Fault Finding & Solutions

Units 12 & 13, Assignment 2

Thomas Robinson
rob21005043

7th March 2023
Solihull College

Contents

1 Problems & Resolutions **2**
1.1 No Internet Connection . . . 2
1.2 Antivirus . . . 3
1.3 Beep Code . . . 4
1.4 Printing . . . 5

2 Information Sources **6**
2.1 Logs & Error Messages . . . 6
2.2 Manufacturer/Developer Resources . . . 6
2.3 Company Policy & Procedure . . . 6
2.4 Company/Personal Knowledge Base . . . 6
2.5 Forums & Q&A Sites . . . 7
2.6 Websites & Articles . . . 7

3 Maintaining Data Security & Integrity **8**
3.1 Methods to Maintain Data Integrity . . . 8
3.2 Methods to Maintain Data Security . . . 8

4 Responding to Users **9**
4.1 Mind Map . . . 9
4.2 Responding via Chat/Forum . . . 10
4.3 Walk Through of a Solution . . . 11

1 Problems & Resolutions

1.1 No Internet Connection

"The computer loads up but when opening the web browser, no websites load, and you cannot connect to local network servers."

Type of Fault This could either be a hardware issue or a software misconfiguration.

Software Reasons Connecting to a network requires many parameters to be set correctly. Often this is handled automatically using DHCP, but they can be configured manually. Examples of misconfigured network settings could be assigning the computer an IP address that is already used or an address that is outside the range of the subnet it is connected to.

Hardware Reasons There could be many causes for a hardware issue. If the computer is connected with an Ethernet cable, it could be damaged or unplugged. Similarly, the computer's NIC could also be damaged. If the computer is connected wirelessly, it may be out of range of an access point or the wireless adapter in the computer could be damaged.

Finding Advice & Guidance

- Diagnostic logs and messages can provide detailed information about errors and issues
- Guides and help resources from the Operating System can provide information about how to configure network settings correctly. An example of such would be Microsoft's Windows support articles[1].
- Online forums are a place where you may be able to find people with similar issues or pose a question to a broad community.
- An organization's knowledge base or internal procedures may provide insights into how similar issues were solved in the past.
- Other people, such as experienced co-workers can also be useful sources.
- Issues with hardware may be outlined in instruction manuals or by using manufacturer support resources.
- Artificial Intelligence chatbots—like ChatGPT and Bing AI—are useful at summarizing information and troubleshooting steps.

Fault Remedies There are multiple possible reasons for the loss of network connectivity.

To check the issue, one could use a different computer or device to see if the connectivity issues are exclusive to the computer. If this is the case, it is known that the computer is the most likely source of the problem. This will determine if there is an issue with the network infrastructure, such as router or switch failure.

[1] support.Microsoft.com

Assuming the issue is with the software configuration, this would need to be rectified to remedy the fault. As an example, if a static IP address was assigned that conflicted with another device on the network, this should be changed, or DHCP enabled to automatically fetch an address if that is desired.

Tool Comparison Using the example above, the best tool would be the internal company documentation or knowledge base. These should describe what the correct network settings are for the computer in question, as well as providing additional insights into any past occurrences of the problem.

Operating System information would describe where to go to change the settings and how to change them, but would not say what to modify in order to rectify the problem.

Fault logs can be used to pinpoint other software issues, such as an invalid configuration. These would be an appropriate place to start if there is no obvious issue.

Assuming an issue with hardware, it would be best to use the manufacturer's resources to solve the problem since they will be most knowledgeable about the product and will be able to provide fixes and replacements should the product be broken.

1.2 Antivirus

"A message from the antivirus software has popped up on the screen saying the computer is infected."

Type of Fault This is a software issue likely caused by the presence of malware on the computer. This could've been installed by downloading an infected program, through an exploit in a piece of software or by other attack vectors.

Software Reasons An exploit in the computer's operating system or an installed program may have provided an entry point for the malware. Human error, such as succumbing to a social engineering attack and explicitly installing a malicious program could be another reason for the presence of an infection.

It is also possible that the Antivirus has produced a false-positive report and has flagged a legitimate program or file. This is common when using tools that are often installed unknowingly, such as cryptocurrency miners.

