e-safety adviser

INSIDE THIS ISSUE:

EDITION 2 – OCTOBER 2012

FACEBOOK EDITION

Welcome to the second edition of this newsletter. I had some really nice feedback from the first edition so thanks for that. Feedback is always good, whether positive or negative.

This month I want to take a look at Facebook. If there is one thing I get asked about the most, the one thing that seems to cause the most grief both in school and out of school, it is Facebook. But, I think a lot of the time that is unjustified.

You see, when we talk about online safety, many people understandably relate that to technology or the Internet. In fact, it has little to do with that.

Let's put it another way, put a speed freak behind the wheel of a car, is it the car's fault or the driver's risk taking behaviour? It is people's behaviour on the Internet and Facebook that causes risk, not Facebook itself.

With that said, Facebook doesn't help matters sometimes: horrendously complicated personal and security settings which can change quite a lot; allowing apps that are controversial to say the least; slow-acting when risks or problems are identified (particularly related to individual problem accounts), questionable moderation and much more.

Mark Zuckerberg, one of the founders of Facebook has always made it very clear that he wants everybody to share everything with everybody. Quite a tall and unrealistic order but that's his vision; knowing that does make you understand why security and personal settings can be so open by default.

Facebook is steeped in controversy; originally called Facesmash, Zuckerberg created a site at Harvard University to compare photos of campus students in a "hot-or-not" contest.

Facebook now has over a billion users; many of them are children and young people, and in this newsletter the risks and issues are what we want to explore.

Enjoy the newsletter. If you do enjoy it let me and your friends know.

Alan

Facebook is great for many different reasons: sharing information with friends and family; keeping in touch with overseas relatives; meeting new people and much more.

But the problem with being so open is that your information is publicly visible for anyone to use as they wish. For the most part this is completely harmless, but as with anything in life there are those people who are up to no good.

There are many arguments for and against children having a Facebook account; I'm not here to preach what is right and what is wrong. The fact is, if your children are on Facebook you must, as a parent, know what the risks are so that you can talk to and help your children.

The policy of Facebook (as well as many other social media providers) is that children under 13 are not allowed an account. You may be surprised to know that the historic reason for that has nothing to do with child protection from predators, it is to do with the advertising laws in the United States (look up COPPA of you are interested to learn more). There is a widely held misconception that it is against the law for children under 13 to be on Facebook. This is incorrect; there is no legal age limit in the eyes of the law, however because Facebook cannot comply with COPPA it is their own policy that restricts the age of users.

WHAT ARE THE RISKS?

THE DARKER SIDE OF FACEBOOK

So what are the risks? If you read the first edition of this newsletter you will already know most of the risks: theft of personal information; trolling, bullying, predator activity; plagiarism, stealing photos….. amongst others. I'm not going to repeat those risks here; just because it is Facebook the risks aren't all that different.

Let's look at a few examples of risks where Facebook has been used as the vehicle.

PERSONAL INFORMATION

Seemingly innocent and fun, counting your savings with Grandma, you take a picture and post it up on Facebook to show your friends. The trouble is, you have shown that to everybody else, including the burglars looking for their next victim. It isn't difficult for the burglars to find you, especially if you have your address on your profile, or if you have global positioning switched on when you take a picture. Within hours, the burglars turned up at the door complete with masks and baseball bats!

BULLIES AND TROLLS

People in the spotlight get a fair amount of abuse, and sometimes that abuse can be turned around on others. Recently one of the X-Factor contestants was getting a lot of abuse on his Facebook account. One supporter of his posted a comment of support; you can probably guess what happened next. The trolling and bullying was turned on the supporter. To make matters worse, her home address was published, her young daughter was targeted for bullying, and a fake Facebook profile was set up in her name depicting her to be a paedophile.

This was taken to court and in a landmark case the courts ruled that Facebook must release the IP address of the computers where the messages were posted from. The IP address is basically a postcode and house number of the computer. In other words, the messages can all be traced.

"I'M 15 YEARS OLD AND RECENTLY A MAN TOOK PICTURES OFF MY ACCOUNT OF ME IN A BIKINI TOP.

HE'S GOING TO PHOTOSHOP THEM SO THAT I LOOK NAKED.

I CAN'T TELL MY PARENTS

I DON'T KNOW WHAT TO DO"

GROOMING AND ABUSE

There is nothing more sickening, more vile than the child abuser. Social media and Facebook in particular has been described as a paedophile playground.

