**Assessment task: 1**

**Outcomes covered 1–4**

**Sample report**

**Organisation:** Coatbank College

**Technician:** Barry Soap

**Date:** 02 May 2012

**Introduction**

Help Desk Trouble Ticket #190347 was submitted at 9:30 am on 01 May 2012 by Mr Arthur Bunyuck (abunyuck), an Accounts Technician in the Accounting Department and was allocated to me at 10:30 am the same day.

Mr Bunyuck reported that when he opened his browser it took him to a site named *Conduit,* rather than his usual home page. He did not know how this had happenedand had no idea how to fix it.

I decided that I would attempt to resolve the problem in a systematic manner by applying the recommended Six-Step Troubleshooting Methodology, ie:

* Identify the problem — question user and identify user changes to computer, and perform backups before making changes
* Establish a theory of probable cause (question the obvious)
* Test the theory to determine cause — once theory is confirmed, determine next steps to resolve problem — if theory is not confirmed, re-establish new theory or escalate
* Establish a plan of action to resolve the problem and implement the solution
* Verify full system functionality and if applicable implement preventative measures
* Document findings, actions, and outcomes

**Investigation**

My first step was to contact Mr Bunyuck to determine a suitable time to meet with him and discuss the problem. He agreed to meet with me in his office at 2:30 pm that day. He was able to demonstrate the problem to me: when he started the browser it opened in the Conduit Search Engine, rather than the college home page, as it did normally. He also pointed out that a new Conduit Taskbar had been installed.

A quick online search revealed that the Conduit Taskbar is a well-known adware application, often installed as a drive-by download when installing other software. I asked Mr Bunyuck if he had installed any new software recently, but he said that he couldn’t recall doing so.



|  |  |
| --- | --- |
| Scottish Qualifications Authority | 4 |
| HN Assessment Exemplar/H177 34/AEX001 V1.0 |  |
| Troubleshooting Computing Problems | **October 2012** |

I then examined the software installed on his machine. It was all standard-issue software, with one glaring exception, a well-known file-sharing client. When I enquired about this he admitted that he had installed it some time ago to allow him to download videos.

Another online search revealed numerous comments from users of the file-sharing client referring to the fact that a recent automatic upload had installed the Conduit Taskbar and reset the default home page.

This looked like the probable source of the problem, so I came to the conclusion that the most appropriate solution would be to reset the home page in the browser options and uninstall the Conduit Taskbar.

I pointed out to Mr Bunyuck that installing the file-sharing client on his machine was a breach of college policy and that I would need to uninstall it as well.

Before proceeding any further, I took a backup of all the data on the machine and created a system restore point, so that the system could be restored to its current status if necessary.

**Planning and implementing the solution**

I decided that the best approach to resolving the problem would be as follows:

1. Reset the Home Page to the college home page using **Tools/Options/General** in the browser menu.
2. Uninstall the Taskbar and the file-sharing client using the Uninstall a Program option in Control Panel.

No additional resources were required to carry out these steps, so I completed them and rebooted the machine.

However, when I started the browser it failed to load the correct home page, and eventually reported a timeout trying to access it. Initially I thought that the college home page might be down, but I was able to access it successfully from another machine, so this obviously wasn’t the case.

Several of the sites I had looked at earlier had mentioned that the Conduit Taskbar could be difficult to remove, so it looked as if there might still be traces of it around. After obtaining permission from my supervisor, I downloaded a malware removal tool and installed it on Mr Bunyuck’s machine.

When I ran the malware removal tool it reported that it was unable to open the *Hosts* file and found this suspicious. (The *Hosts* file contains hand-coded IP addresses for frequently-visited sites, allowing these sites to be accessed without the need for a DNS lookup.)



|  |  |
| --- | --- |
| Scottish Qualifications Authority | 5 |
| HN Assessment Exemplar/H177 34/AEX001 V1.0 |  |
| Troubleshooting Computing Problems | **October 2012** |

I opened a text editor using ‘Run as administrator’ and was able to open the *Hosts* file using this. It turned out to contain an incorrect entry for the college home page, so I deleted this and saved the file.

I again rebooted the machine. On opening the browser it loaded the college home page successfully and there was no sign of the Conduit Taskbar, so it appeared that the problem had now been resolved correctly.

At this stage I completed the Technician Response section of the Help Desk Trouble Ticket.

**Review and evaluation**

In general the troubleshooting process worked effectively. If more detailed research had been undertaken it may have been apparent that the initial steps taken would not be sufficient to solve the problem, but this was soon rectified.

Full details of the problem, and the steps taken to resolve it should be circulated to all technicians. All staff should be reminded of the college policy on unauthorised downloads. All machines should be checked for these at the next scheduled maintenance session.

**Note** —An alternative version of this sample answer in blog format can be found at:

<http://h17734.wordpress.com/>