

Welcome to our Autumn Newsletter!

Windows 10 Updates...

Windows 10 is generally very good and an improvement over previous versions. However, Microsoft keep shooting themselves in the foot with their inability to produce reliable and easy to install updates. Their latest, the First Anniversary Update, has caused all sorts of problems, especially to people with small networks.

The update process on all versions of Windows 8 and 10 can lead you to think your PC is not booting up. You may get a blank screen with no obvious sign of activity when you switch the PC on. This can be caused by a Windows Update installing it's self on start up. If that happens, don't panic. Leave the PC for a few minutes – once the installation is complete Windows will restart. Whatever you do don't keep switching the PC on and off as it can corrupt the installation and end up damaging Windows.

One irritating feature is the 'Let Windows Manage my Default Printer' setting. This effectively changes your default printer to the last one you used. Not a problem if you only have one printer. However, if you have a label printer, for example, as well as a normal printer, every time you print a label the label printer will be set as the default printer. If you forget to set it back, next time you print a document it will be printed to the label printer, wasting loads of labels. You can switch this off in Settings/Devices/Printers.

Surplus Equipment...

We have been having a clear out of old PCs and monitors etc. and consequently have a number of items for sale. Obviously, these are all second hand and come with no warranty.

- Intel i3 PC with 4gb RAM Windows 7 - £75 or £100 with monitor and keyboard
- Intel Dual Core based PC with 4gb RAM with Windows 10 - £75 or £100 with monitor and keyboard
- A number of monitors of varying sizes with prices starting at £10
- A Creative Labs speaker set with a large subwoofer - £10
- Computer Desk with two drawers - £15
- Canon Pixma iP4950 with set of spare inks – barely used - £30
- HP LaserJet Printer - £25

Computer Security...

I am sorry that we keep repeating warnings about telephone and virus scams in our newsletters. However, as some clients continue to be caught out it seems wise to repeat them.

Computer security continues to be one of the biggest problems facing PC users worldwide. The spate of fraudsters phoning claiming to be from Microsoft, Windows Support, BT or Talk Talk etc. show no signs of abating. There have been several largescale prosecutions but as soon as one group are closed down another seems to start up.

We must all be very vigilant when answering the phone to someone claiming to know of a problem with your PC, phone line or Internet connection. Invariably, there is nothing actually wrong with your system and what they tell you is usually nonsense. They can be very convincing, however. Bear in mind they may quote a small, reasonable sounding fee but once they have got your credit card details they can charge whatever they want. One client was recently defrauded out of over £1,000 by a very genuine sounding telephone crook! Others have lost over £200.

Another common scam is caused by the Cryptolocker virus (or variant). This is usually attached to an email as an attachment. The message in the body of the email may refer to delivery of a parcel or an invoice for goods supplied. There are a variety of versions. Once you open the attachment your hard drive is encrypted, i.e. your documents, photos etc. are made inaccessible unless you pay the fraudsters for an un-encryption key.

If you are a company running a network with 'mapped' network drives, you should take particular care. Cryptolocker will encrypt mapped network drives as well as the local drive. If your 'mapped' drive links to your server then all your company documents are at risk. One local company lost all their documents, drawings, accounts information, personnel files etc. Fortunately, they had a recent backup so only lost a day's work. Others have not been as fortunate.

One of our business clients lost all their financial records, as well as important documents last month. They had no recent backup so were seriously affected. They had anti-virus software installed but because they opened the attachment they effectively gave the virus permission to run. We know of a number of local companies and individuals who have been similarly affected over the last year or so.

It is often hard to tell a false email from a genuine one. You need to read the text very carefully looking for clues. The most usual clue is poor English or grammar. Context is also very important. Why would someone like Fedex or the

Post Office contact you out of the blue about a parcel delivery or a company you have never heard of send you an invoice?

The usual rule is don't open any attachment from ANYONE (including friends) unless you are expecting it. Install a good anti-virus program – but don't rely on it. Remember, if you open an infected email attachment you are effectively giving the virus permission to run. Good discipline and a recent backup is the best protection. The free anti-virus programs are adequate but you really do get what you pay for when it comes to virus protection.

We continue to recommend Bullguard Internet Security, which won Which! magazine's best anti-virus package of the year award for the fourth year running