I worry about what my children might find on the internet.

Should I be worried?

The short answer is “yes”! A survey by ChildWise found 58% of children aged seven to ten have internet access in their bedrooms, compared to just 9% in 2004. Sentry (a leading provider of parental control software) claim that potentially 1 in 5 children could be sexually solicited online and only 18% of the most serious incidents are actually reported. Without taking precautions, your child could have access to: unmoderated social networking sites, unmoderated chatrooms, sites with persistent bad language, visual material of a sexual nature, horror content and extremely violent content.

Several of my customers have asked me about parental controls that protect their young children from the dark side of the internet. One has even had an embarrassing call from their child’s head teacher asking why she had allowed young children to access adult websites.

One simple answer is - parental control software

What is parental control software?

Software solutions range from basic key-word-blocking to intelligent-monitoring. Key word blocking stops your child typing ‘suspect’ words. Some more complex systems maintain up-to-date databases of unsuitable websites and prevent your child accessing any of them. The most intelligent monitoring systems actually route your internet thought their computers so they can check everything that goes back and forwards, this process is called a ’proxy server’ – You can even receive an e-mail report if your child has tried to access anything inappropriate.

How can I get it?

There are a huge range of solutions readily available. “K9” is very basic system that is a free download, some versions Windows provide enhanced security options, Sentry Parental Controls software has been rated 4 stars on Amazon and other internet security packages such as Kaspersky and Norton offer their own versions – see their websites for details.

Some internet providers also offer protection: TalkTalk is to offer a filter called “HomeSafe” and BT offers “BT family Protection”. Virgin and Sky also have options.

Does it work?

The simple answer is - to a degree: however a lot of children are more PC literate than their parents, so using a simple system can easily be bypassed. Just type in “parental control software” into Google and you will see a multitude of options on offer. Then type in “how to bypass parental control software” and you will be presented with just as many options. So you might spend too much time and money downloading and configuring parental control software only to find that your bright little angel will be able to de-activate it in 5 minutes!

What about Mobile phones?

Most mobile phones can now access the internet, and technology is moving fast, parental control software struggles to keep up. Most mobile phone service providers offer free parental control services which limit the content children can access via the mobile network to items suitable for under 18s. However, they may not always be automatically switched on so be sure to check with you mobile phone provider. Kaspersky has announced "*Kaspersky Parental Control"* which provides a set of tools to prohibit children from visiting unsuitable or potentially harmful websites on Android phones.

Personal photos and videos from your child's mobile phone can easily fall into the wrong hands. Unless your child understands to risk of sharing this type of content, embarrassing or inappropriate photos or videos could easily be passed between phones and put online. Once sent or put online, control over the images is lost and they could end up in the hands of strangers. Photos or videos may also be used to fuel bullying or harassment. Visit the www.thinkuknow.co.uk website for more information and advice on this.

Chatrooms are popular with youngsters and while mobile providers' own chatrooms aimed at children may be moderated, others might not be. Visit the www.Chatdanger.com website for more information and advice on this.

If your child has a profile on a social networking site like Facebook they may access it on their mobile phone. Ensure they know why it is important to allow their personal information only to be shared with people they know in the real world.

Reporting inappropriate material

Research by Ofcom has found that 25% of children and young people say that they're uncertain about what they would do if they came across inappropriate material on their mobile phone. So you could offer to help by encouraging your children to tell you about anything they have seen or heard that has made them feel uncomfortable or scared. You can report incidents to their mobile network operator and in instances of sexual contact to the Child Exploitation and Online Protection Centre (CEOP) at ceop.police.uk using their report abuse button.

So what do I do?

As with all parenting decisions there is never just one answer. Clearly you cannot prevent a determined child from accessing anything on the internet, but you can make it very clear what is acceptable and what is not. Setting up some reasonable parental control software gives a clear message and some control.

One option I would recommend is to explain to your child that you are installing this software to protect them; this will give you a good forum to discuss the things that you will allow or not allow. If you use a system that gives you feedback on their activities, you can also agree that you will remove this after a certain time.

If you want any advice contact Bills-IT – or any other reputable computer technician.