We were looking forward to an interesting talk by Kevin on the safe use of home computers. It was not to be. He was forced to cancel. With just two hours notice Chris took up the challenge and spoke about setting up a home network and the security implications of using it.

The population of computers is increasing due to the multiplicity of new uses for them and the falling cost of ownership.

More and more households have a second or third computer as well as other devices that can be attached to them. We are not just talking about printers and scanners here, but of Playstations and Wii devices; of televisions and DVD players for films; of music being piped into any room.

(Not to mention that fridges, freezers, central heating controls, external lighting and security cameras can be networked now – but let's stay with computers.)

The incentive to set up a home network is the economy and convenience of sharing. This can be the sharing of internet connections or attached devices such as printers or file storage.

Imagine sitting in the lounge with a laptop and sending instructions to a printer in another part of the house without having to connect the laptop to the printer with a lead or to transfer the file to the computer running the printer. Bliss.

In the same way you could have a special colour printer for high quality output (expensive) and a cheap black and white one for ordinary stuff – and select which to use by a click of a mouse.

The networking set-up is easy (isn't it always!) provided you follow the instructions in sequence.

A bit of reading up about it all is a good idea. (Type "home networking" into Google and have a browse around.)

Chris summarised the process for us with the help of slides (added to our website as an *aide memoire* for those who were there) and explained about IP addresses and how the devices communicate.

Your network can be all wireless; all cabled or a mixture to suit your needs. The machines do not have to be using the same operating system.

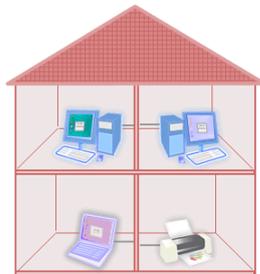Chris spent some time stressing the need to keep a network secure.

Be aware that the device in your home that connects to the Internet is your router, NOT your PC. If anyone can connect to your router they can download material in your name and without your knowing – until the law knocks on your door! There will be more about that another time.

Some facts of interest:

It took radio 38 years to reach 50 million people. It took television 13 years. The World Wide Web did it in 4 years.

Each device connected to the Internet needs its own unique number. About 4.5 BILLION was thought to be enough. It wasn't. The replacement system will allow thousands of numbers for every person on the planet.

There are over 1.3 billion people on the internet at any one time.

The next meeting will be on Tuesday 9th March. Ceri will be looking at features of Microsoft Office 2007. Visitors and new members always welcome. For more information ring Howard on 029 20708439.

In Brief

Computer Club

The next meeting will be on Tuesday 9th March to look at features of Microsoft Office 2007. Visitors and new members always welcome. For more information ring Howard on 029 20708439.