Penarth Computer Club Home Network Security 11th June 2010

Nobody goes on holiday locking all the windows and leaving the front door wide open. Chris made the comment during his talk on why and how to keep a home network secure.

Do you have a network? If you have several pieces of kit connected together, yes you do. If they are connected by cables, then there is little danger of intrusion providing your access to the internet is secure.

There are, however, many advantages to having a wireless network apart from fewer cables. You can use a laptop anywhere – even in the garden. Several computers can share one printer. Files can be shared without having to copy them to an intermediate device such as a CD or a flash drive.

But you must ensure security. Wireless transmissions can be picked up from the road outside your house just as easily as in your garden; after all, that is precisely what modern laptops are designed to do – pick up transmissions. It is vital that your signal cannot be used unless your access code is known.

The code is set by the original manufacturer. If it is a secure code it will be fine. If it is a standard default code it can be known to someone who wants to hi-jack your network. It is crazy not to change it and “leave the front door open”.

At this point Chris reminded everyone that all equipment carries a code hard-wired into it by the manufacturer to identify the equipment precisely to other pieces of equipment that need to ‘talk’ to it, including your internet access device. Your access will also have an internet address.

All this means it is possible to identify your network as the destination of any illegal downloads. It makes sense to protect your system to avoid being held responsible for an hacker’s illegal download.

Chris then gave several tips on how to keep things safe. Every system has an administrator who sets up standard accounts for other users.. An administrator might well set up a standard account for him/herself for normal use. In that case if anyone should access his/her standard account, they will not be able to interfere with other accounts or with the system.

Passwords should be strong. That means impossible to guess; not birthdays, house numbers, pet’s names etc. They should include capitals and lower case letters, numbers and unusual keyboard characters such as £$%&. They must also be memorable. Suggestions were the number plate of a first ever car; a line of a favourite poem or a family saying.

A final note: if the kit is not switched on it cannot be hacked. If it is not being used switch it off. Not several times a day, but over a weekend away or longer. It’s also “green”.

The next meeting will be on Tuesday 22nd June. An end-of-term social evening with Chips & Chat and a music quiz by Mike J. 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 22nd June. An end-of-term social evening with Chips & Chat and a music quiz by Mike J. Visitors and new members always welcome. For more information ring Howard on 029 20708439.