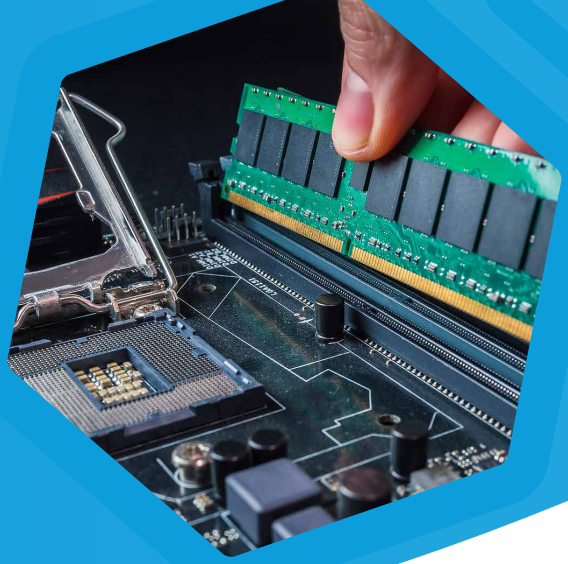

IT Fundamentals

Unit - Hardware

Lesson 1.6.1 Troubleshooting Methodology

Cyber Connections
- Hardware & Software

IT Fundamentals Objectives (FC0-U61)

Objective 1.6 - Explain the troubleshooting methodology

- Identify the problem:
    - Gather information; Duplicate the problem, if possible; Question users; Identify symptoms; Determine if anything has changed; Approach multiple problems individually
- Research knowledge base/Internet, if applicable
- Establish a theory of probable cause
    - Question the obvious
    - Consider multiple approaches
        - Divide and conquer
- Test the theory to determine the cause
    - Once the theory is confirmed (confirmed root cause), determine the next steps to resolve the problem; If the theory is not confirmed, establish a new theory or escalate
- Establish a plan of action to resolve the problem and identify potential effects
- Implement the solution or escalate as necessary
- Verify full system functionality and, if applicable, implement preventive measures
- Document findings/lessons learned, actions, and outcomes

Grade Level(s)

8, 9

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Teacher Notes:

Troubleshooting Methodology

What seems to be the problem?

Computers, like any time of machine, breakdown. With a computer, issues can be related to hardware, software, or a combination of the two. Whenever an issue occurs, there should be a step-by-step troubleshooting method implemented to identify, correct, and prevent the issue(s).

The first troubleshooting step should be a rather obvious one, identify the problem. If the problem is a large one, break it down into smaller problems. Afterwards, we'll need to consider who or what is/was affected? If the issue affected multiple users, we can view their logs to gather as many details as possible regarding the issue. After gathering this information, we can determine if anything has changed and attempt to duplicate the problem.

After identifying the problem, the next step requires research. We well want to look at previous help desk tickets in case the issue has happened before (that way we know how to quickly and correctly resolve the problem). Along with help desk tickets, utilize resources such as private or public knowledge bases and the Internet. Common problems may be discussed on online forums and should be considered.

After researching the issue, we need to establish a theory of probable cause. The more things we can eliminate as potential causes, the better, so look for simple and obvious causes first. After eliminating these potential causes, consider factors that could indirectly cause problems. For example, a power issue could simply be an issue with the Power Supply, the outlet, or a breaker, however, it could also be more complex problem like an issue with one of the tracks on the motherboard.

Now that a theory of probable cause has been established, we'll want to test that theory (just like testing a hypothesis in Chemistry). We'll want to only change and test one potential solution at a time (think of controls and variables, like in, I don't know, Chemistry?). After testing our potential solutions, we should be able to determine the root cause of the issue. If necessary, escalate the issue to a professional.

Teacher Notes:

Since the root cause of the problem has been found, we will want to establish an action plan by preparing a specific method for implementing the solution. If possible, test the solution in a sandbox first. If, when we implement the solution, there is a possibility of affecting other users, we need to notify them. Because there is always a possibility of damage/corruption, back up configurations and data first.

Once the solution has been implemented, we can't assume everything is fine and "back to normal". We need to verify functionality by first ensuring the solution has in fact solved the original problem without introducing new problems. After we have verified this, preventative measures will need to be applied if possible. To ensure the same issue can be resolved quickly and accurately in the future, document the solution and steps taken in the solution.