Hardware Reasons Plugging in unknown devices can be an attack vector for malware. This is a possible hardware-related cause of the infection.

Finding Advice & Guidance

- The antivirus software will say what it detected and may list probable solutions that can be taken
- Company policy may dictate procedures to take upon learning of an infection. These could include isolating the machine and resetting it.

Fault Remedies Choosing to follow the guidance of the Antivirus software may include quarantining or removing the offending programs/files. The software will provide the location of these and may include built-in tools for secure deletion. This is true of most popular antivirus software solutions, such as Windows Defender, Malwarebytes, or Bitdefender.

Tool Comparison Removing the detected files with the antivirus software would remedy the problem, but it may fail to remove all files left behind by the infection. For example, if the infection is a virus, it may have injected malicious code into other programs which may go undetected.

Wiping the device and reinstalling the operating system of the device would remove all user data that has not been backed up elsewhere, which may not be ideal. This solution, however, will ensure that any malicious software installed on the device's storage medium is removed.

1.3 Beep Code

"The computer starts but one long continuous beep code is given."

Type of Fault Issues with the boot process accompanied by a beep code indicate an issue with the hardware or software configuration of the computer. This beep code is generated by speaker on (or attached to) the motherboard.

Hardware Reasons A multitude of issues could be the cause of the beep code. These range from unsupported hardware being installed—for example a newer CPU than the motherboard firmware supports—to a fan being unplugged.

Software Reasons There may be an issue with the firmware of the motherboard, preventing the system from starting. This could be due to corrupt firmware or an invalid configuration setting by the user.

Finding Advice & Guidance

- Checking the motherboard instruction manual will provide a list of the beep codes and potential troubleshooting steps
- Online forums and discussion platforms may provide insights and experiences that are not given by the motherboard manufacturer

Fault Remedies A solution would be to decode the beep code by using the motherboard's documentation. This will explain the problem and may provide steps that need to be taken to resolve it. For example, if the CPU is incompatible, it will need to be swapped for one that is supported.

Tool Comparison Using the motherboard's guidance will describe the problem, however it may not go into depth on how to resolve it. Online discussions could provide other users' experience and more in-depth knowledge. They also provide a place to ask questions to a wide audience for assistance.

1.4 Printing

"The user is unable to print out documents to the local printer plugged in to the system."

Type of Fault This could be a problem with either the printer or the computer it is attached to. These could take the form of either software or hardware. There is no single, simple solution and additional troubleshooting is required.

Software Reasons The printer may be unable to print documents due to a software misconfiguration, such as a lack of appropriate drivers or an incorrect setting.

Hardware Reasons The printer may be turned off, broken, or unplugged.

Finding Advice & Guidance

- The printer manufacturer's help resources—e.g: Epson.com/support.
- Operating System help resources—e.g: support.Microsoft.com

Fault Remedies Assuming there is an issue with the printer drivers, one should uninstall any previous versions before following the manufacturer's instructions for downloading and installing the appropriate drivers.

Tool Comparison The most useful resource will depend on the location of the problem. If the printer itself is at fault, or there is an issue with manufacturer software or drivers, the manufacturer's help resources may provide troubleshooting steps and additional information that could contribute to solving the problem. If there is an issue with drivers or the Operating System configuration, its documentation may also prove useful.

2 Information Sources

2.1 Logs & Error Messages

Fault logs, error messages and other diagnostic resources can be instrumental in diagnosing the root cause of a fault. Examples of useful logs include the Windows Event Viewer, logs in Syslog (Linux), or general program logs. These each could contain technical error information that can be used to diagnose a problem.

These tools are a useful resource for diagnosing a problem and figuring out which area of the software or hardware it pertains to. This is as much as they are able to do, however; they cannot rectify the problem themselves or provide instructions on how to rectify it.

2.2 Manufacturer/Developer Resources

Resources created by the manufacturer of a hardware device or the developers of a piece of software can be useful in diagnosing specific errors or gaining a better understanding of how the piece of hardware or software functions.

Guides and instruction manuals may include a troubleshooting section for frequently encountered problems, which could also have steps to resolve the issues.

These resources will only cover specific, targeted problems and if the issue is not covered, they will not be useful.

Offline resources, such as manuals, may become out of date but are accessible even in the event of an internet outage. Online resources, such as support centres and digital copies of manuals, can be kept up to date and are easily searchable.

