Troubleshooting Methodology

Troubleshooting is a critical skill for IT professionals. When working in different technology departments you can experience different issues. A large part of helpdesk is having the ability to diagnose and solve computer and network-related issues. CompTIA provides a framework that guides us toward finding the answers we need. The CompTIA trouble shooting methodology consists of six steps to help solve problems.

The first step is identifying the problem. It's important to recognize that the root cause of specific issues is not always apparent. For example, a failed login attempt might seem to indicate a username or password problem, when instead the real issue may be a lack of network connectivity that prevents the authentication information from being checked against a remote server. The goal of this step is to gather more information and learn about the symptoms the user may be experiencing.

The second step is to establish a theory of probable cause. This stage may require significant research. Vendor documentation, your organization's own documentation or a Google search may all be required to provide the basis for your theory. It's best to start with the simplest solution and escalate up. The third step is testing the theory. This will let you know if the problem can be solved or if you should continue researching the problem.

The fourth step is to establish a plan of action and to implement a solution. You need to plan because some solutions may require reboots or other more significant forms of downtime. For example, downloading software, patches, drivers, or entire operating system files before proceeding. Your change management procedures may require you to test modifications to a system's configuration in a staging environment before implementing the fix in production. After these things have been done you can implement a solution. This methodology ensures business continuity.

The fifth step is to verify full system functionality and implement preventive measures. When possible, have the users that rely on the system test functionality for you. They are the ones that really know how the system is supposed to act and they can ensure that it responds to their specific requirements. Depending on the problem, you may need to apply the fix to multiple servers or other devices. For example, if you've discovered a problem with a device driver on a server, you may need to update the drivers on several servers that rely on the same device.

The sixth step is to document findings. Documenting troubleshooting steps, changes, updates, theories, and research could all be useful in the future when a similar problem arises (or when the same problem turns out not to have been fixed after all). Another reason to keep good documentation as you go through the entire methodology is to communicate to others what you have tried so far. Such documentation is also useful in case the changes made had unintended consequences. It's easier to reverse changes or change configurations if you have good documentation on exactly what you did.

Common Helpdesk Issues and Solutions

1. User cannot log in
    a. Make sure the employee isn't trying to enter a password with caps lock turned on. Also, check to see if the password has expired, or the account is suspended due to

inactivity. Send the employee a password reset link. Other solutions can involve establishing a self-service password reset portal or adopting password management software in your organization.

2. Computer is too slow
    a. Assess the user’s CPU usage to determine if they have too many apps running at once – especially if these use up a lot of memory. Remove any temporary files from the Windows folder with the user’s permission and delete any large unused programs and files taking up space on their hard disk drive. Also, check that the user does not have viruses or malware on their machine.
3. Printer issues
    a. Identify the specific issue. Get the user to check the printer is turned on and that the printer is showing up for them to print to. They may need to add a specific network printer in their settings. For other issues such as paper jams, talk them through the instructions from the manufacturer relevant to the specific machine.
4. Computer Virus
    a. This machine needs to be isolated from your network immediately so that it doesn’t impact the company more widely. The next steps will depend on the actual virus that is on the machine and what is needed to remove it.
5. Blue Screen of Death
    a. This indicates a system crash. Often the issue is caused by either the hardware or one of the computer’s drivers. Sometimes all it needs is a quick reboot. If this fails, you may need to get the user to disconnect any unnecessary hardware to eliminate external causes. Also, attempt to boot the machine in safe mode. Other solutions include checking the hard drive for bad sectors and installing any necessary updates.