

## **The Impact of Facebook on Our Students**

Demonize it, or extol its admissions and alumni-network virtues; the use of Facebook in our schools is likely to elicit strong opinions. One thing is for certain, the use of Facebook repeatedly comes up in discussions about Internet safety, age-appropriate exposure, and student online behavior. Though many schools have different policies for using or accessing Facebook, we share many of the same concerns.

Through our Internet safety organization, ChildrenOnline.org, we've surveyed the Internet behavior of thousands of Independent school children and teens. We've learned a great deal about their use of Facebook and the inherent issues they face, as well as their schools, because Facebook is one of the 2 most popular websites for independent school students across grades 4 - 12. (The other site is YouTube.) I would like to summarize our shared concerns and address the issues that impact our students, and our communities.

*NOTE: Though this article targets Facebook specifically, due to its popularity, it also applies to the many other social networks our students frequent. They include YouTube, MySpace, Hi5, Friendster, Xanga, DeviantArt and others.*

### **1. For those schools that allow it, the use of Facebook in our communities can take an inordinate amount of Internet bandwidth.**

And for those schools that allow access to Facebook, how do we reconcile our concerns that younger and younger children are using this adult social network? Four years ago it was rare to learn of a child under 7th grade with an account. Last fall, for the first time, 4th graders began reporting to us that they had Facebook accounts. We now estimate that about 60 - 70% of 7th graders have accounts and the number is higher for 8<sup>th</sup> graders. These children are too young to be using Facebook or other adult social networks for the reasons detailed below.

### **2. Using Facebook takes time. Often, a LOT of time!**

The greatest motivating factor for children to use technology in grades 7 and up is to connect to others; to socialize. Their irresistible need to connect with their peers, coupled with the development of 24/7 accessible technologies, can make the use of sites like Facebook all consuming. We have concerns for children and teens today growing up in a world where they are wired 24/7 without a break. For many of our kids there is little or no "down time." Some have difficulty disengaging from their social life. For some, it even raises their anxiety level to be without their cell phones for a few hours! We don't believe this is healthy for them.

### **3. To our students using Facebook, there is a false sense of privacy.**

Couple this false sense of privacy with the feeling of anonymity and lack of social responsibility that often develops from using text-centered telecommunications, and we see that many students post embarrassing, humiliating, denigrating and hurtful content in both text, photos and videos. We need to teach them that *NOTHING IS PRIVATE* online,

especially their social networks. We need to show them examples of the serious consequences that have occurred to those whose egregious online behavior has been made public. Students have been expelled from high schools and colleges. Students have been denied acceptances to intern programs, admission to independent high schools, colleges, and jobs at summer camps. Students, and their families, have been sued for slander and defamation of character. Students, and their parents, have been arrested. All because of the content they've posted in their "private" social network accounts. People are trolling their accounts. Hackers, scammers, reporters, police, high school and college admissions officers, employers, parents and summer camp directors...Adults ARE looking and the kids don't get it! Also, they don't realize that the instant they post something to Facebook (or MySpace or YouTube, etc.), they've just lost control and ownership of that content. Try reviewing the privacy rights of Facebook with your middle and high school students. It is quite an eye opener!

In the fall of 2007, Dr. Nora Barnes, Director for the Center of Marketing Research at UMASS Dartmouth, published a study that showed more than 20% of colleges and universities search social networks for their admissions candidates. Do you think that percentage will decrease, increase or remain unchanged in the coming years? Ask your high school students that question!

<http://www.umassd.edu/cmr/studiesresearch/cmrblogstudy3.doc>

Students often ask us how can anyone possibly get into their private Facebook pages. Here are the most common methods and a link to a sample article about each:

- a) Security and software flaws are exposed. Software is hacked.  
<http://www.techlearning.com/blogs.aspx?id=15098>
- b) Accounts are phished when users are tricked into clicking an email or IM link taking them to fake login pages. Once phished, scammers use various applications to suck out personal information from a user's entire network of friends. Scammers try using the phished information, including the login password, to access banks and credit card accounts because they know that most people have one password for all their accounts. They also target teens Facebook accounts because they've learned that a small percent of their parent's use combinations of their children's names and birthdays as passwords to their financial and credit card accounts.  
<http://www.techcrunch.com/2008/03/26/phishing-scam-targeting-facebook-users/>  
[http://www.wired.com/politics/security/news/2008/01/facebook\\_phish](http://www.wired.com/politics/security/news/2008/01/facebook_phish)  
<http://thenextweb.com/2008/08/10/facebook-under-massive-phishing-attack-from-china/>
- c) Perhaps the most common reason that teens' private information is exposed is because they are easily tricked into accepting friend requests from strangers. Though there isn't a lot of research available on this point, some research and informal studies suggest that teens allow into their Facebook networks 44% – 87% of the strangers that knock on their door. This trick is best described as the “wolf

in sheep's clothing." Many kids, especially girls, have a difficult time saying "no" to a friend request. (see below regarding the definition of the word "friend.")  
[http://news.cnet.com/8301-10784\\_3-9759401-7.html](http://news.cnet.com/8301-10784_3-9759401-7.html)

