

# ChildrenOnline

Devoted to the safety of children and teens online

Phone: 413-214-1225

A Division of Web Safe Consulting

## Quick Links

[Previous Newsletters](#)  
[Resources for Parents](#)  
[Children Online Website](#)

## Join Our List

[Join Our Mailing List!](#)

## Related Resources:

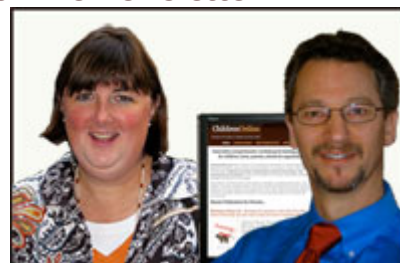
1. A funny video that makes the point about putting yourself at risk for serious consequences due to "over-posting" is the [video by Edan Freiburger and Nicholas Chen called Overexposed](#), winners of the 2010 Trend Micro contest.
2. [Privacy smackdown: Facebook versus Google+](#) by Woody Leonhard at Windows Secrets.com
3. Video: [How to Disable Facebook's Facial Recognition Feature](#) by the Electronic Frontier Foundation ([EFF.org](#))
4. [Researchers show the power of Facebook facial-recognition software](#) by Nathan Olivarez-Giles from the LA Times.

## Issue: #51

August 2011

### 51st Edition of the Children Online Newsletter.

Recently a colleague of ours posed a question across our listserv, "does anyone have any good resources or advice for talking to kids about online privacy?"



We thought it was a great question but we couldn't find any worthwhile resources to recommend. We decided to write our own.

As always we welcome your comments and suggestions.  
 Best wishes,  
 Marje Monroe and Doug Fodeman

ChildrenOnline.org is accepting workshop dates for the 2011-2012 academic year. If you are interested in having us conduct student, parent or faculty workshops, please contact us via email or phone (413-214-1225).

### Talking to Kids About Online Privacy

Michael Novak, American Philosopher and novelist, once said "even rock stars are entitled to privacy." Privacy is one of those under-valued intangible rights that is easily eroded. Adults better understand the value of privacy than do children or teens. Adults also understand that losing one's privacy online can result in serious consequences, both financial and personal. Online privacy is simply not on the radar of children using the Internet. And while teens are more concerned about their online privacy than children, they are naïve, unaware, misled or simply careless about their online activities when it comes to protecting their privacy. This can be especially risky living in an age where many of the devices we hold in our pockets and purses can

5. Video: [Facebook New Privacy Settings 2011](#)

6. Video: [Facebook Tutorial 101 - How To Set Your Privacy Settings Part 2](#)

7. [House Committee Approves Controversial Measure to Require Data Retention for All Internet Users](#) from the [Electronic Privacy Information Center](#)

8. [Can My Employer See My Private Facebook Posts?](#) by Ken Kolburn of the East Valley Tribune, October 11, 2010.

9. [When can cops gain access to my personal info on Facebook?](#) by G.W. Schulz, from the Center for Investigative Reporting.

10. [Facebook stole every contact and phone number in your phone --here's how to undo the damage](#) from Zach Epstein, August 12, 2011.

11. [The Phone Hacking Scandal and Social Media](#), by Omer Tene, July 28, 2011

12. For a little humor, watch this spoof video about ["Gmail Man"](#) produced by Microsoft 365

14. Can your old Facebook status updates suddenly reappear without your permission? Apparently. Is

tell companies, law enforcement, marketers, and others where we are, or where we were from the photos we took and uploaded to the web.

So how can parents (and school Internet education programs) raise children's and adolescents' awareness and teach the concept that privacy matters and does not exist online? Our recommendation is to create a multi-step approach that is appropriately directed at the developmental levels of kids.

