What is Really happening ON THE INTERNET

a head's up to parents

by Philip M. Rosenthal

I am not your typical Jewish boy. I didn't go to law, medical, business or accounting school. I did go to college, but I ended up doing something totally different than anyone, including myself, expected. I hope that I have your attention by now. I went into Law Enforcement. Specifically, I went into a new area of Law Enforcement called Computer Forensics. I know, you are asking, "A cop!? What kind of a job is that for a nice Jewish boy?" Don't worry, my mother keeps asking me the same thing. It is, however, a worthy profession. I am one of what is becoming a growing specialization in the field of Law Enforcement. When I started, there were less than a handful of others like me. Of course, the only Jewish ones were in Israel, but that's a story for another time.

Most of you associate forensics with a crime scene detective lifting fingerprints or DNA off of a doorknob or glass at a bank robbery or murder. My job is really no different. I lift electronic fingerprints and electronic DNA off of hard drives and other electronic storage media. There are many types of computer crimes that I investigate, but for the sake of this article I am going to concentrate on the one that is plaguing everyone today including the Orthodox community. I used the word plaguing, and I meant it.

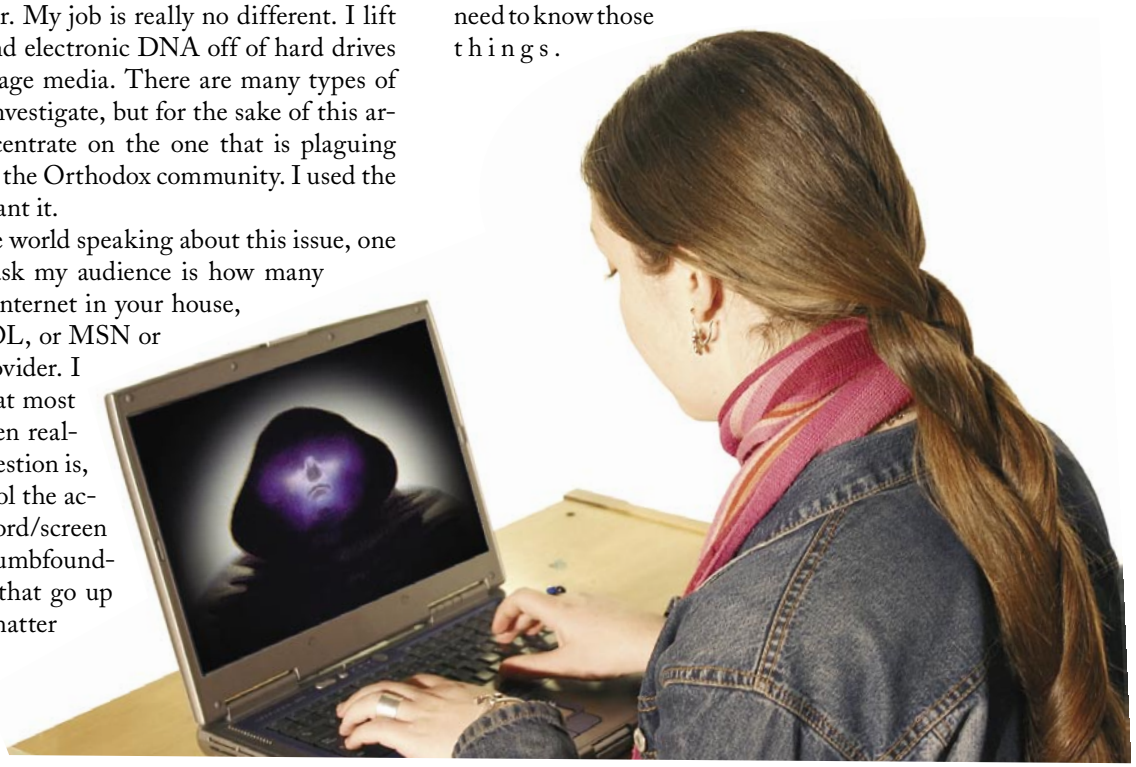
As I travel around the world speaking about this issue, one of the first questions I ask my audience is how many of you have high speed Internet in your house, how many of you use AOL, or MSN or some other front-end provider. I then ask the question that most parents don't seem to even realize is a problem. That question is, "How many of you control the access to the Master password/screen name?" I am absolutely dumbfounded by the lack of hands that go up in the gathering. As a matter of fact, I am shocked by how many parents don't even know what I am talking about when I ask that question. (See sidebar.)