2.3 Company Policy & Procedure

A company may have specific policies and procedures in place for common faults. This ensures a consistent application of technical support and ensures that one can skip the troubleshooting step once a problem has been diagnosed. If something is outside the scope of the policies or is not documented as a procedure, then other methods must be used to solve the problem.

2.4 Company/Personal Knowledge Base

Knowledge bases are a collection of information that is useful to a company or individual. This could be a collection of troubleshooting steps for common problems, or a list of common faults and their solutions. These notes can be useful for solving problems that are not covered by the manufacturer's documentation, without having to resort to other resources.

2.5 Forums & Q&A Sites

Forums—such as Reddit[2] and LinusTechTips[3]—and Q&A sites—like StackOverflow[4] and StackExchange[5]—are websites where users can ask questions and receive answers from other users. They are frequented by people with a wide range of knowledge and experience, and can be a useful resource for finding solutions to problems that are difficult to diagnose or are unique to a specific situation.

2.6 Websites & Articles

Online sources, like blog posts and articles, often appear in search results when searching for a solution to a problem. These can be useful for finding a solution to a problem, but they may not be as reliable as other sources. They may be outdated, or the information may be incorrect. They may also be written in a way that is difficult to understand, or may not be specific to the problem at hand. Their varying quality makes them difficult to rely on, though they can be useful for finding a starting point for troubleshooting.

[2] Subreddits such as reddit.com/r/Networking provide a space for discussion about specific topics

[3] The LTT forums have a networking and tech support section: LinusTechTips.com/forum/45-networking

[4] StackOverflow.com is for programming questions

[5] StackExchange is a network of Q&A forums for different topics, for example NetworkEngineering.StackExchange.com is for computer networking questions

3 Maintaining Data Security & Integrity

As an IT professional, it is important to be aware of the risks that could be posed to data and how to mitigate them. This is especially important when working with sensitive data, such as personal information or financial data.

Data Integrity is the accuracy and consistency of data. File corruption, data loss, and data modification are all examples of data integrity issues.

Data Security is the protection of data from unauthorized access, modification, or deletion.

3.1 Methods to Maintain Data Integrity

Backups Backing up data is a method of ensuring data integrity. In the event of a problem, lost data can be restored from a backup. For example, before working on a computer, one could make a backup of the hard drive. If the computer is damaged further during the troubleshooting or repair process, the data can be restored from the backup.

Recovery Procedures A recovery procedure is a set of steps that can be followed to restore a system to a previous state. For example, if a computer is infected with a virus, one could follow the recovery procedure to restore the computer to a previous state before it was infected. This may involve restoring the computer from a backup, or reinstalling the Operating System.

3.2 Methods to Maintain Data Security

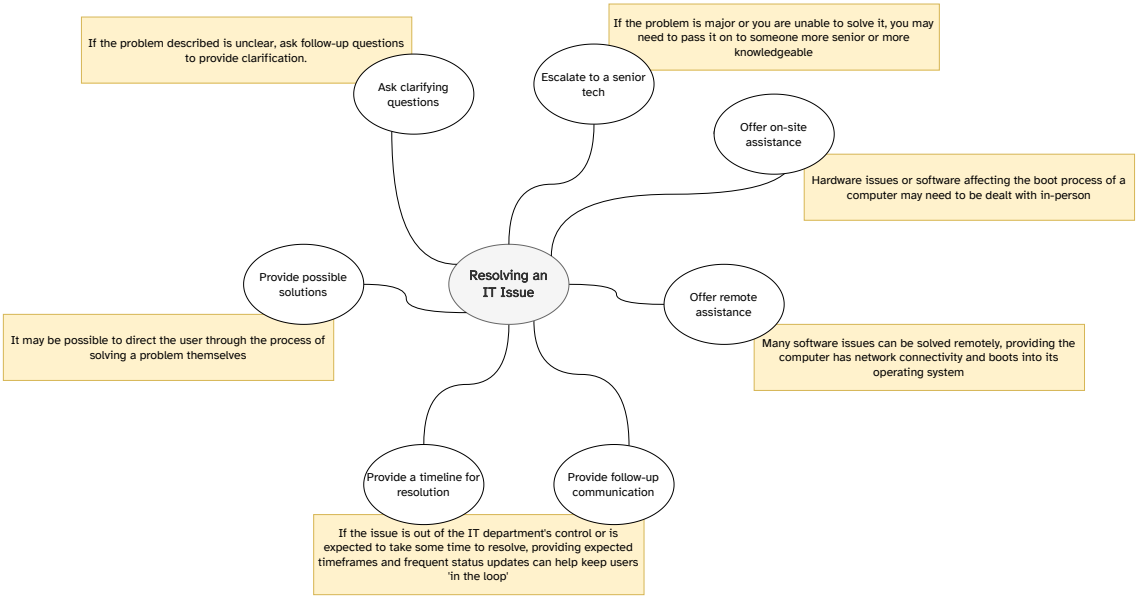
User Access Rights User access rights are a method of maintaining data security. They can be used to restrict access to certain files or folders. For example, a user could be given read-only access to a file, so that they can view the contents of the file, but not modify it. Regularly ensuring that files, folders, and programs have appropriate access rights can help to maintain data security by preventing unauthorized access.