As I mentioned right at the beginning, sometimes Facebook just doesn't help itself.

Not so long ago there was a Facebook group set up to promote the child abuser. Its slogan was "Pedophiles are people too". A complaint was made to Facebook, their answer was, "Thanks for your recent report of a potential violation on Facebook. After reviewing your report, we are not able to confirm that the specific page violates Facebook's Statement of Rights and Responsibilities."

I'm sure you'll agree, that's pretty lame when a policy decision overrides child protection and plain old common sense.

Recently a young man was arrested and imprisoned for grooming many young girls aged between 12 and 15 on Facebook. He collected personal information; including mobile phone numbers of over 1,000 children in order to entice them back to his flat. His enticement and grooming method was simply to compliment the young girls on their photographs.

Police found many videos of the young girls on the man's phone. Worryingly whilst on bail, a 14 year old girl was reported missing and was later found at the man's home.

His sentence? Three and a half years and banned from social media for six years. I'll keep my opinion to myself!!!

A 10 second search on a popular Questions and Answers Internet site, I found the following:

Right I've made this account with a false age to ask the question in this section.

I'm 15 years old and recently a man took pictures off my account of me in a bikini top, he threatened me to photo shop them so I look naked and send them around. He said if I sent him certain pictures he would leave me alone. Recently he's been asking for more and more and I just can't do it anymore. I really don't want my parents to know.. Please help!!!

I'm sure you'll agree, this type of post is hugely concerning for three reasons: firstly that the girl is in trouble and doesn't know what to do; that she has been targeted in such an easy manner and threats are being made against her which could do significant psychological and physical harm; and that she feels she can't go to her parents.

LESS THAN A THIRD OF PARENTS TALK TO CHILDREN ABOUT THEIR ONLINE ACTIVITIES

Ask yourself this question; if your son or daughter came to you with a similar problem, would you know what to do?

Another question; do you think your son or daughter would be able to come to you with such a problem? Have you ever asked them?

Would you know what to do?

People can get very wrapped up in the technology. As I have mentioned before risks and issues on the Internet have very little to do with the technology, but technology and the Internet in

DID YOU KNOW ?

Children say cyberbullying is the worst feature of the Internet. The second worst? Facebook timeline!

Teenagers stress the importance of trust and discussion about online safety between children and parents.

Most kids want to take their own responsibility for protecting themselves online but want support from their parents

(Quotes from UKCCIS 2012)

particular can heighten the risks. So here is some advice:

Take the technology out of the equation; what would you do if this was "real world" and not "virtual world"? You would go to the Police! You would also talk to your son/daughter's school to see if there have been any behaviour changes or concerns.

Security and privacy settings – ensure you and your children have your accounts completely locked down so that only Friends can see posted information. It is impossible in this newsletter to go into all the possible combinations of settings so take a look at the links at the end of this page. Check these settings regularly, perhaps once a month. Facebook does make regular changes which can sometimes leave your account open again.

Remove personal information – why would you want people to view your personal information like your address, phone number, after-school clubs etc. If they are your friends they will know that already.

Ensure you and your children know how to report a concern about something online. Find out what social media they use and understand that they know how to report any type of abuse.

Facebook, like other social media is a wonderful resource – if used properly! The majority of problems encountered are because of people putting themselves or others at risk.

Facebook is such a huge subject it is impossible for me to go into any great detail but I hope this newsletter has given you an appetite to find out more. I have included some great links below where you can learn lots more. In the meantime, have a great October and I will see you in November.

USEFUL WEBSITES:

Lots of information for parents about keeping your children safe, from the experts – CEOP
http://www.thinkuknow.co.uk

Making a report to CEOP
https://www.ceop.police.uk/Ceop-Report/

Reporting a violation to Facebook
https://www.facebook.com/help/?page=204546626249212

Facebook Family Safety Centre
https://www.facebook.com/safety

Securing your Facebook account
https://cyberexchange.isc2.org/UploadedContent/SecureYourFacebook.pdf

I hope you have enjoyed this edition, maybe learnt something new or perhaps it has given you some food for thought.

NEXT MONTH: I'm thinking of moving away from the risks for a month and perhaps looking at some of the technology that is available for you to protect your children at home.

Also, I will hopefully have a new design for the newsletter, I think this design is a little dull.

You can SUBSCRIBE to this newsletter at: www.parentsonlinesafety.com