So, here goes:

I am Shosh14. I have long brown hair, my favorite music is Weezer and I go to _____Hebrew Academy. My hobbies are getting my nails done, shopping, shopping, hanging with my fav peeps and shopping. If I'm not shopping, I like to go to the mall.

My parents r boooorng and WAYY 2 restctv. BoySs r most imprtnt and if u don't agree then ur just stupid.

Do you know what the above is? It is called a profile. Now AOL, MSN, etc. have a freeform area that people use to fill with all sorts of personal information about themselves. This space has NO redeeming value. We will discuss this in more detail, but suffice it to say that your kid's friends already know those little tidbits about them and the strangers in the world don't need to know those things.



Make your child get rid of this profile now.

In addition to this profile, there is a website called Myspace.com. It is possibly, in my opinion, the single most dangerous website in existence today. Ask your child if they have a Myspace profile. I bet they do if they are over 12. The website requires that you be 14 or over, but kids will defy that rule. This site allows you to put, not only personal information on there, but pictures as well. Go to www.myspace.com and see for yourself. When you get to the site do a search and look for any name you can think of. I don't think that I have to tell you any more for you to take measures to get your kids off this site immediately.

I recently worked on a case where a 15 year-old girl, "Devora," [names are changed for privacy] had her profile on myspace.com. While she was out shopping, one of her "friends," "Rachel," with whom she had just had a fight, went online and logged on to Devora's profile using her name and password. Rachel totally changed Devora's profile to one of a rabid racist, complete with accompanying anti-Semitic rhetoric, swastikas and other Nazi-related icons. Devora had no idea that this had happened and was more than surprised when the next day at school, she was met with threats of death and all sorts of physical harm. The school was required to provide her with protective escorts to class until the problem could be sorted out. Luckily, we were able to trace the culprit and solve the case, but not before this young girl was scared to death for no good reason. The lesson here: Don't share your password with ANYONE, EVER!!

Now back to the profiles. Part of my job is to go online and pretend to be a young person. First, I go to one of these services and create a screen name and profile. Then I sit and wait. It doesn't take more than a few minutes for someone to come knocking at my (electronic) door. One case in particular, the predator turned out to be a 53 year-old lawyer who proposed that I run away and live with him in Florida. Of course, he didn't just start out by making this proposal. First, he "groomed" me for three months, thinking that he was building and establishing my trust in him. He wanted to make sure that I felt so protected by him that I would not hesitate for a moment to run away with him. Imagine for a moment what would happen if I had actually was a young child and actually ran away with this man. What do you think would happen after I was there and had fulfilled his warped fantasy? Surely, he wouldn't send me back home to Mom and Dad. He couldn't. Even though this guy is sick, he understands that he can't send me home. At the very best, my eternal memory would be on the side of a milk carton under the words, "Have you seen this girl?" Most likely, of course, I would end up in a 50-gallon drum, well hidden behind a Kmart or a Wal-Mart somewhere, never to be heard from again.

So, how is it possible that all of this is going on right under parents' noses? Simple, it's not under their noses. How many of you let your children have

How Can You Minimize the Chances of Your Child BEING VICTIMIZED:

- Communicate and talk to your child about sexual victimization and potential on-line danger.
- Spend time with your children on-line. Have them teach you about their favorite on-line destinations.
- Keep the computer in a common room in the house, not in your child's bedroom. It is much more difficult for a computer-sex offender to communicate with a child when the computer screen is visible to a parent or another member of the household.
- Utilize parental controls provided by your service provider and/or blocking software. While electronic chat can be a great place for children to make new friends and discuss various topics of interest, it is also prowled by computer-sex offenders. Use of chat rooms, in particular, should be heavily monitored. While parents should utilize these mechanisms, they should not totally rely on them.
- Always maintain access to your child's on-line account and randomly check his/her e-mail. Be aware that your child could be contacted through the US Mail. Be up front with your child about your access and the reasons why you need to have it.
- Teach your child the responsible use of the resources on-line. There is much more to the on-line experience than chat rooms.
- Find out what computer safeguards are utilized by your child's school, the public library, and at the homes of your child's friends. These are all place, outside your normal supervision, where your child could encounter an on-line predator.
- Understand, even if your child was a willing participant in any form of sexual exploitation, that he/she is not at fault and is the victim. The offender always bears the complete responsibility for his or her actions.
- Instruct your children:
  - To never arrange a face-to-face meeting with someone they met on-line;
  - To never upload (post) pictures of themselves onto the Internet or on-line service to people they do not personally know;
  - To never give out identifying information such as their name, home address, school name, or telephone number;
  - To never download pictures from an unknown source, as there is a good chance there could be sexually explicit images;
  - To never respond to messages or bulletin board postings that are suggestive, obscene, belligerent or harassing;
  - That whatever they are told on-line may or may not be true.