Physical Security It is important to be aware of the physical security of systems and their data. Awareness of social engineering attacks can also help to maintain data security. For example, when entering a building or restricted area to tend to an issue, one should be wary of anyone who may be 'piggybacking' and following them into the secure space. Another example would be ensuring that data is stored securely both at-rest and in-transit, such as by using encryption. This would prevent unauthorized access to the data if the device were to be stolen or compromised.

Virus Protection Using antivirus software can help to maintain data security. Malicious software can be used to steal, modify, or delete data. Antivirus solutions are able to detect and remove these threats. Regularly updating antivirus software can help to ensure that it is able to detect the latest threats. It is important to note that antivirus software is not a replacement for good security practices, such as using strong passwords and ensuring that secure access rights are set.

4 Responding to Users

4.1 Mind Map



4.2 Responding via Chat/Forum

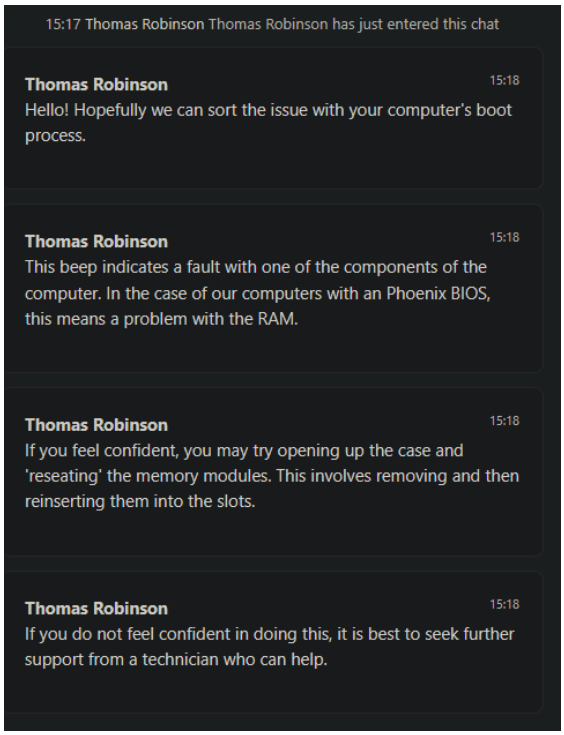


Figure 1:
In response to *"A PC starts to boot but one long continuous beep code is given."*