All children, including teens, first need to understand what counts as personal information. Besides the obvious data such as name, address, home phone, cell phone and birthday, point out that personal information includes such information as:

- Gender and age
- School attended
- Sports teams/clubs/groups/activities in which they participate
- Personally identifying features such as sports team jersey number and game schedule, screen names, and religious affiliation
- Friends list on social media sites such as Facebook and Google+
- Any photos they, or their friends, upload to Facebook due to Facebook's face-recognition software
- Any information about their parents or siblings

### **Elementary Age Children:**

Teach younger children what type of information is considered "personal information" and that it is NEVER OK to provide that information to anyone on the Internet without a parent's permission or supervision.

Younger children spend a great deal of their online time in gaming websites and YouTube. Gaming web sites will typically ask children to set up accounts and ask for lots of personal information such as name, address, email and, in some cases, cell phone numbers. Also, scammers and unscrupulous marketers target children in game sites, trying to extract even more information from them. We have seen scam ads asking children for such information as a mother's

that an infringement on your privacy? Read "[New Facebook Features Shows Your Old Status Updates from 2010 & 2009](#)" by Ben Parr, posted August 13, 2011.

15. [Are Your Teens Oversharing Online?](#) at Today.com, January 5, 2011

### Announcement:

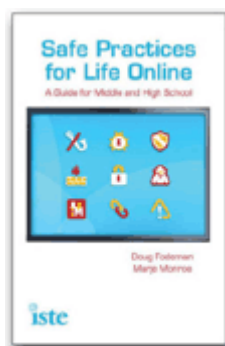
We are very pleased to announce that our first book, "Safe Practices for Life Online", published by the International Society for Technology in Education, will be available in four languages in 2012. It is also currently available for the Kindle. The second edition is due out in mid-2012 and contains more than 100 classroom exercises.

We have also recently signed our next book contract. Look to 2012 for our next book!

## INTERNET SAFETY CURRICULUM

Safe Practices for Life Online

Children Online has a curriculum



maiden name, birth date and cell phone numbers. Scam emails, disguised as emails from Game site administrators, YouTube, iTunes, and even the FBI ask for login information such as passwords, social security numbers and more. The difficulty for our children is that many websites require them to provide some personal information in order to use the website. Parents will need to decide how comfortable they feel about providing a child's personal information or whether to use their information and register under the parent's name and allow the child access.

### Middle School Age Children

The risks for children in grades six through eight increase as they begin to explore more areas of the Internet and use applications that can reveal more information about them. Of course it is still important that tweens and young teens understand what counts as personal information, and that they should be very careful what they reveal and to whom. However, they can also understand that information has value and their personal information may be sold to marketers (legitimate and unscrupulous), spammers or thieves. They should also understand that their online activities may be closely monitored. Our [December, 2010 newsletter](#) ("Privacy and Our Children's Online Reputation") specifically addressed this point and included a link to a feature N.Y.Times article titled "[On the Web Children Face Intensive Tracking.](#)"

This age group should also be taught **NOTHING IS PRIVATE ONLINE**. Though it may not be immediate or in every instance, someone unintended will sooner or later see something they have written or posted. Explain that the most common ways in which this happens, besides hacking, software "bots", and marketing tools that "scrape" data on sites, is through:

1. "Over-the-shoulder" viewing such as when a parent looks at a child's screen
2. Over-sharing such as when a teen passes on a text or picture to other friends
3. Passwords to accounts get hacked, are shared or become known
4. Teens are not aware that their account settings expose some their personal information in those accounts

on Internet Safety that includes nearly 100 student exercises and lots of information on many topics including social networks, instant messaging, cyberbullying, online marketing, scams directed at kids, protecting privacy online, avoiding identity theft and impersonation, creating strong passwords and more.

There is also a student edition which includes cartoons and "Did you know" sections of interesting facts for students.

