Social Networking CHALLENGES

Every Parent Should Know

by [Content] Watch® makers of

Net Nanny social℠

www.netnanny.com
801-508-3600
marketing@contentwatch.com
6949 S. High Tech Drive,
Midvale UT 84047

This document provides parents with information on the challenges associated with kids spending time on social network sites.

PANDORA internet radio

tumblr.

flickr

myspace

photobucket

orkut

ISSUES Discussed in This Report

- State of the Social Network Union
- Big Challenge
- Self-Esteem
- Age Differences
- Cyberbullying
- Hiding Behavior
- Other Social Networks
- Privacy
- College Admissions
- Depression
- Predators
- Online Criminals
- Dangerous Friendships

Opinions expressed in this booklet are of ContentWatch—makers of Net Nanny.

State of the Social Network Union

74% of households have the Internet at home.

54% of kids between 8 and 15 have a social networking profile.

50% of parents with kids between 5 and 15 feel like their kids know more about the Internet than they do.

41% of kids go online in their bedroom.

41% of adults believe that content online is regulated.

35% of kids aged 12 to 15 own a smartphone.

Big Challenge

Parental control software usage dropped from 43% in 2009 to 37% in 2010.

Parents who don't have parental controls say they either closely monitor Internet usage or just trust their kids to follow the rules.

This fact is precarious since kids know more about the Internet than their parents.

Self-Esteem

This occurs when the person who logs on to Facebook experiences a self-esteem boost by using their profile to affect how others see them online.

However, another study suggests that Facebook leads users to feel dejected and worthless, because they constantly compare themselves to their online friends and to others, including high-profile personalities.

Challenge

Parents need to keep their finger on each child's pulse. Everyone reacts differently, but it's certain that social networking can have an effect on mood. Most kids won't talk about these things with a parent. Please talk to your children and ground their self-worth on real family relationships, not fake online social interactions.

Age Discrimination

Facebook's user policy clearly states that no one under 13 should create a profile on the site – but preteens everywhere are doing it anyway. Facebook envy is real.

In 2011, Facebook said that an average of 20,000 underage Facebook accounts are shut down daily. But 3.6 million underage users in the U.S. are on Facebook each month.

Challenge

If an 11-year-old signs up and represents that she is 13 years old, then in five years when she is 16, she will start getting articles and ads that are "adult" in nature. Facebook would assume by then that she is 18 and policies allow for different material to be served to adults.

Part II of the same challenge: Once a person turns 18 years old, Facebook can make her profile public to adults. That means solicitations and contacting from strangers can begin.

Part III of the same challenge: A group at NYU-Poly created a list of high school students' profiles at three schools by using one student—who was shown as an adult because she lied about her age on Facebook. Information included full names, locations of hometowns and high schools, grade-levels, and profile pictures. This minimal data could be used to gather even more data, such as parents' names, street addresses, and phone numbers.

Luckily, the NYU-Poly study was conducted by a respectable university.

However, the not-so-good-guys interested in this type of data are data collectors, advertisers, malware makers, and even sexual predators, who could stalk and hurt minors using the information gathered in the attack.

Cyberbullying and Fighting

Social networking sites create a platform for cyberbullying. There are many ways that cyberbullying can occur. Over half of teens with a social network account have experienced negative consequences.

Cyberbully Stats

Arguments - 35% of teens argue with friends online. Most kids don't tell a parent about these things.

Ending Friendships - 20% end friendships resulting from online interactions.

Unsafe - 7% of teens fear for their safety and don't tell a parent about it.

Fist Fights - 4.5% of teens get into physical fights over issues related to online interactions.

One study says 15% of teens have hacked into another person's social network account.

Challenge

Fake Account - A classmate (bully) of a 12-year-old girl named Chelsea created a Facebook account for Chelsea and then added friends from school. The bully added pornographic content to Chelsea's Facebook page. As a result, Chelsea started getting questioned by her classmates about her behavior.

