



Email Confirmation

Subject: Children Online Newsletter

You're receiving this email because you signed up at ChildrenOnline.org.

You may [unsubscribe](#) if you no longer wish to receive our emails.



Quick Links

[Register Now](#)
[Resources for Parents](#)
[Children Online Website](#)

Join Our List

Join Our Mailing List!

Issue: #20

January 2009

20th Edition of the Children Online Newsletter.

Last month we addressed one of the two most popular reasons that kids are drawn to using the Internet. Playing games. This month we look at the other major attraction - socializing.



Realities of Friending

During the summer of 2007, Sophos, a web security company, conducted an experiment with Facebook users. They created a fake Facebook profile and randomly sent out friending requests. More than 43% of those requests were accepted and 41% gave access to personal information.

More specifically, this month's newsletter takes a look at Facebook. Facebook is the most popular social network amongst 7th - 12th graders.

Though the Internet is constantly changing, we have found one "constant" during our 13 years giving workshops on Internet safety... Whatever kids are doing on the Internet this year, they will be doing the same thing next year at a younger age. Last fall, for the first time ever, we had 4th graders reporting to us that they had Facebook accounts. As you'll read, we don't believe these adult social networks are healthy or safe places for our children under sixteen to be spending time.

Our related article about Facebook, titled "The Impact of Facebook on Our Students", will be posted on the NAIS.org web site this February and posted in their eBulletin as well. If

Scammers are far more surgical and successful in their campaigns to "friend" teens as a way to get personal information, manipulate, and defraud them. We've heard unsubstantiated reports that some scammers successfully trick nearly 90% of the teens they contact into letting the scammer into their account, and into their network of friends. Scammers use programs like the Fox Adder, Mass Friend Adder, or Rude Adder to target a Facebook demographic. These programs allow them to construct a message and send it as a "friend request" to thousands of "private" Facebook users of a particular location, age, gender, etc.

Once inside a Facebook network, scammers use similar programs to locate and copy all of the personal information they can find. Personal information is primarily culled for possible financial and identity theft.

Scammers can

you would like to receive a copy of it, please let us know.

As always, we welcome your comments. Our telephone number for Children Online is 413-214-1225.

Best wishes,
Marje Monroe and Doug Fodeman

Contact Marje or Doug via email at marjem@childrenonline.org or dougf@childrenonline.org for information about our programs or consulting services.

Living With Facebook

An old college friend contacted me recently. Not on the phone or through the mail, but on the social networking site, Facebook. Adults, like me, who admit to carrying typewriters to college, are now finding themselves online and "meeting" friends. While I have been researching and studying teens' use of Facebook for several years, I have only recently used Facebook for pleasure and, for the most part, it is a pleasure.

It is a mistake, however, to confuse an adults use and interaction with Facebook to a child's or even a teen's use. Quickly becoming the number one website with young teens, Facebook has become a transforming instrument. What started as a unique and creative way to connect to lost friends, or create new friends, has morphed into a complex site filled with advertisements, marketing scams, phishing attempts, and pornography.

As younger children and teens have rushed to social networking sites, lured by being part of a community, they have frequently been faced with issues they may not be ready to handle. Today a teen's weapon of choice against someone else is most likely Facebook. Emboldened by a feeling of privacy, anonymity and a moral disconnect created by the screen, teens often post words or pictures that they would never use in person. Meanness and harassment litter the pages of young Facebook users. Fake sites attacking teachers, parents, ex-friends or employers have popped up creating a great deal of anguish for the attacked party. As anyone can create a site, and pretend to be another person, it is impossible to block slanderous and mean material from going online. Once online, it can be extremely difficult to have material removed completely.

Unbeknownst to most children or teens using Facebook, they are being targeted daily with marketing scams, phishing attempts and fake sites set up to lure them to malicious or inappropriate sites. Scammers use sophisticated software to

.....
 easily create [fake pages](#) using services like "Fake My Space" to populate their pages with dozens and dozens of "friends." They can then push bogus products, websites that result in [drive-by spyware downloads](#) and other scams. [Try entering the words fake, social, network and pages into Google's search field.]

How Do Strangers Get In?

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. Students often ask us how anyone can 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.

gather personal information that can be used for identity theft or impersonation. As the Internet has grown, people have quickly realized the moneymaking opportunities on social networking sites. Teens and children follow links and pop-ups hoping to win free merchandise, make more friends or gain entry to a cool new world. The lure of exciting pop-ups or a "once in a lifetime" deal is hard to resist. These ads or sites may lead to exciting and fun opportunities. They can also lead to spyware, adware, rip-offs, identity theft and manipulation.