To learn more or place an order visit our [publications page at ChildrenOnline.org](#) or go directly to our publisher's pages:

[Teacher's Edition at ISTE](#)

[Student Edition at Lulu.com](#)

### 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 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**

5. Popular news or sexually suggestive content is used to trick teens into installing spyware (and other forms of malware) onto their computers
6. Their own mistaken posts in web areas that they assumed were private

### High School Age Teens

The risks for high school age teens can be significant because some are exploring very risky behavior and much more can be "at stake" such as college acceptances, internships and job opportunities as well as revealing deeply humiliating or embarrassing behavior. Also, when they sign up for such activities as team sports they often pledge to honor team behavioral expectations. They don't realize that sometimes coaches, school administrators and others have the means and skills to monitor some online activities. Or, as is often the case, parents and other students may bring breaches of behavioral expectations to the attention of school officials or other parents. They are also at risk because, as web-savvy as they consider themselves to be, they often trust their personal data with complete strangers and friends-of-friends who may abuse access to their social networking accounts.

In addition to the tips mentioned for the younger age groups, it would also be wise to do the following with high school age teens to reduce their risk of over-exposure of their privacy online and raise their awareness of the issues:

1. Ask them to read some recent articles about other kids who have had serious consequences as a result of exposure of their online behavior. It is easy to find articles by doing searches for the words Facebook and teens (or kids) combined with words like arrested, suspended, fired, or disciplined. We have provided a [set of links from such news stories posted during the last couple of years](#).
2. Since teens spend a great amount of their time socializing in social networking sites, impress upon them that there is no privacy in such sites. Examples that illustrate this point are:
  - Google Buzz conversations are searchable in Google
  - Facebook's privacy settings change, on average, three

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](http://ChildrenOnline.org).

Â© Children Online 2011  
 Doug Fodeman & Marje  
 Monroe.  
 For permission to reprint  
 please contact  
[DougF@ChildrenOnline.org](mailto:DougF@ChildrenOnline.org)

- times a year and at least one of these changes reverts users back to the most public settings
- Scammers routinely hack teens and target their Facebook accounts to gather information that has financial value and to trick teens into installing spyware to target their parents. Pay a visit to [FaceCrooks.com](http://FaceCrooks.com) for up-to-date scams making their way around Facebook.
- "Zombie" flash cookies contain information about our online browsing behavior. These cookies are not removed by wiping out the history and cache of a web browsing session. [They require other software tools to get rid of them such as [Flush](#) (Mac) or [Flash Cookie Cleaner](#) (PC) [See "[You Deleted Cookies? Think Again](#)".]
- The average high school junior has 802 Facebook friends\*. If they set their account to "friend of a friend", and assuming each of their friends has 400 other unique friends, it would mean that they are sharing their personal information with 320,800 other people. And according to a study conducted by TRUSTe, 68% of teens friend complete strangers.
- [College Admissions officers](#), [police](#), and [employers](#) have routinely gained access to "private" Facebook pages.

3. Instruct teens that when they install Facebook add-ons, they are giving away the keys to their privacy completely. Many add-ons don't play by the rules and abuse users personal information. Some are disguised malware. For those teens with a Facebook account, give them the following challenge. Ask them to guess how many Facebook add-ons they think they have installed to use with their Facebook account. Then ask them to log into Facebook and actually check. I recently did this with one teen and she was shocked to find 45 apps were using her personal data when she thought she had only installed 10-12. To check on the apps:

- a) Log into Facebook, click ACCOUNT and select Account Settings
- b) Select Applications from the left menu bar

4. Teach teens never to save passwords or personal information in web browsers. Encourage them to have a

second "junk" email account which they should use to give web sites or marketers who require an email address in order to use their services. They should closely guard their personal email account. Encourage them to have slightly different passwords for different accounts. They should **NEVER** have a bank account that uses the same password as a social networking site.

5. Clicking a Like button just about anywhere on the Internet reveals a great deal of information about ourselves to marketers and is then used to influence our behavior and purchasing decisions. [See the WSJ article "[Like Button Follows Web Users.](#)"]

6. Finally, impress on them that we all leave digital footprints everywhere we go online and when using smart phones. These digital footprints are extremely difficult to erase.

\*Based on our 2010-2011 research.