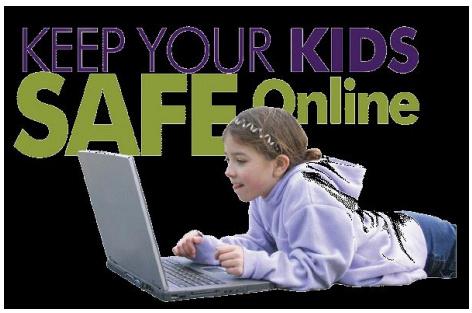
Kids and Internet Safety: 5 Lessons to Consider



Presentation on Protect Children
Bucks University Conference http://youtu.be/fE6yI43-ipI

When I started undercover work, in search of online predators back in 2003, when the web was becoming ‘social’ -- and hardly as dangerous -- a place as it is today.
Chatrooms was my main focus, because they weren't monitored, and because adult subject matter was easily accessible. Whenever I ventured into the dark and seamy realm of the chat world, I could always find someone breaking the law and taking advantage of a child, or what they thought was a child. And I found the perpetrators in a matter of minutes.
As a law enforcement officer, I didn't want to add to the anxiety, instead, I wanted to be part of the solution, to help teach and promote online responsibility. But one of the most striking things I found through my investigations was the fact that children, themselves, were, are behaving in ways that put them at risk. Using this information, I now try to teach kids how to navigate the Internet safely, how to give them the knowledge and power to feel protected whenever they were online.
Technology continued to change over the years, and I saw that more ‘students’ were interested in communicating through their computers via Instant Messaging (IM). Setting up an IM account also included the ability to create an "Online Profile." I think this is when the technology industry realized that there was an interest in moving the web to a more social environment. Shortly after this, MySpace became the hottest way for people to connect online and create their own digital identity. I remember getting phone calls and requests to talk to students and parents about Social Networking. The concern was that parents didn't know about this form of communication; and parents feared that their kids were spending too much time on Social Networks.
As with all great inventions, there's always going to be someone out there who exploits it. And so I started seeing cases where children were meeting strangers online through this emerging social media. There were also cases that involved bullying and cyber-bullying.

Parents lacked an understanding of the technology, and how to make it useful without it being a threat. Over time, MySpace popularity dropped people eventually left MySpace for Facebook.
One of the reasons for this migration, in my opinion, was that Facebook originally required you to have a school/college email address, so it wasn't available for everyone. This gave kids more freedom online from prying parents. But, again, I started to get calls from parents. The big question was: "What is Facebook, and why are my kids spending so much time there?"

Social Media Rules the Web.

I don't care who you are, but I'm sure you either have an email address, LinkedIn account, or Facebook or Twitter account. You're living on the social web, and it's important to maintain a positive image of yourself and be more responsible with your identity in this rapidly expanding digital environment.

This form of technology clearly isn't going away. And, as a result, I need to focus on teaching children how to stay safe and protect their privacy and reputations on social networks. I also need to give parents the solutions and tools to monitor their kids' social web activities. Parents are able to watch over their kids in the real world; now I must help them oversee their children in the digital world.
Here are five lessons learned that I have gathered over the years I believe crucial for parents -- and their kids -- to consider:

- Concerns over online predators: Although the risk of encountering an online predator may be low, the risk is there. To help lower the risk, children should only communicate with people they know from the ‘non-online’. Predators can pretend to be someone they are not, (like another child) and may show up in places where children like to play online (Social Media / inc Habbo / Club Penguin).

- Cyberbullying:

  Children should only give their passwords to mum & dad. They should never share their passwords with their friends. Children will give their passwords to friends though in the following instances: a friend may be better at an online game and can earn them credits to purchase online goods; they may have a friend whose parents don't allow them on the same sites as your child so they let them borrow their site. The problem is this: Those who are your friends today, may not be your friend tomorrow. These ex-friends now have your password. And if you are like many people who only have one password for all your accounts, now they have access to them as well. These ex-friends can now log into your accounts, pretend to be you, and start vicious rumours and turn your other friends against you.

Therefore regularly change your passwords. Make the password strong, not simply ***'Middle Name, Football Team etc, perhaps something like 291260+190565=6, either way make it strong'. (That password isn't used by me but is memorable)***

- How to teach responsibility: Parents should teach their children to never post hurtful comments and/or say anything that may be offensive. If anyone should post such comments on their page, they should remove them immediately. If you wouldn't say it in person, you shouldn't say it online.
- Geotagging / Geolocations services:

  Parents and children need to know what the capabilities are of the devices they use. If you have a Smartphone, iPod, iPad or any wireless device that can take pictures, you should turn off the location services for the camera. Location services turned "On" with the camera will embed a "Geotag" with the latitude and longitude of where the person was standing at the time they took the photo and/or video. If these images are then posted online via Facebook or any other site, someone can locate them based on the geotag.
- Social Networking settings: Make sure you check your Privacy Settings on any social media site at least once a month. Sites are always making changes and these changes may take your settings and set them back to the default, which may not be as secure as you originally set them.

I tell people that if you're going to live your life like an open book online, people are going to read it. And that's why -- more than a decade after starting my quest for greater Internet safety -- I continue to do all that I can to protect children, educate parents and safeguard schools, when it comes to the web.

In conclusion, I feel strongly that parents must take this issue seriously today; and they must step up and monitor their children on social networks. The bottom line here is that the social web is simply not a game or a toy.

Jonathan Taylor MSc
Internet Safety Advisor
besafeonline@ymail.com
www.besafe-online.co.uk

http://wp.me/p1K9Rb-E