One Net Nanny customer wrote in:

> I received a phone call one night from a neighbor. She told me to get on Facebook because a pornographic video was displayed on my 15-year-old daughter's page.
>
> I was shocked. I logged on and did find a pornographic video on her page. It even had thumbs up suggesting she liked it.
>
> Distraught and confused, I turned to my daughter and asked "Did you post this!?"
>
> Of course, my daughter, with tears in her eyes, said "No, Mom. I would never!"
>
> Her Facebook page had been hacked.

Cyberbully Methods

- *Upload videos* to YouTube that embarrass their victims
- *Create fake Facebook accounts* acting as a victim, but in a negative light
- *Pretend to be a victim* in chat rooms, acting in embarrassing ways
- *Share the victim's personal information* in a public forum
- *Post rumors or lies* about the victim in a public forum
- *Share embarrassing pictures* of the victim in a public forum or through email
- *Use text messages, instant messages, or emails* to send mean or threatening messages

Hiding Online

Since kids are more knowledgeable with technology than their parents, many parents give up trying to keep up because they don't know how to monitor online behavior.

70% of teens hide their online behavior.

Challenges

What are teens doing?

- 48% look up answers online
- 43% access simulated violence
- 36% access sexual topics
- 32% access nude content or pornography
- 31% access pirated movies and music
- 16% look for test answers on their phone

Parents are oblivious to the things their kids are getting away with—77% of parents say they are not very or not at all worried about their teens cheating online and 74% trust their teens to not access age-inappropriate content online. The stats say otherwise.

The "Other" Social Networks

A recent survey showed Tumblr is slightly more popular now than Facebook among the 13 to 25-year-old crowd with 59% using it regularly and 54% using Facebook regularly. Tumblr was first conceived as a blog site, but it's mainly used by teenagers now for re-posting cool photos. Some teens don't even know that you can post text on Tumblr.

Challenge

Parents might get focused on monitoring Facebook but forget about other social network sites such as Google+, Pinterest, Twitter, or LinkedIn.

Having to monitor multiple social network sites can seem like a daunting task. What can parents do? Try a "social network monitoring" software program such as Net Nanny Social [shameless plug].

Social Network Privacy?

Social networks make money on advertising. Period.

Therefore, social network privacy is really an oxymoron. Social network sites sell data about users to advertisers and others. Most social network sites say they don't sell individual data, but just aggregate data.

Challenges

Your teen can be targeted for inappropriate ads because of “dumb stuff” he chose to casually “like” years ago when not really thinking about consequences.

One teen we know, now an adult, was contacted by his mother who saw something on Facebook that suggested her son was a fan of a very inappropriate product. The son had no recollection of the issue. The ad was based on a ‘like’ from years past on a somewhat related product.

Suggestion

Talk with your child about their privacy settings on Facebook and other social networks. Make sure settings are set to the strictest level.

In addition, parents should consider monitoring a child’s activity on social networking sites, because no amount of privacy settings can prevent a teen from sharing too much information in a wall post or private message.

Want to go to College?

It’s important to be cautious about things a teen posts. You never know who’s watching, including the college admissions board and potential employers.

Challenge

Kaplan conducted a survey in 2012 that revealed that colleges are looking at prospective applicants’ online presence, including Facebook and Twitter.

Not surprisingly, college applicants who post inappropriate things are more likely to be rejected.

Suggestions to manage your social media footprint:

- *Search for yourself* on Google to see what comes up. Then fix it.
- *Limit your profile searchability* – make yourself viewable to friends only.
- *Keep your profile photo appropriate*. (Enough said.)
- *Control who can contact you* – allow “friends of friends” and not everyone.
- *Remove past posts and comments* from public view.
- *Take control of tagging* on your profile and don’t allow friends to tag you.
- *Filter your Friends network* by setting up a list for friends and another for others with different settings.
- Make your account permission-only if possible.
- Change your online handle or name to avoid direct correlation with you.
- Be smart and think about everything you post online before you do it.

Depression

Teens and kids spend an inordinate amount of time connected to digital devices.

Challenge

According to recent studies, depression among college students has risen, with a correlation to excessive Internet usage. There was a 56% percent rise in depression among college students within the last six years.

Students with depression use excessive amounts of Internet, more than an average student without depression.

