**Internet safety**

The first thing you can do to make the internet a safer place for your children is to set aside a small amount of time to learn how it works and what you can do to control what content is available to view. The basics are not difficult and most answers to questions are already on Google, just do a search. Take time to talk with all your family regularly, discussing concerns and potential problems with online material. We as parents are generally not as ‘tech savvy’ as our children and one of the reasons is fear. That fear is the fear we will mess something up. Children do not have that fear of technology because for one, they will not have to fix the problem. Two, they won’t have to pay for it; three, they have not got the life experience to know how their experimenting with technology will affect themselves and others. They also communicate and work with other children extremely well in order to overcome a computer or internet problem. The levels at which they will do this can be amazing. They will also share this information extremely well with others. As adults we could learn a lot from our children and share internet safety advice we have learned with other parents. Teach your children about internet safety and don’t be afraid to learn from them too.

**Internet controls**

You can install controls to try and limit the harmful material that can be stumbled across, often, quite easily and by accident. Below is a link to a website that will allow you to easily set up parental controls on almost all equipment in your home that connects to the internet.

It will take a little time to go through all of it but you don’t have to do it all on the same day. I suggest dedicating a period of time, say 30 minutes, grab a tea or coffee and take a look. Stay focused and complete one section at a time. Also, get a notepad and write down passwords and usernames in a clear and logical manner for later reference.

<http://parentalcontrols-on.org/>

When you click on the link it gives descriptions of the types of material you may wish to restrict. If you click on “protect my family” a picture of a house with five sections appears. The top section deals with parental controls for internet providers. Click on yours if it’s there and scroll down to see screenshots of how to set up parental controls. If yours is not there, check your provider’s website for help with this. When you are done click “HOME” to return to the start page. The next section on the left deals with tablets and mobile phones, just click on “Apple or Android” and scroll down to set controls. The section on the right deals with controls on things like ‘I Player’, ‘You Tube’ and ‘Netflix’. Click on the ones relevant to you and apply parental controls as instructed.

The section on the bottom left deals with controls on gaming devices. Pick the ones relevant to you and apply controls as instructed. The section to the right deals with mobile networks and blocking inappropriate content. Click on your provider and read how to activate the controls for your children’s phones.

**Check out your router**

If you are feeling a bit more adventurous you may wish to look at your router logs to see when people in your house are logging onto and off your WIFI. As this is different for different internet providers and routers, just search on Google, You Tube or your internet provider’s website as to how to do this. Usually access is through something like

<http://198.61.1.1> typed into your address bar. Below are some popular router access addresses:

BT Home hub access **192.168.1.254**.

Virgin router access [http://192.168.0.1](http://192.168.0.1/)

Talk Talk router access <http://198.61.1.1>

Sky router access 192.168.0.1

You will need your default username and password to enter your routers settings. You may want to change the router username and password once you have accessed it. Don’t change any of the settings in the router unless you fully understand what you are doing but you can usually monitor activity and online time easily enough. Just check with your provider on their website.

**Cyber bullying**

If your child is sent something upsetting or something they are uncomfortable with, tell them not to respond or get involved in any type of conversation. Just take a screen shot, save the details, block the person and report it. It can be very difficult not to get involved but if you respond and there are any further dealings, you may be implicated by responding to the person that sent it in the first place.

**Online friends**

Be firm and clear to your children that online friends they have never met personally should not be in their address book or online friends list. I personally spent over a week trying to convince one of my children that it was not okay to be in communication with someone they had never met. Similarly, the needy person with all manner of emotional issues probably was not the person they thought they were. This message was extremely difficult to get across and had to be revisited and discussed a number of times before we met in agreement. Keep an eye out for unusual behaviour and maintain good communication with your children ensuring you know what they are doing whilst connected to your WIFI.

**Keep your information private**

Try this, type your name and the area you live into Google or similar search engine. If you have been careful to protect your identity, you probably will not find any information about yourself. However, if you have posted photos of yourself and tagged them or you have been tagged in photos you could well pop up on a search engine. If you signed a petition or donated to a charity you may also show up online, not to mention your visibility on Facebook, Twitter, Instagram, Snapchat and many other social networking sites. Therefore it is good practice that your children do not use their real names or location when signing up to social media and gaming accounts. This can help protect your children’s identity from others searching to find an individual thus helping your children remain anonymous to bullies etc. Following this advice allows only their real friends to be able to communicate with them or search for them having been given their username previously.

Explain to your children that posting anything online can stay visible forever and to never post something you would not say to a person’s face. There have been many cases where people have posted something online, realised their mistake, deleted it straight away only to find it reposted seconds later after a screen shot was taken. It could be a twitter comment, a post on a discussion, a petition or a comment or video on ‘You Tube’ or ‘Snap Chat’. I have known people lose their jobs from things they posted online. I also know for a fact that recruiters search the internet for information about individuals after they receive job applications. A dodgy profile, comment or pictures posted of an unsavoury nature can have a detrimental effect on an individual’s success.

**GPS SETTINGS**

Beware of enabling GPS settings. There are many apps that now want GPS settings enabled. If you take pictures on your camera or phone with GPS enabled and later post them online, it is relatively easy to find and trace where those photos were taken. It also allows someone to build a profile about you and see what other pictures you have posted and where and when they were taken depending on where you post them. Experiments have shown that locations and habits of people are easily created from posted pictures online. It is possible to see areas you visit, when you visit, frequency and also potentially see inside people’s homes if they have posted any pictures taken inside their homes if GPS is enabled. This can be linked to additional information posted online in other areas for example Facebook, Twitter etc. Please don’t get paranoid but be aware of the wonderful technology in your hand and how powerful it can be for both good and bad.

To turn off GPS on IPhone and IPad try this link:

<http://www.imore.com/how-to-turn-off-photo-geotagging-protect-privacy-iphone-ipad>

On Android – SETTINGS – LOCATION - SWIPE ‘OFF’ FOR LOCATION OR UNTICK BOX.

Beware, apps that need this will ask you to re-enable this feature. Other apps may need this on also but at least you know how to turn it off for photos.

Here is some more info on GPS and photo’s:

 <http://www.digital-photo-secrets.com/tip/1401/how-do-you-find-the-gps-coordinates-of-your-photos/>

Very interesting reading regarding GPS or Geotagging:

 <http://www.wikihow.com/Avoid-the-Potential-Risks-of-Geotagging>

I hope you found this information useful and informative. Don’t forget to share what you have learned with other parents.