

Children's Online Safety Conference

by Karen Gershenhorn

Albany was the site of New York State's third annual Cyber Security Awareness Conference: Kids Safe Online, held October 17, 2007. The conference, with a focus on keeping children safe on the Internet, is held annually in recognition of National Cyber Security Awareness Month. This year 1,000 participants—students, teachers, parents, law enforcement, and other adults—took part. This conference was hosted by the New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) in collaboration with public and private sector organizations.

"You wouldn't give your six-year-old the car keys and say, 'have fun driving your friends around, see you in a couple hours,'" a recurring comment, underlined safe and responsible Internet use throughout the conference. Another reminder throughout a number of presentations was that the adage "don't open the door to strangers" applies to the Internet: Online communication opens up a door far wider than the front door at home.

The session for fourth and fifth grade students included Krysten Moore, Miss Teen New Jersey International 2007, speaking about cyberbullying and how to take action against it. Their session also featured "Cyber Citizens: Defenders of Cyberspace," an interactive play.

For the adults, workshops were offered on:

- Online Gaming: Virtual Citizenship and Its Potential Dangers;
- Online Safety and the Internet Crimes Against Children Task Force;
- 21st Century Literacy Skills and Cyber Security Go Hand-in-Hand;
- Strategies to Avoid Being a Victim of Identity Theft;
- Internet Safety—A Parent's Guide to the Internet;
- Being a Good Cyber Parent Shouldn't Require a Ph.D. in Computer Science;

Karen Gershenhorn serves as associate managing editor of SLR and other publications. © Karen Gershenhorn.

Visit the CSCIC website for tools to promote cyber security awareness, bulletins, real-time advisories and alerts, and links to other resources: <http://www.CSCIC.state.ny.us/>.

- Project Safe Childhood;
- What Every Teacher Needs to Know About the Internet;
- Safeguarding Common Internet Transactions and Communications; and
- Internet Safety for Middle and High School Students.

Project Safe Childhood

This workshop featured Thomas Spina, who currently works with the FBI's Innocent Images Project and the New York State Internet Crimes Against Children Task Force (components of Project Safe Childhood). Announced in 2006, the Project Safe Childhood Initiative is a response to the threat of sexual predators soliciting children for physical sexual contact and to the dangers of the production, distribution, and possession of child pornography.

Band of Soldiers. Former Attorney General Alberto Gonzales referred to the war against Internet crimes against children in this manner:

As a society, we already share a revulsion for what these criminals do to our children. . . I have a vision for Project Safe Childhood that will make it the foundation on which we will build a national, zero-tolerance culture. First, to put it in the simplest of terms, we need to get pedophiles and predators off the street. This means being aggressive in the cases you bring—show the world that there is no gray area when it comes to hurting kids. . . We must therefore train ourselves so that no lead will ever cross the threshold of a U.S. Attorney's Office, local police precinct, or advocacy center without some kind of follow-up and action. If there is evidence that a child has been hurt, I want to see an arrest, a thorough investigation, and a merciless prosecution if you have the evidence. . . [O]ur band of soldiers grows stronger every day. Parents and community groups will be our infantry. The Internet Crimes Against Children Task Forces will be our cavalry. And our prosecutors will be our artillery. (Alberto Gonzales, "Prepared Remarks of Attorney

General Alberto Gonzales at the Project Safe Childhood Conference," Washington, DC, Dec. 4, 2006; available at http://www.USDOJ.gov/ag/speeches/2006/ag_speech_061204.html.)

Initiative Components. The cornerstone of the Initiative is the creation of local task forces to address online exploitation. There are five components:

1. Integrated federal, state, and local efforts to investigate and prosecute;
2. Participation with partners in national initiatives, including getting leads out more quickly to local enforcement;
3. Increased federal involvement in child pornography and enticement cases;
4. Training federal, state, and local law enforcement to keep up-to-date with advances in technology (for example, in the past, agents simply pulled the plug on seized computers; data encryption now occurs automatically when computers are shut down); and
5. Community awareness and educational programs.

