

ChildrenOnline

Phone: 413-214-1225

A Division of Web Safe Consulting

Devoted to the safety of children and teens online

Quick Links

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

Join Our List

[Join Our Mailing List!](#)

Related Articles and Resources:

[1. Cramming: Mystery Phone Charges](#)

[2. Fact Sheet on Adolescent Brain Development \[pdf\]](#)

[3. Why teenagers are moody: Scientists find the answer](#)

[4. Man arrested for robbing Runescape virtual characters](#)

[5. A guide to scammers in the Webkinz Trading Room](#)

[6. SCAMDEX: The Internet scam resource](#)

Issue: #32

January 2010

32nd Edition of the Children Online Newsletter.

In last month's newsletter we addressed the primary reasons why kids are motivated to use the Internet. This month we follow up with a look at why kids are so easily scammed.



Scams are perpetrated against children and teens in nearly every popular online venue. Club Penguin, Runescape, kids gaming sites and, especially, social networks, like Facebook and MySpace, have all been used to target children and teens. Scammers also utilize popular tools such as Twitter, instant messaging and cell phones. Cell phone scams even have their own name called "cramming." (Google the words: cramming phone bills) Even newly popular games such as Facebook's Farmville are used to scam kids via manipulative and dishonest advertisements.

Children and teens, more than ever, need to be better educated how to recognize and avoid scams, and to understand how their own behavior is manipulated by these clever social engineers.

As always, we welcome your comments and suggestions. 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.

[7. Kids' Scams: The Good, the Bad and the In-Between](#) from Scambusters.org

[8. Teach your children to recognize and avoid Internet scams](#) from Scambusters.org

[9. How to spot scams targeting kids](#)

[10. Five steps to good decision-making skills for teens](#)

[11. A complete guide to avoiding online scams](#)

[12. Educational games on Internet and media literacy for ages 5 - 15](#)

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

Why Kids Can't Avoid a Good Scam

Whenever we conduct workshops with children and teens, regardless of age, we show them a variety of scams they are likely to have seen based on their age and Internet experiences. The best scams have most, if not all, of the following characteristics in common:

1. The scam is very attractive.

The graphics or photos employed are very pleasing to kids (and adults). They may contain cartoon characters, moving graphics, kid-friendly colors, "edgy" words or phrases or the suggestion/hint of being "edgy" (e.g. connecting to something potentially pornographic or violent).

Look at these images of various scams taken from kids gaming sites:

[1-PuffgamesEvonyAd1](#)

[1-PuffgamesEvonyAd2](#)

[2-WinnerAd](#)

[2-WhatHaveIWon](#)

[3-LoveCalculator](#)

[4-CursorManiaAd](#)

[5-GamevanceAd](#)

[5-GamevanceAd2](#)

The first two, found at PuffGames, give the impression that anyone signing up to play the role-playing game Evony will likely experience more scantily-clad women. Online bloggers speaking about this shameful advertising tactic have stated that the game actually doesn't contain any graphics or game-play that could be considered indecent or pornographic. The ad, of course, suggests otherwise. The second group of ads tells the viewer they have won a prize. Notice that the ad guaranteeing 5 free ringtones or \$5000 contains a timer indicating the time remaining to enter the contest. However, once it counts down to zero, it simply restarts and counts down again. In each of these cases the user is asked to give up personal information. The ringtone ad leads to a second screen that asks for a lot of personal information, including mother's maiden name. The Love Calculator ad puts the fine print in a color that is difficult to read. Most kids won't read the fine print anyway, nor notice the charges at the top of the ad that will appear on their parents' cell phone bills. The last set of ads, from CursorMania and GameVance, can actually lead to the installation of adware on the user's computer. These ads are

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 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.

Book for Parents:

[Racing to Keep Up: Talking with your kids about technology use and strategies to protect the home computer](#)

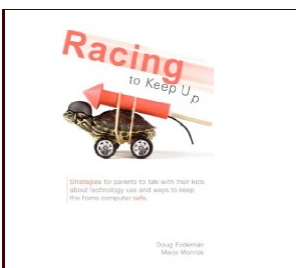
playful and two of them are even game-like themselves in order to entice and engage the viewer.