This resonates personally in terms of using social media as an outlet to cope with depression. One student said, “My Internet usage is actually pretty ridiculous. I know when I’m feeling extra down, I’d rather sit around and check Facebook over and over again, knowing that there’s nothing exciting going to happen.”

Suggestion

Monitor Internet usage and social media usage but, more importantly, talk with your child.

Sexual Predator Playground

An investigative reporter, Chelsea Schilling from web site WND, went undercover to reveal the dark side of social networks, specifically Facebook.

She created several fake female profiles, all of which appeared promiscuous or flirtatious.

She then searched through profiles to find “friends” with similar inappropriate interests, those who openly receive explicit pictures and those with fan groups of certain sexual activities.

She “friended” these people – the most dangerous and perverted Facebook members. Once they were friends, she accessed their photo albums. They were filled with illegal pornographic images.

Facebook is the playground on which countless children spend hours a day or week and it’s frequented by predators ready and willing to harm and exploit.

Parents have to monitor their child’s activity.

True Story

At ContentWatch, we indirectly observed this Facebook-friend-gone-awry scenario.

One of our software quality assurance testers (we will call Michael) created a Facebook account for a fictional girl, Savannah, with a provocative photo in a bikini. Her Facebook profile says she’s just turned 14 years old.

We used the account for testing the integration of Net Nanny with Facebook.

We did not actively update the page. To satisfy curiosity, Savannah (or Michael) accepts all "friend" requests, and there have been almost 700. Savannah never posts comments or replies to messages.

Within a few months, this Facebook wall was littered with inappropriate comments from "friends" and non-friends. There were hundreds of private messages with vulgarity and sexual content. Sadly, many of these "friends" were men in their 30s, 40s, 50s and 60s.

The moral of the story: parents must be aware of their child's Facebook use because there are hundreds of potential "friends" looking to contact and lure a child into dark and scary places.

How Criminals Use Social Networks

With more than 1 billion users, Facebook is the largest social networking web site. If you think about it, 1 billion users is more than three times the population of the U.S.

With that many people, there are bound to be problems.

Challenges

Roughly 20 percent of Facebook users have been exposed to malware and 600,000 reports of hijacked log-ins occur every day at Facebook.

Criminals do the following:

1) **Hacking into accounts** (figuring out user name and password): once hacked, an account can be overtaken and used as a platform to deliver spam or it can be sold.
2) **Commandeering accounts** (log in as the person): Using sophisticated password guessing software, the criminal logs in and has the victim's entire friend list at their disposal – and a trusted cyber-identity. The impostor can use this identity for a variety of confidence schemes, including the popular "London Scam" in which the fraudster claims to be stranded overseas and in need of money to make it home.
3) **Profile cloning** (creating an account exactly like someone else): the crook will then send friend requests to the victim's contacts who will likely accept since the request appears to be from someone familiar. Once accepted, the crook has access to the target's personal information, which can be

used to clone other profiles or to commit fraud.

4) **Cross Network Profile Cloning** (create a user account exactly like someone else, but on another social network): the abuse of such accounts is described in #3 above.

5) **Phishing**: the hacker poses as a respected person or group and asks for personal data, usually via a wall post or direct message. Once clicked, the link infects the users' computers with malware or directs them to a website that offers a compelling reason to divulge sensitive information or to send money.