Agent Spina noted a strong correlation between collecting child pornography and molestation behavior, stating that girls aged 12 to 16 are often targets, especially since that demographic often communicates online and is surprisingly willing to give out personal information to someone they do not know or post photos of themselves or their friends. Half of them provide their age or date of birth. Spina described a number of cases of child sex predation in New York that have been successfully prosecuted. Urging all Internet users to think about the Internet as a way of inviting predators into your home, Spina reminded participants that something posted cannot be taken back; it continues to exist in cyberspace where anyone can see it.

Children Are Most Critical Infrastructure

CSCIC Director William Pelgrin opened the afternoon session by stressing the need for continued attention to cyber security issues' growing volume

See SAFETY CONFERENCE, next page

SAFETY CONFERENCE, from page 19

and complexity and stating his belief that “children are [the nation’s] most critical infrastructure.” Pelgrin screened a CBS News report that featured child safety expert Ken Wooden luring college students from Princeton and John Jay College of Criminal Justice into a car with a complete stranger by using various ploys. In one instance, the student allowed Wooden to duct-tape his hands. Parents would be shocked by what their kids would actually do, Wooden says.

“They look out for a monster-type person, not someone with a good story, not someone who has the art of deception down

“They look out for a monster-type person, not someone with a good story, not someone who has the art of deception down to perfection.”

to perfection.” (See http://www.CBSNews.com/stories/2006/09/27/earlyshow/main2042235.shtml?source=RSS&attr=_2042235.)

In recognition of her outstanding efforts and her commitment to protecting children on the Internet, Janice Grieshaber, executive director of the Jenna Foundation for Non-Violence, was presented with the 2007 Kids Safe Online Leadership Award. Additional information about New York State’s efforts to protect children online was provided by Denise O’Donnell, New York State assistant secretary for Criminal Justice, and Mindy Bockstein, chairwoman and executive director of the New York State Consumer Protection Board.

Katie Canton recounted her personal experience at age 15 of being groomed by an online sexual predator and lured into a potentially dangerous situation. Katie stressed that predators have very sophisticated methods of grooming children, preying on the common need to feel attractive and get attention. She serves as the Ambassador to Youth for Web Wise Kids. (See <http://www.WebWiseKids.org/>.)

“When Hormones Meet High Speed”

Robin Raskin, a nationally-recognized technology expert and advocate for online safety, used a swimming pool analogy in her keynote speech: Teach children how to swim—forgo alarms, fences, and legislation

against pool owners, and instead empower children to protect themselves.

Raskin believes there are three phases of reactions to technology and that the United States is currently between numbers two and three:

1. Fear;
2. Knowledge/learning; and
3. Action (programs and steps to solve problems).

Part of the reason for the lag is that the technology industry has been remiss and has put out technology without thinking through the ramifications.

Raskin firmly feels that children should have information, not scare tactics.

Technology is a necessary survival skill, and when kids understand how the Internet works, they are smarter. To that end, in her presentations to students, parents, and educators across the country, Raskin explains how relational databases work and why the net economy can hurt children. Children can be caught up through such tactics as typosquatting (also known as URL hijacking), email requests to visit a site, and entrapment.

During her presentation, Raskin surfed live to demonstrate the information children are sharing on social networking sites. All it takes, as she puts it, “is one dumb friend on your buddy list” and your security is compromised. She emphasizes that social networking sites are searchable relational databases. Predators can search for victims by location, age, hair color, hobbies, etc.

Parents should remember that technology can help keep kids safe as they are learning to protect themselves. Filtering software can send a message to children that their adults care. Suggested options include:

- Built-in browsers (lots of kids do not want to run into trouble);
- Paid filters; and
- Serious solutions like keylogging software (a “this premises is being surveilled” message is sent with a solution like this).

(For more information on blocking content and parenting in the digital age, visit <http://RobinRaskin.com/>.)