- d) Students' passwords are easily guessed or hacked with readily available "cracking" software. We've met 5<sup>th</sup> graders who have demonstrated knowledge of using hacking tools such as password crackers. There are numerous examples of kid's accounts being hacked simply because someone guessed or figured out their password. Last September Gov. Sarah Palin's personal e-mail account was broken into when the hacker figured out that her password was a combination of her zip code and birth date.

<http://www.cnn.com/2008/POLITICS/09/22/palin.email.probe/index.html>

*NOTE: Police, and other investigative authorities such as the FBI, can have access to "private" Facebook pages. Also, we strongly suspect that Facebook itself sells access to information posted on private pages to third party marketers willing to pay the fees. At least, that was what one former employee in the social network industry who wished to remain anonymous described to us.*

#### **4. There are 1000's of scams targeting teens in their social networks, especially Facebook and MySpace.**

These communities are predicated on a certain level of trust. Our students, though very knowledgeable about using technology, are often naive and easily manipulated (though they would hate to think so). A simple example is a scam that hit Facebook users late last fall. Many teens had their accounts phished and the phishers sent out posts from those accounts to their friends that said "OMG! There are some photos of you on this website", along with a link to the website. The website showed hazy photos in the background that were hard to make out and appeared to be somewhat pornographic. A popup told the visitor they would have to register for an account in order to view photos on the site. We're certain that many kids were tricked into revealing a lot of personal information about themselves in this scam. In another scam that targeted MySpace in the last couple of years, more than 14,000 users were tricked by fake MySpace pages into visiting music web sites to purchase music for \$2-3 per album. Instead of getting music, the site charged their credit cards \$300-600. Kids are easily fooled. They want to believe what is said to them, especially when it appears that others believe. Scammers use this trick against them by creating 1000's of fake pages on social networks that talk about bogus web sites to buy stuff, products that don't work (e.g. herbal meds) and cool pages that only result in drive-by spyware downloads.

#### **5. Spyware and Adware installations are very serious concerns.**

Those of us with PCs running Windows OS in our schools already devote a great deal of time, money, and other resources to these threats. Giving kids access to social networks in our school environments greatly exacerbates these threats. We need to teach our students that "Free" usually has a price when it comes to the Internet. We need to teach them how to try to determine if software, such as a Facebook Add-on, is likely a

disguised piece of malware. (Much of it is!) Below are links to 3 related articles:

<http://www.pcadvisor.co.uk/news/index.cfm?newsid=102800>

<http://sophos.com/pressoffice/news/articles/2008/08/facebook.html>

[http://www.theregister.co.uk/2008/04/02/facebook\\_spam/](http://www.theregister.co.uk/2008/04/02/facebook_spam/)

*NOTE: "Mac owners" are not completely off the hook. Last June, the first 3 spyware apps were discovered against the Mac OS and late last fall there was evidence of hijack-ware successfully targeting Firefox on a Mac.*

## **6. We need to acknowledge that screens act as a moral disconnect for many of our students.**

Every day online there are thousands of kids who say mean and hurtful things because they can. They are increasingly living their social lives in a world without caring, loving adults watching out for them, without expectations for their behavior, and without boundaries. Research shows that children grow up healthiest in a world with love, communication, structure and boundaries. These qualities hardly exist online for our children/teens. Instead, harassing language is normalized, the sexualization of girls/women is common-place, and the lack of supervision creates an "anything goes" wild-wild-west. Here is a simple case in point. Would Texas Longhorn lineman, Buck Burnette, have said the same thing about President-Elect Obama if handed a microphone at a school assembly in front of hundreds of students? Would he have written his posted statement on a large poster and held it up in downtown Houston for a few hours? I doubt it. Visit:

<http://ncaafotball.fanhouse.com/2008/11/06/texas-c-buck-burnette-learns-why-racist-obama-facebook-updates-a/>

Our students need to learn to be nice and kind to others online. They need to be respectful and thoughtful about what they say and how they act online, just as in real life. We need to do a better job of teaching them that disengaging from social responsibility while using telecommunications is not acceptable behavior.