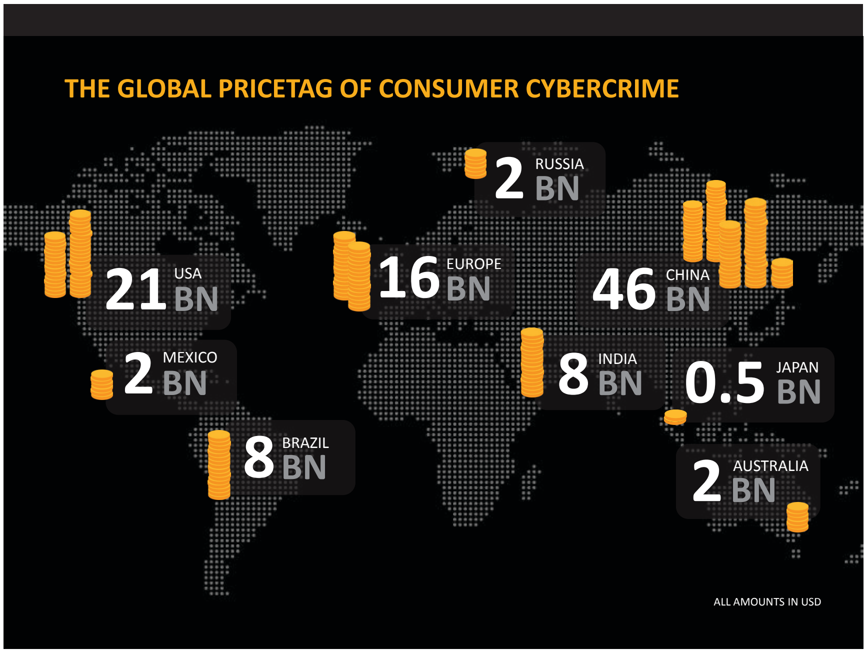
6) **Fake Facebook**: a common form of phishing; the scammer directs users via some sort of clickable enticement, to a spurious Facebook log-in page designed to look real. When victims enter usernames and passwords, they are collected in a database, which the scammer will sell. Scammers can take advantage of their assumed identity through apps like the Facebook Marketplace to buy/sell a laundry list of goods and services.

7) **Affinity Fraud**: con artists assume the identity of a person to earn the trust of those close to them. The criminal then steals money or information. Facebook facilitates this fraud because people end up with "friends" they do not know but seem to trust. Criminals infiltrate a person's group of friends and then ask for sensitive info or offer deals or investments that are part of a scheme.

8) **Mining Unprotected Info**: users frequently reveal their emails, phone numbers, addresses, birth dates and other pieces of private data. Hackers use this info as passwords or as answers to secret security questions. The majority of unprotected information is mined for targeted advertising but can be a means to more pernicious ends such as profile cloning and identity theft.

9) **Spam** (mass sending of ads to users' personal accounts): social networking sites allow for a new kind of spam called *clickjacking*. Clickjacking, which is illegal, involves the hacking of a personal account using an advertisement for a viral video or article. Once the user clicks on this, the program sends an ad to the person's friends through their account.

Parents need to be aware of these tricks and teach kids about them. Don't wait until you are victimized.



Friendships that Lead to Assault

Teens and children are inherently trusting. Social networks are full of users posing as someone or something other than their real identity. These users are proficient at creating friendships of trust and using common language.

Once a friendship is formed and trust is created, a face-to-face meeting is set up.

Challenge

There are countless horror stories of this type of scenario going wrong. Typically, these encounters are between adults and children. Some sexual predators will travel cross-country to engage in these types of meetings.

Even after a child is harmed, sometimes the meetings are repeated due to fear on the part of the child.

Solution

Parents need to have open communication with their children and, more importantly, monitor all 'friend' requests on a child's social network.

While the pace of technology requires us to be ever-vigilant about new online threats, the ultimate solution is to have a great relationship of trust with our children. Frequent, heart-felt and non-judgemental conversations are the best vehicles for protecting our loved ones. Though sometimes difficult and time-consuming, there is no better solution to keep a family safe and intact.

At ContentWatch, our mission is to protect families, and while we are all in the business of raising families, every bit of help, advice and sharing is needed in today's digital village.

Feel free to share this report with everyone.

– Your ContentWatch Friends

As a courtesy, please notify us at marketing@contentwatch.com to let us know you are doing this; this will let us inform you of other resources.

Sources:

- CNN: Survey: 70% of teens hide online behavior
- Huffington Post: Facebook removes 20,000 Underage Users Every Day
- Kaplan: 10 Ways To Manage your Social Media Footprint
- The Post: Internet usage could be directly related to depression
- WND: Facebook: Child Predator Playground
- 24/7 Wall Street: 9 Major Ways Criminals Use Facebook
- TechEye: Kids give their parents the runaround online
- CDC: Cyber bullying Methods, 2011
- Norton: Cybercrime is a Global Problem; Increasingly Social and Mobile (2012 Norton Cybercrime Report)