

What's Really Happening on the INTERNET

WHAT EVERY PARENT MUST KNOW

by Philip M. Rosenthal

“I apologize for the shock value here, but this article needs to shock ...”

This is my second article in NCYI Viewpoint magazine (Part I appears in Viewpoint, Winter 2006) regarding a topic that is arguably one of the most important issues for parents and families to deal with in this generation. As little as ten years ago, there was really no such “worry” about Internet Safety. Today, the almost daily headlines blast the latest arrest for child pornography or a predator preying on unsuspecting children.

In my last article, I told the story of a fictitious young girl (actually me, working undercover) that resulted in an arrest of a 54-year-old individual who thought that he was going to realize a demented and sick fantasy. Instead, he got to go to prison. That story had a happy ending because there really was no young girl, it was just me (B”H). It could have been your daughter or son.

In this article, I want to address some of the safety issues more in depth and suggest some very concrete tips for helping to minimize our children’s exposure to the perils of sharing too much information on the Internet. Without exaggeration, this information could save your child’s life. And lastly, please do

not think that these issues are only in “the outside world”. These problems have arrived in the Orthodox Jewish com-

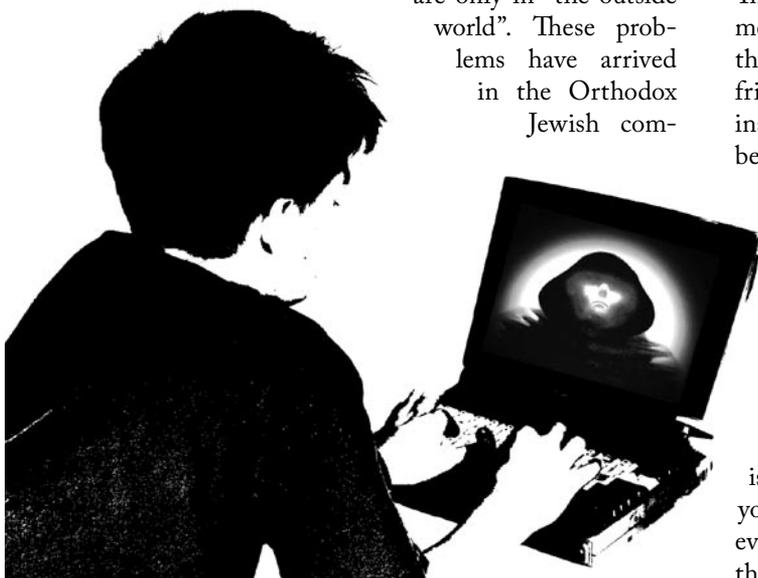


munity at cyber speed. We are most definitely not immune. Share this information with your friends and relatives. Just because your house is protected doesn’t mean that your children aren’t exposed at someone else’s house, the library, internet café or even on the school bus using their cell phone.

INSTANT MESSAGING

So, let’s jump into it. Your kids live for one thing today. IM’ing, or Instant Messaging. It is why they get out of bed. What used to be passing notes in school or sitting on the phone at home “yakking,” is today, online or on the cell phone text messaging endlessly. The average child spends upwards of 15-20 hours a week IM’ing. Most kids are using AOL Instant Messenger to do this. As I travel around the world speaking, I always ask students by way of raising hands, how many “Buddies” they have in their Buddy List. I think you will be as shocked as I am when I tell you that on average kids have in excess of 200-300 people listed as Buddies. I travel to locations all over the world on a regular basis and know people on at least three continents, and I can tell you that I don’t have 300 friends. So how can your child have that many friends? They don’t. What they do have, are 300+ people that they have met as referrals from other friends, some of whom “referred” themselves. Children have a misconception that “my friend’s friend is my friend”. This is very dangerous. I can very easily insinuate myself into one IM and then almost immediately be referred to other kids because I am “cool”. In a matter of

hours or at the most, days, I am now in any number of kids’ Buddy Lists. If I were to then ask any one of these kids who that person is, they would tell me that they know me and that I am a friend of one of their friends. When I speak, I explain that no one should be in your Buddy List that you have never actually met face to face. (That, of course, doesn’t mean to meet some stranger.) I am talking about a friend from camp or school or a relative, etc. A friend referred from a friend doesn’t count. That is simply a stranger and should be avoided. **Tip #1:** Check your child’s Buddy List and have them break down to you every person in their list. Make them get rid of anyone that they cannot identify to your satisfaction. Also understand that



they can use their cell phone to Instant Message as well. It is not limited to the computer. Cell phones can use AOL, Yahoo, MSN, etc. for chatting. This is in addition to plain text messaging.