When talking with teens, they proudly discuss their ability to set their sites to private and universally state they are very careful not to let just "anyone" into their site. While there is no single statistic available, our work with children and teens indicates that young people find it very hard to turn down friend requests. Young teens may have more than 200 "friends" who have full access to their pages. In addition, young people communicate daily through blogs on their sites, which often contain harassing, suggestive or inappropriate material. Social networking users are ripe targets for adults with harmful, or even criminal, intent. Pretending to be a cool sixteen year old, any adult or teen can fake a site, ask for entry to thousands of unsuspecting teen sites and gain entrance to their "private material." Once on a page of someone belonging to a network, every user in the network is now open for the person to see and /or exploit. Most teens are, in fact, connected to multiple networks such as sports teams, schools or clubs.

What teens and most adults don't realize is that the small print of social networking sites explicitly states that the site has the right to archive, copy, retain, transfer or use the material in any way they deem necessary. In essence, any words, images or videos put up on most social networking sites including My Space, Facebook, and YouTube by rights belong to the sites and not to the individual who posted them online. Adolescents making mistakes and pushing boundaries online can, and do, create serious implications for their futures including college admissions, secondary school admissions, employment checks or simply personal humiliation.

Strategies for Social Networking Sites:

- We recommend that teens fifteen and younger not have access to SNS.

Given the numerous marketing scams, exploitation possibilities, access to sexually graphic and harassing language and opportunities for meanness and bullying,

b) [Accounts are phished when users are tricked into clicking an email or IM link taking them to fake login pages.](#) Scammers try using the phished information, including the login ID and 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 own financial and credit card accounts.

Additional articles:

[Wired.com](#)
[TheNextWeb.com](#)

c) Perhaps the most common reason that teens' private information is exposed is because [they are easily tricked into accepting friend requests from strangers.](#) This trick is best described as the "wolf in sheep's clothing." Many kids, especially girls, have a difficult time saying "no" to a

younger teens are not developmentally ready to navigate the site safely. Teens are more vulnerable to exploitation and marketing.

- If your teen already has a site, ask them to let you see their pages.

Start by giving them 24 hours notice and then explain that you will ask, from time to time, to see their site. If the child refuses because of privacy, explain your role as a parent to keep them safe, tell them that they may only have access to the site if you are allowed to see the site from time to time.

- Read the Fine Print

Ask your teen to print out the acceptable use policies for the site and then read the fine print. Read it with them to fully understand their privacy and user rights, or lack thereof.

- Use software to help you create time boundaries for SNS use

Given their choice, teens might be online all night. Appropriate software can help parents create limits for Internet use. For example, you can set Internet access to shut off at 10pm or during dinnertime or study hours. (See our [May, 2008 newsletter for Parental Control software recommendations.](#))

- Explore the various SNS sites yourself.

We recommend you not use your work or home emails to set up accounts online. Use an Internet email service, such as Yahoo, Hotmail or Gmail, to set up temporary email accounts. Create an account in an SNS that places you in the 13-17 year old age group. Use a fake screen name and begin exploring some pages. You may not be able to enter private sites unless you ask a member of the site to enter.

- Ignore your child's outrage about privacy, honesty and distrust.

It is common for teens to be outraged when they realize that "adults" have been looking at their sites. In reality the sites are not "private" even when set to a restricted setting. Teens feel a false sense of ownership of the Internet and SNS sites in particular. Be clear about

friend request.

d) Students' passwords are easily guessed or hacked with readily available "cracking" software. We've met 5th 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.

About Children Online

Children Online 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

your role in keeping them safe.

- Explain that there is no privacy online, especially on SNS.

Begin by showing your child the actual terms of condition for a popular site such as Facebook or YouTube. Explain that everything online can be copied, archived, or transferred to another site or person. Explain that colleges, future employers and others are in fact searching through Facebook and other social networking sites.

- Google words combinations such as "Facebook" and "scams" or "hack" or "attacks" and ask your child to follow links to see how easy it is to hack into accounts or trick users on these sites.
- Remind them that they lose all control of content once posted online.

**© Children Online 2009
Doug Fodeman & Marje Monroe.
For permission to reprint please contact
DougF@ChildrenOnline.org**

of the internet on the social, emotional and language development of young people.

Doug Fodeman and Marje Monroe, experts in technology, counseling and education, work together to provide invaluable research and tools for parents and schools with practical real-life solutions to the issues faced by young people online. Since 1997, Marje and Doug have spoken to thousands of students, teachers and parents. They have several publications in the area of Internet safety and offer a free online newsletter. More detailed information can be found at ChildrenOnline.org.

[Forward email](#)

✉ [SafeUnsubscribe®](#)

[Update Profile/Email Address](#) | Instant removal with [SafeUnsubscribe™](#) | [Privacy Policy](#).

Email Marketing by



ChildrenOnline.org | 19 Everett Paine Blvd. | Marblehead | MA | 01945