a computer in their own room or in a place where they can log on in total privacy? I will guess that quite a few of those reading this article do. If you are not able to walk behind your child and see what he or she is doing at any given moment, then you are exposing your child to something potentially harmful. All of us were told by our parents not to talk to strangers. Today that stranger is no longer lurking in the park or in a van parked on the corner. No, today, that stranger walks right through your front door, past your alarm system, and down the hall into your child's bedroom. That stranger is teaching your children about sexual matters that even you don't know about. If you are going to let your child have a computer in his or her bedroom, at least take the door off the hinges. Tip: If you walk by your child and he shuts off the screen so that you can't see what they had been looking at, you have a problem.

Well, now that I have probably scared you to death and caused some of you to even conclude that you should just get rid of the computer and Internet altogether, wait! That may not be the best solution. I am sure that many of you have, at one time or another had to punish a child for some misdeed. One of the ways that I was (all too often) punished was by "grounding". Now, any parent knows that you cannot ground a kid forever. Usually a week or two was sufficient. Getting rid of the computer is like telling a child that they can never go out with their friends on Saturday night again. It is too harsh and makes the child feel hopeless. In the case of going out, excessively harsh punishment may cause that child to begin acting out in other ways. Taking the computer and Internet away permanently, will drive them underground. The Internet is a part of our lives and isn't going away. By removing it from the house, you will make children seek out other ways of gaining access to it. They may go to the library or to a friend's house, and then you have absolutely no way of knowing what they are doing. Rethink that option before jumping to implement it. If your child approaches you about having seen pornography online, don't overreact. Remember, it is daunting for a child to show something like this to an adult. Compliment them for being brave and doing the right thing by sharing this information with you. This could happen accidentally, by mistyping an internet address, however, if this is being sent via emails, shut the computer down and contact the authorities.

What are some of the responsibilities that we, as parents, have regarding computer and Internet use? Well, we should make sure that we, ourselves, understand the computer and its use. Most of the problems that I have encountered have come from homes where the parents were so intimidated by the computer that the kids were in charge of it. Sort of the tail wagging the dog. Review what your children are doing online. Who are the people in their buddy lists? Are they talking to strangers? Have they shared their passwords with anyone? Do you have the master screen name and password and not your children? Are the computers in a public place? Do your kids come home from school and bypass the fridge in order to get online and start chatting with the same kids they just rode home with on the bus (or worse, strangers)? There is actually a diagnosis in the mental health care profession now of computer and Internet addiction. If your child isn't stopping for snack after a long day in school, seek assistance.

One last note: Yet another problem has arisen via the Internet. It is called "bullying". When I went to school, the bully was relegated to the playground or maybe the hallways in between classes. Today the bullies are online and can torment children to point that there have now been documented suicides as a result of this bullying. Typically, the child that is being bullied will be afraid to discuss it. If your child is recently exhibiting behavior that is making them withdraw socially, try talking with them. If you can't get them to talk about it, then seek professional assistance. I cannot stress this enough.

I have discussed quite a bit here. Many of these online predators will try to get a young person to meet them at the mall or someplace that the child feels comfortable. This can be literally lethal. If you sense that something is going on, call the police and ask if they have a high-tech or computer crime squad. Make the report even if it turns out to be unfounded. Usually parents have a sixth sense, so go with your gut feelings.

One last point. Don't assume that your child is only chatting via the computer. Today, with text messaging and SMS (Short Message Service), cell phones are a very easy way to be able to chat privately. Keep your eyes open and be safe in the cyber world. It's not going away and, as matter of fact, it is most certainly going to become even more pervasive in our lives.

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 and 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.

Philip M. Rosenthal is available for speaking engagements and may be reached through NCYI at 212-929-1525 Ext. 150.