2. The scam employs an old fashioned "slight of hand" to distract the visitor/viewer from things that should make them suspicious.

The above ad with the timer counting down is a perfect example of this distraction. The timer is intended to make the viewer feel rushed into making a decision, to act impulsively, which kids are developmentally and neurologically wired to do anyway (more on that later). Another example of distraction is this scam taken from a Facebook ad recently that promises a [free MacBook Air computer](#). Whenever we ask teens to [look carefully at the full ad](#) and identify something suspicious in the ad, most are able to figure it out. First is the fine print "Free with reward offer purchases." The Better Business Bureau group that exposed this scam noted that participants were required to purchase at least \$2,500 in other goods and services before coming close to owning a laptop. Second, Apple has never produced a MacBook Air in any other color but silver.

3. The scam makes an effort to connect personally and/or emotionally with the viewer and thereby manipulate their behavior.

This form of "social engineering" is often used by malware writers to manipulate viewers into installing malware or paying for goods/services they really don't need. This category of scam includes email scams that many of us receive, such as fake notices from UPS or DHL about packages that can't be delivered (so please download the attached form to schedule delivery), or "click the link to see Angelina Jolie naked", or click the comments posted under a YouTube video saying "lol. Nice vid. Check mine out at.....". They are just tricks to manipulate us into downloading the attachment, clicking the link or visiting a website which results in a computer infection. Check out this [friend request from Emily on Facebook](#). Thousands of these are routinely sent out. This one was disseminated across Facebook with the same photo used with, at least, three different names. In each case the link led to extortion-ware. The visitor receives a popup notifying them that their computer contains multiple viruses. The visitor is further told that software can be purchased to remove the viruses. Sadly, the software actually



installs malware once purchased to remove the non-existent viruses. Perhaps the most effective scam we have ever found to manipulate the behavior of teens was this [Facebook scam that appeared in the Fall of 2007](#) and tricked thousands of teens into infecting their computers with malware and giving up their login credentials to personal accounts such as Facebook. Facebook account holders were told told by a "friend" (who's account was hacked into) that "OMG, there are these pictures of you on this website! You better check them out"! The trick made the recipient feel that the photos were personal and possibly embarrassing.

Reasons why children and teens are vulnerable to scams:

a) Poor decision-making skills: Kids have difficulty making good decisions. That is, in fact, part of growing up. As they grow up and mature they learn how to make better decisions. They learn, for example, how to delay decisions that may be more self-gratifying for decisions that may be healthier, the "right thing to do", or that postpone gratification. Neurologists have understood this for some time now. Generally speaking, brain maturation occurs back to front. The frontal lobe of the brain is the last portion of the brain to mature. Yet the frontal lobe is the seat of higher-order thinking, critical analysis and decision-making skills. The frontal lobe doesn't fully mature, on average, until we are in our twenties.

b) Impulsiveness: Any parent can tell you that kids are impulsive. They act without thinking ahead about the possible consequences of their actions or the impact of their decisions.

c) Too trusting: Kids tend to be very trusting of others on the Internet. Though they routinely lie online, they often believe what others say to them. This is, in part, because they want to connect to others so much. This is especially true of teens.

d) Naivety: While kids may be extremely savvy HOW to use the Internet and technology, it doesn't mean they can easily recognize scams, subterfuge and manipulation. They are still, after all, children of various developmental levels of maturity.

Adults need to help kids think critically about what they read and see online. Schools should consider incorporating age-appropriate education around these and related topics such as media influences in their life. Their world, and ours, is changing. It is our obligation as parents and educators to help prepare them for life in the virtual world.

INTERNET SAFETY CURRICULUM

Safe Practices for Life Online

Children Online has a curriculum 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](#)

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

[Forward email](#)

✉ [SafeUnsubscribe®](#)

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