## **7. Our students have very little knowledge about how much they are being marketed to; how their purchasing decisions and attitudes are being manipulated; how their personal information is used, and even how valuable that personal information is.**

Most don't understand the damage that can come from identity theft and impersonation. They are heavily targeted on Facebook and their data is heavily "scrubbed" and used. Facebook's announcement about Beacon in November 2007, brought such a huge negative assault from users that Mark Zuckerberg had to back-step and tell users that they were automatically opted OUT, rather than IN, as planned. Most users saw Beacon as a privacy nightmare. We need to help our students become more media-savvy, understand the value of personal information, and how to protect it.

<http://gigaom.com/2007/11/06/facebook-beacon-privacy-issues/>

[http://news.cnet.com/8301-13507\\_3-9829401-18.html](http://news.cnet.com/8301-13507_3-9829401-18.html)

<http://www.pcmag.com/article2/0,2817,2228622,00.asp>

**8. Our research shows that children and teens are increasingly using telecommunications technologies, including Facebook, to avoid difficult face-to-face conversations.**

For example, it saddens us to hear 16-year olds say that they would rather break up with their girlfriend/boyfriend by texting, IM-ing or posting on their Facebook wall than tell them in person (or over the phone). When asked why, they'll tell you "because it's easier." We believe this avoidance will have increasing negative ramifications on their communication skills throughout life.

**9. Also, children are increasingly turning to making friendships and building relationships online.**

This includes the use of Facebook. Socialization skills in children are best learned in real life. Children are far too inexperienced to use telecommunications tools to make friends and build relationships in a healthy and safe manner online.

**10. The meaning of the word “friend” is changing for our students and this change puts them at risk in several ways.**

Ask an average teenager how many friends they have in their Facebook account and from some you may hear numbers between 200 and 500. “Friending” is a verb and for many of our students, some of their friends are complete strangers. We need to challenge them to think about what a friend is and consider the ways we typically value friends. Words like trust, love, support, and sharing come to mind. However, student’s risks rise when they apply traditional real-life values to the “friendships” some of them develop online in sites such as Facebook.

I have a Facebook account and actually see it as a wonderful, and valuable, resource. However, just because Facebook says that anyone 14 years or old CAN use Facebook, doesn't mean that they should. It isn't an age-appropriate or developmentally healthy place for our children and younger teens to hang out. Facebook is not working to protect our children and the laws in our country are terribly inadequate to safeguard our children online, in general. Not enough is being done to protect and educate children and teens against the risks that come from using the Internet, and Facebook in particular. We (adults, parents, educators) need to do more.

In addition, during the last few years our schools have been welcoming an influx of a new generation of teacher. These younger teachers are typically more comfortable with technology because they’ve grown up with it. This also presents some challenges as well. Case in point... Must independent schools consider setting policies for teachers regarding the use of social networks like Facebook? Should we set guidelines for the possible social interaction of our teachers with their students in sites such as Facebook? Many independent schools are currently debating these questions. Articles related to this topic make very plausible arguments for setting guidelines for teachers, as well as students.

[www.sun-sentinel.com/news/education/sfl-flpfacebook0601pnjun01,0,370501.story](http://www.sun-sentinel.com/news/education/sfl-flpfacebook0601pnjun01,0,370501.story)  
To read more articles such as this one, visit Google and enter the words *teacher*, *Facebook*, and *content*.

ChildrenOnline.org produces a free monthly newsletter that is designed to keep educators and parents informed about the latest issues affecting children online, and to address specific questions often raised by parents and teachers. We invite you to subscribe to it.

One final note: The Internet is constantly changing, as are the ways that kids are using it. From recent visits to some independent schools, we have learned of a rising interest about which we are very concerned. Some middle and high school students have begun to discover online live broadcast TV, known as “social broadcasting.” BlogTV.com is one such site where a visitor is able to use a built-in video camera to broadcast him or herself live on the Internet. Anyone can stop by, enter a chat window, and anonymously interact with the person broadcasting. As you can imagine, without any controls, standards or boundaries, this technology can have some serious negative consequences for some children and teens. For some of our students, using this technology can be irresistible, especially younger children who see themselves as being on real TV.

Doug Fodeman  
Co-Director, ChildrenOnline.org and  
Director of Technology  
Brookwood School  
Manchester, MA 01944  
(978) 526-4500 X6233  
[DFodeman@Brookwood.edu](mailto:DFodeman@Brookwood.edu)

ChildrenOnline.org offers innovative and comprehensive workshops on Internet safety and online education to students, parents, faculty and administrators. Our approach, unique in the field of Internet safety, combines a thorough understanding of Internet technologies, child development and counseling, to focus on the impact of the Internet on the social, emotional and language development of young people.

© Children Online, LLC. 2009. This article may not be reprinted without permission.