CHATROOMS – DIFFERENT TYPES

There are many different types of chatrooms that your kids can get into. I will skip over some of the more esoteric ones in the name of brevity for this article. We will focus on mainstream stuff here. When someone enters into AOL, Yahoo, MSN, etc., they can do one of a few things. They can simply send an IM (Instant Message) to someone in their Buddy list, they can send an IM to someone that they have looked up who is another member of that particular service, or they can enter into a chatroom. A chatroom is a public place listed as one of literally thousands, by topic. Some of those topics may seem harmless, like Jewish Teens Only or Bais Yaakov Girls Only. Other chatrooms may be listed as Bondage for Hire, Married Females Seeking Married Males, etc. **I apologize for the shock value here, but this article needs to shock, unfortunately.** Then there are private chatrooms. These private rooms are set up in real time by a couple of people who want to make what is essentially a conference call via



the keyboard. Two or more people can do this and no one can get in except for those who were invited. If your child is chatting with their approved buddies in this manner, then that is fine. Anything else (chatrooms, that is) is totally unacceptable. Let me assure you that just because the chatroom says Bais Yaakov Girls Only, means nothing. A predator will be drawn to that room like bees to honey. Public chatrooms cannot be limited and cannot be made private. Only a private room can be made private and they do not by their nature have names associated with them since they are done in real time and are temporary. **Tip #2:** Find out what chatrooms, if any, your kids are using and STOP them from future use.

PRIVACY

The previous discussion really leads us to a much bigger topic: Privacy. When you post things on the Internet, you really do not have any privacy. Certainly, there are ways of storing, sending or receiving secure items, but that is not the intent of this article. When you post a picture or text on the Internet, no matter where (i.e., MySpace, AIM, etc.), that is then subject to being resent and distributed all over the world. I recently worked on a case where a student was punished by his teacher. In order to “get even,” he went onto the school’s website and downloaded a picture of the teacher. He then downloaded another picture of a woman that, let’s just say, didn’t show her in her best form. He then superimposed the face of the teacher onto the body of the other person and posted this on the Internet while also printing multiple copies and distributing them all over the school. That picture will float around the Internet forever. The point here, of course, is that you should never post anything on the Internet that you wouldn’t want the whole world to see. I have a website that advertises me as a public speaker on the topic of Internet Safety. I want as many people as possible to see it (www.philiprosenthal.org). What I didn’t do on that website was put anything personal about myself or my family. To do so would expose my family to ANYONE with Internet access. If I were to shut

down that website as you read this, the information will still be available basically forever. There are actually companies that do nothing but copy and archive websites for historical or other purposes. **Tip #3:** Be extremely careful about what you post or send out on the Internet. It could come back to haunt you or your family.

MYSPACE

There is no doubt that MySpace is the single most dangerous website available today. For those of you who do not know about it, I will give a brief description. A number of years ago a couple of young entrepreneurial young guys decided that they wanted the world to be able to read about them and the music they played. Since they had no recording contract, they decided to program a website that would allow people to find out about them and any other like minded musicians. In no time at all, the website expanded and it became what is now called a social networking website. People go there and create profiles of themselves, to be shared with any and all people who are members. As of today, there are over 100 million users. Recently, Rupert Murdoch bought the company for millions of dollars. Ask any kid today and they will tell you (if they are honest) that it is their life. By its nature, it drives a member to try to be “friends” with as many people as possible. A person’s profile can be “private,” however, that is somewhat self defeating. If your profile is private then people cannot find you and therefore you don’t get new friends. Imagine this website from the perspective of a sexual predator. It is like shopping at a super center for them. **Tip #4:** Get rid of any and all MySpace accounts.

XANGA and FaceBook are similar websites. Follow the same advice as above.

SELF-PORNO

It’s one thing that our kids are living online in places like MySpace, FaceBook, AIM, etc. Because these young people seem to think that they are both anonymous and invincible, they do some pretty thoughtless things. One of those is posting nude or semi-nude

photos of themselves online. Please, please, please don't shrug this off and say, "Oh, not my child." I could shock each and every one reading this article out of their collective minds with some of the pictures I have seen of some of your own sons and daughters from the frum community. I am not talking about the "modern" only. I am talking about Chasidish, Yeshivish, Chabad, Litvish, Young Israel, nobody is immune here. I do not understand the dynamic that leads our children to do this, but it is rampant. Please understand, I am not telling you to start mistrusting your child. I am simply telling you that this is happening more than any of you can imagine.