FBI’s Innocent Images National Initiative

Concluding the conference was an informative demonstration by the Innocent Images National Initiative (IINI) undercover operation that illustrated the prevalence of online predators. (See <http://www.FBI.gov/innocent.htm>.) IINI fulfills its mission to aggressively enforce federal law and prosecute sexual predators, identify and rescue child victims, train enforcement personnel, and raise public awareness of child exploitation on the web by focusing on:

- Online communities, etc. that exploit children for profit or personal gain;
- Child pornography producers;
- Individuals who travel—or indicate a willingness to travel—for the purpose of engaging in sexual activity with a minor;
- Major distributors of child pornography, such as those who appear to have transmitted a large volume of child pornography through the Internet on several occasions to several other people; and
- Possessors of child pornography.

Pornography Is a Crime Scene.

LimeWire, a peer-to-peer file-sharing network, was the first live demonstration. Deputy Salvatore Greco from the Rensselaer County Sheriff’s Office logged on and identified users who wished to share their files of child pornography with other users by browsing for known favorite keywords of child pornographers. He would then be able to download those photos off any computer that was online. During investigations, photographs of known victims can also be downloaded to confirm the victim is a minor and verify that the depiction is real. Special FBI Agent Dave Fallon pointed out, in regard to the pornographic photographs, that they are crime scenes, not just pictures.

Chatrooms. In chatrooms, children have no way of knowing if they are chatting with another child or with an adult predator. By going undercover online into predicated locations, utilizing fictitious screen names, and engaging in real-time chats or email conversations with subjects, agents are able to obtain evidence of criminal activity. Investigation of specific online locations can be initiated through a complaint by a citizen or an online provider; a referral from a law enforcement agency; or the name of the online location (such as a chatroom)

See SAFETY CONFERENCE, page 25

SAFETY CONFERENCE, from page 20

Cyber Security Toolkit

In his proclamation recognizing Cyber Security Awareness Month in New York State, Governor Spitzer remarked, “We are providing important information to our citizens, especially our families. Just as we protect our children at home, at school, and on the playground, we must also protect them online.”

In addition to the conference, New York State’s 2007 Cyber Security Awareness Campaign includes the creation and distribution of a cyber security toolkit designed to promote the delivery of a consistent cyber security awareness message by reinforcing core themes in

practical, informative, entertaining, and usable ways. The New York State Toolkit includes the following:

- Cyber security awareness posters;
- The Parent’s Guide to Cyberbullies (<http://www.CSCIC.state.ny.us/cscorner/events/2007/documents/Final%20Parent%20Guide%20to%20Cyberbullies.pdf>);
- Guidelines for information security and Internet usage (<http://www.CSCIC.state.ny.us/cscorner/events/2007/documents/Guidelines%20for%20Information%20Security%20and%20Internet%20Usage.pdf>);
- Internet Safe Kids Pledge (<http://www.CSCIC.state.ny.us/cscorner/events/2007/documents/Internet%20Safe%20Kids%20Pledge.pdf>);

- Cyber security awareness book-marks;
- Cyber security awareness kids’ calendars (<http://www.CSCIC.state.ny.us/cscorner/events/2007/documents/Final%202008CyberSecurity%20Calendar%20MS-ISAC.pdf>);
- Archived National Webcast Initiative broadcasts and documentation (<http://www.MSISAC.org/webcast/index.cfm>); and
- Cyber security toolkit instructions for printing and customized branding (<http://www.CSCIC.state.ny.us/cscorner/events/2007/documents/2007%20NYS%20Toolkit%20Instructions.pdf>).

Source: <http://www.CSCIC.state.ny.us/cscorner/events/2007/index.cfm>.

that suggests illicit activity (“I like older men,” for example).

Posing as a 14-year-old girl, Deputy Greco went into an online chatroom and demonstrated how “she” was immediately solicited for explicit photos (both to send and to receive) and graphic language.

An interesting side note is that when undercover officers send photos to poten-

tial targets, they must be of sworn law enforcement officers—and not many of them appear in photographs to be underage.

Knowledge Is Power

A false sense of security, a feeling of invulnerability—common attitudes for young people. While safe online in their

rooms, playing games or conversing with friends, children may unwittingly be conversing with predators. Children—and adults—must have the tools and knowledge to protect themselves in a rapidly evolving technological world. The groups at the conference are working to share that knowledge and empower the public to surf wisely and safely. ■