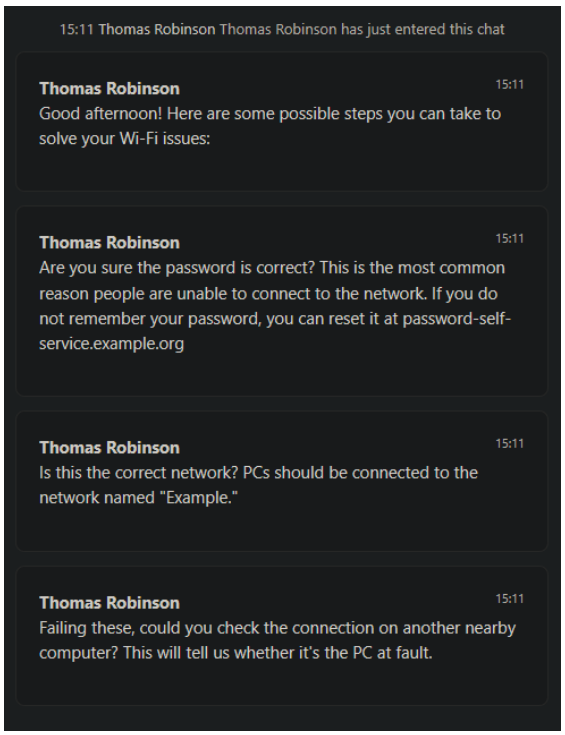


Figure 2:
In response to *"A PC will not connect to the Wi-Fi network."*

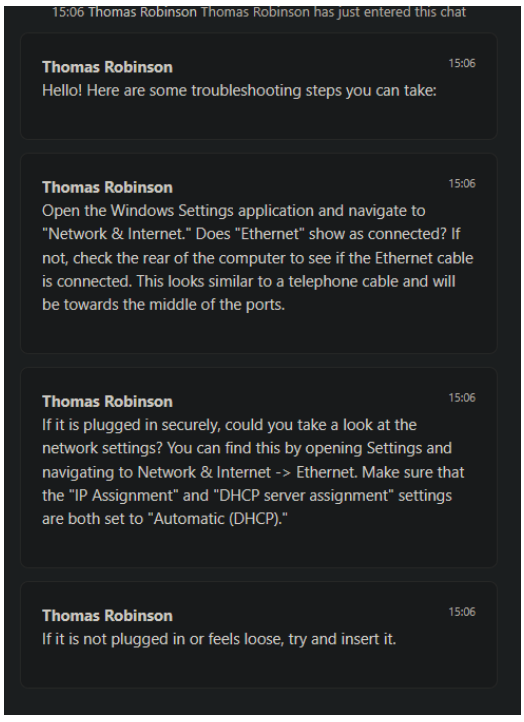
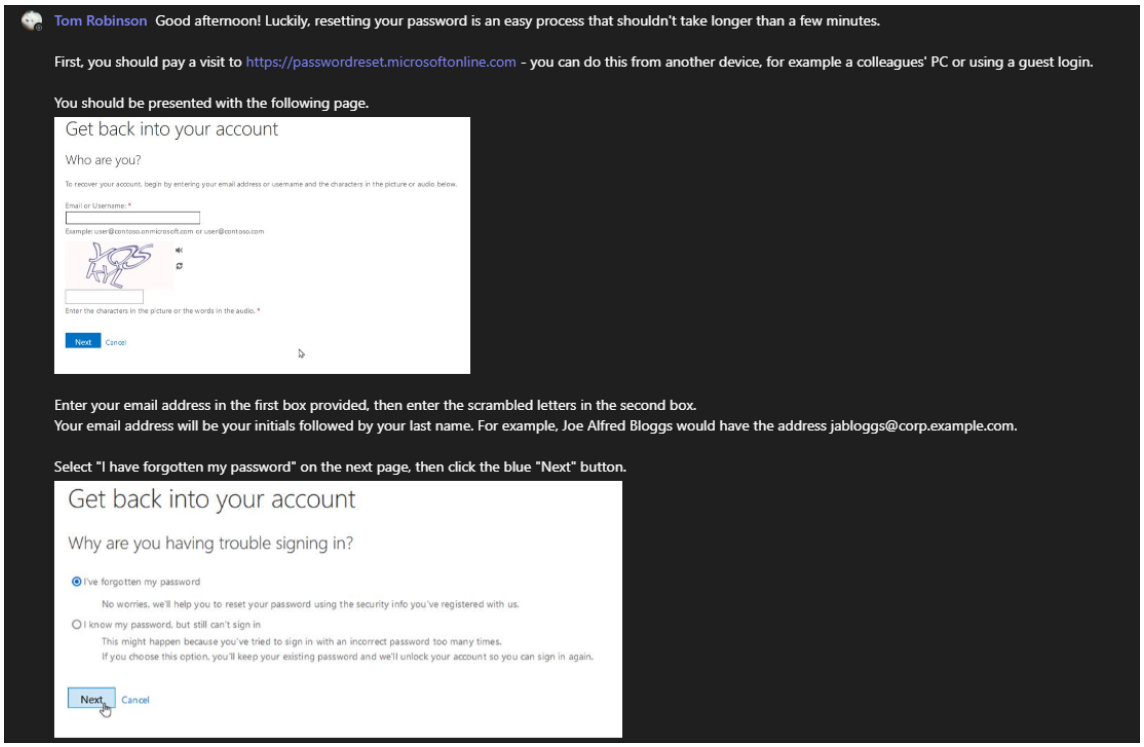
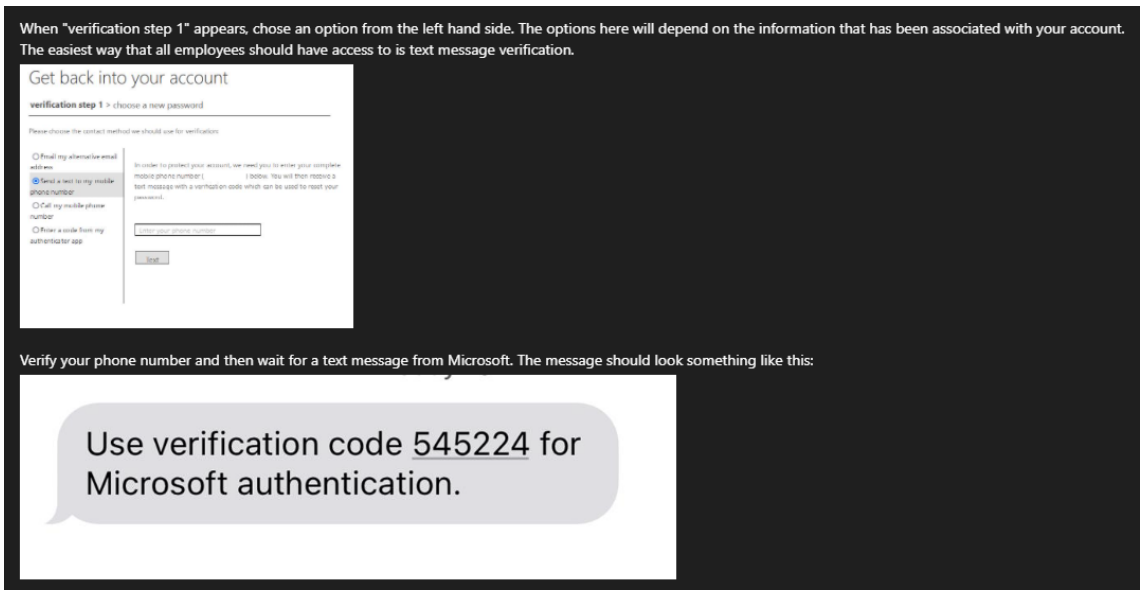