Tip #5: Research software programs that track your internet use. I recommend eBlaster and BeSafe Net; there are others. [Check my web site for more information, www.philiprosenthal.org] It would please me beyond words for you to contact me and tell me that I don't know what I'm talking about. Unfortunately, I do know and that is why I implore you to act on this.

BLOGS/BULLYING

The newest form of keeping up with the news these days is via blogs. Imagine when you go to the grocery store. As you enter the store there is a bulletin board on the wall and essentially anyone can post almost anything there. Let's say you stop to read what was posted there and then decide to write your own comments next to it. As other people enter, they also add their thoughts. This is what a blog is. All in all, it is not a bad thing. The problem arises when your children (or adults for that matter) use the blog for purposes that are hurtful. When we were younger we all remember the schoolyard bully. Today that same mentality exists, but it exists online. Kids are bullying each other via blogs, email, chatrooms and other means. It has become so bad that there have been documented suicides because of it. So, here is **Tip #6:** If you have noticed that your child has become withdrawn and isn't socializing as much as usual, talk to him or her. If you suspect that they are being bullied, get them some counseling, immediately. If, on



the other hand, you suspect that your child is being a bully, for sure get them some counseling. This is an absolutely unacceptable behavior.

ID THEFT, FINANCIAL FRAUD

This subject can make up an entire article by itself. I will address some basic tips to help minimize your risks of identity theft.

Doing an online credit card transaction is really no more dangerous than standing at the counter in your favorite store and giving the clerk your credit card. Let me explain. Your store hires people to work for it and hopefully only hires trustworthy employees. The problem that can arise is if the clerk is dishonest. If so, when you give them the credit card there are a number of ways that your credit card information can be stolen. It is wise advice to watch everything the clerk does with your card and make sure you get it back. How many of us go to a restaurant and trust the waiter to walk away with the card and come back later for a signature. It is simple for them to scan your card while they have it and then return it to you without you suspecting a thing.

So, how does that work on the Internet? As long as you do your transaction on a website that uses SSL (Secure Socket Layer), your transaction CANNOT be snatched out of the air. It is really encrypted so well that no one can get it. However...that is only while the information is traveling from you to

the company that you are buying from. Once the information gets there, you are just as susceptible to an unscrupulous employee as you were at the store itself. But, at some point you have to trust someone. Therefore, I state here that most mainstream online companies could not possibly stay in business very long if their employees were ripping people's credit card numbers off. I can tell you that I do all of my banking and 99% of my bill paying online. I regularly buy items online and I even sell some of my collector's items (old junk) on eBay, occasionally.

There are two things to watch for when doing an online secure transaction. First, when you get to the screen where they ask for your credit card information, look in the line where you type www, etc. You should see the following: <https://>. Make sure that you see the "s" after the http. The reason is that that means Secure. If it doesn't say that, then do not complete the transaction. At the same time, look at the bottom right corner of your screen. You should see a small gold colored lock there. Again, if you don't see that, do not do the transaction. Actually, if you don't see both of these things, you should not complete the purchase. Some hackers have found a way of putting up a fake screen that makes you think that the <https://> is there, but luckily, they haven't found a way to put that and the lock there. So, again, if you don't see both the <https://> and the lock, shop somewhere else.

Needless to say, you should never give out any of your personal information on the phone. Likewise, you shouldn't just throw the credit card offers in the garbage. Go to your local office products store and buy a cross-cut shredder for \$30 and grind those endless offers into confetti. People will go through your garbage, steal those offers and apply for credit in your name.

Tip #7: Get your credit bureau reports and look them over. In New York State and most others, you are entitled to one free copy of each of your reports once a year. Here are the three credit reporting company's websites. Go there and get your reports right now.

www.experian.com

www.transunion.com

www.equifax.com

You will have to dig around a bit to find how to get the free one, because they want to sell you the subscription. Don't waste your money. Get the free one. It's there you just have to look for it.

If you find that you have been violated, call your local police and report it. That's what you pay them all of your tax money for. Besides, they can't catch any bad guys if you don't call them and tell them what happened.

