# ABOUT SOFTWARE

If hardware is the computer’s physical components, software is the set of instructions or programs that ‘run’ on a computer. There are two main categories of computer software:

**System software** is what is used to manage a computer, an example being the operating system which might be MacOS, WindowsOS or AndroidOS. If a device does not have an operating system installed, when switched on, the screen will be blank. System software allows users and hardware to interact with each other. This type of software is used to manage the behaviour of computer hardware in order to complete most of the basic and most of the complex tasks.

**Application software** is any programme that enables the user to complete tasks. Every programme that you use on your device is application software. Examples are Microsoft Word, Excel, internet browsers such as Google Chrome and Apple Safari, and video games. If a device did not have any application software installed, you wouldn’t be able to use it for anything other than pre-installed features which come together with an operating system.

Software can be copied from a CD or DVD, downloaded from the Internet onto a computer’s hard drive/USB drive, or accessed on demand via an internet connection to the Cloud. (see guidance [ABOUT THE CLOUD](https://getreadyforcyberessentials.iasme.co.uk/guidance/about-the-cloud/))

### ****PATCHING****

Software is made up of thousands of lines of code which is how the computer interprets information to complete its functions. In every 1000 lines of code there is on average 10-15 errors. Most of these errors are not noticeable to you as the user, however, each error is a potential opening for cyber criminals to access your data. These openings are often called ‘vulnerabilities’.

Within a piece of software’s functioning life span, as soon as an error or ‘vulnerability’ is discovered, the manufacturer creates some additional code to correct and close the opening. This is known as ‘patching’. All modern software will need to ‘update’ on a regular basis as part of its maintenance which ensures that vulnerabilities are patched within 14 days of the update, and other ‘bugs’ (faults) corrected.

### ****UNSUPPORTED SOFTWARE****

When software that is considered ‘end of life’ or no longer viable with modern technology, the manufacturer will cease to create patches. This means application becomes a ‘legacy software’ and is no longer supported and therefore no longer secure. Not only the vulnerabilities are left un-patched, but they become common knowledge for hackers, and therefore easy to exploit. It is a good idea to set your computer and other devices to auto-update, which means that patches are automatically applied when they are released.

### ****MANUFACTURER APPROVED SOFTWARE****

You should only use software that is from an official source that is approved by the manufacturer/vendor. This way, you can be confident that the thousands of lines of code are not designed to harm your device or data. Some examples of official sources include the Google Play store and the Apple app store. Software acquired from questionable sources may be counterfeit and unlicensed. Not only will it be of an inferior quality and unable to receive ongoing support, but there is also a high chance it will contain malware. (see guidance on [ABOUT MALWARE](https://getreadyforcyberessentials.iasme.co.uk/guidance/about-malware/))

### ****UNUSED SOFTWARE****

Many devices and software come from the manufacturer with many features enabled that you do not use. These are sometimes called ‘plugins’. The code in each ‘extra’ feature can potentially offer additional openings for cyber criminals to reach you. It is a good idea to permanently removed unused software by uninstalling it. (see guidance [HOW TO REMOVE UNNECESSARY SOFTWARE](https://getreadyforcyberessentials.iasme.co.uk/guidance/how-to-remove-unnecessary-software/))

### ****BEST PRACTICE TO MINIMISE YOUR COMPUTER’S EXPOSURE TO SOFTWARE VULNERABILITIES****

* Only use software that the manufacturer still supports with patches.
* Apply patches as soon as they are released.
* Remove any extra features that you do not use.