Figure 3:
In response to *"A classroom PC won't connect to the internet. The icon on the lower right of the taskbar shows the Windows 'no internet' icon."*

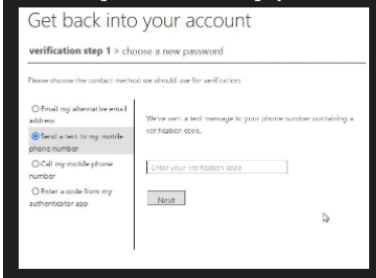
4.3 Walk Through of a Solution

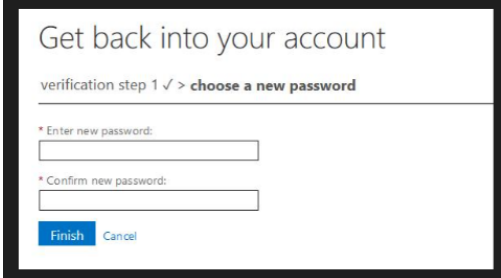
In this hypothetical scenario, an employee of Example.org has forgotten their password. This communication was sent using the Microsoft Teams application.





After entering the code in the message, you will be able to set a new password.





Note that new passwords must adhere to the password rules, laid out in the IT Acceptable Use Policy. For example, you may not reuse a password across multiple accounts.

If you are having difficulties with the process, please visit the IT helpdesk in-person with your employee ID badge and we can set a temporary password for you.
You will need to change this as soon as possible next time you log on to a system.