CELL PHONES

This discussion has centered mainly on computers and the internet. I want to point something out to you. The cell phone that your child "had to have," is also an internet access device. They can surf the internet, chat with anyone, take pictures of themselves or others and generally do almost anything that they could do on the computer. I will save the overall discussion for the future, but please take heed to this: Your children are sitting up until 2 and 3 o'clock in

the morning chatting with their friends via the cell phone. Teachers are complaining that the kids are falling asleep in class. It isn't because they are up late doing homework. So, here is my last tip for this article: **Tip #8:** Put the chargers for the cell phones of your house in your bedroom. Make your children leave their phone in your room at night and they won't stay up all night getting into who knows what.

So, in a nutshell, become knowledgeable about the following and take the advice offered above :

- #1 Buddy List
- #2 Chatrooms
- #3 Personal Privacy
- #4 Social Networking (MySpace, FaceBook)
- #5 eBlaster and BeNetSafe
- #6 Blogs and Bullying
- #7 Credit Bureau Reports
- #8 Cellphones

I have tried to provide you with what I know to be very practical and helpful tips on minimizing your family's exposure to the perils of the Internet. It is

by no means a total solution. There is no total solution. If you rip the internet out, you are forcing your children to go underground. If you don't institute these things you are putting their lives in jeopardy. There has to be a middle ground. The most important tip I can give, I have saved for last. Be a parent. The internet is not your babysitter.

If you would like to arrange to have me come and speak in your community or your child's school, please contact me via my website www.philiprosenthal.org.

Philip M. Rosenthal has worked in the hi-tech world of computers for over twenty-three years. During his tenure with the Rockland County Sheriff's Department, he has investigated and solved numerous cases involving intrusions, encryptions, industrial espionage, hacking, child pornography, identity theft, financial fraud and hate crimes. Rosenthal is an internationally recognized expert in the field and has worked with numerous Federal and State agencies investigating computer crime.

Instant/Text Messaging Shorthand Dictionary

^URS Up Yours
 143 I Love You
 2NITE Tonight
 404 I Haven't a Clue
 411 Info
 4ever Forever
 A/S/L/P Age/Sex/Location/Picture
 ALAP As Late As Possible
 ASL Age/Sex/Location
 BB4N Bye-Bye for Now
 BM Byte Me
 BRB Be Right Back
 BT Byte This
 BTW By The Way
 CRS Can't Remember Sh**
 CUL8R See You Later
 EWI E-mailing While Intoxicated
 F2F Face-to-Face
 FF Friends Forever
 FOAF Friend of a Friend
 FWIW For What It's Worth
 FYI For Your Information
 GR8 Great
 HAK Hugs and Kisses
 Hugz Hugs
 IMHO In My Humble Opinion
 IWSN I Want Sex Now
 IYQ I Like You

KEWL Cool
 KPC Keeping Parents Clueless
 LHOS Let's Have Online Sex
 LKTR Little Kid in the Room
 MorF Male or Female
 MSNUW Mini-Skirt No Underwear
 MYOB Mind Your Own Business
 NAZ Name, Address, Zip
 NIFOC Nude in Front of the Computer
 NOYB None of Your Business
 OTP On the Phone
 P911 Parent Alert
 PAL Parents are Listening
 PAW Parents are Watching
 PIMP Peeing In My Pants
 PIR Parent in Room
 PITA Pain in the Ass
 POS Parent Over Shoulder
 POP Parent on Patrol
 ROTFL Rolling on the Floor Laughing
 SMAIM Send Me an Instant Message
 SorG Straight or Gay
 STM Spank the Monkey
 STR8 Straight
 SUP What's Up
 TDTM Talk Dirty to Me
 TLK-2-U-L-8-R Talk to You Later
 TM Trust Me

TOY Thinking of You
 TTFN Ta Ta for Now
 TTYL Talk to You Later
 U You
 VM Voice Mail
 WAYD What Are You Doing ?
 WAYN Where Are You Now ?
 WDYT What Do You Think?
 WE Whatever
 WTGP Want to go Private
 WU What's Up?
 WUF Where You From?
 WWY Where Were You?
 WYCM Will You Call Me?
 WYP What's Your Problem?
 WYRN What's Your Real Name?
 WYT Whatever You Think
 WYWH Wish You Were Here
 XME Excuse Me
 XOXO Hugs and Kisses
 YDKM You Don't Know Me
 YGBK You Got to be Kidding
 YGBSM You Gotta Be Sh**ing Me
 YOYO You're On Your Own

WE APOLOGIZE FOR THE SHOCKING LANGUAGE - WE DELETED SOME OF THE WORST - BUT UNFORTUNATELY, YOU NEED TO KNOW THE REALITIES OF THE INTERNET.