NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTER
A program of the National Institute of Justice

From Summer 2002 *TechBeat*

TECH b•e•a•t

Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences

Child Internet Safety

A 38-year-old man was arrested early this year when law enforcement officers discovered a missing 13-year-old Pennsylvania girl bound to a bed in his rented house in Virginia. The man, a systems program analyst, met the young teenager on the Internet and persuaded her to meet him in person on New Year's Day, police say.

A family was surprised to find U.S. Secret Service agents at their door one morning. Their teenage boy had brought home expensive computer equipment that he said came from swap meets. It did not. The boy purchased the equipment over the Internet with an unauthorized credit card. Evidently, he then used his computer to e-mail a threatening message to the President.

The role of the law enforcement officer is to protect the community, particularly its children, but when the community expands to include the virtual world of the Internet, providing that protection presents a new set of challenges.

Children and teenagers are the fastest growing group of Internet users, with an estimated 45 million expected to be online in 2002. The number of Internet crimes against children is growing almost as rapidly. A survey of children ages 10 to 17 found that 1 in 5 had received an unwanted sexual solicitation in the past year, and 1 in 33 had received an aggressive solicitation for offline contact.[1] Pornographers entice children to visit their websites by disguising them with popular children's brand names like Disney® or Barbie®.[2] Seventy-five percent of children are willing to provide personal information about themselves and their families in exchange for goods and services.[3]

Computers are a permanent part of children's lives. Even if the home has no computer, a child may have access to the Internet at school, the library, or a friend's home. To help protect children who go online, Det. Leanne Shirey, a 23-year veteran of the Seattle Police Department, developed a class that provides the information and tools needed by parents, teachers, and others to supervise children's online experiences and protect them from online victimization.

The class was developed after Shirey tried to find information online that addressed supervision of children on the Internet. Although the Internet provides good resources, Shirey says, too many parents either do not know how to access the information or, when they do, they find only brief or generic information that does not answer their specific questions. So Shirey and her fellow officers pulled together information they thought parents should know and organized it into a 7-hour lecture and hands-on class they call The Internet and Your Child.

Shirey says the need to arm parents with basic skills and knowledge about the Internet is clear. As she and her fellow officers investigated cases of children who had been victims of sexual predators on the Internet, they found obvious evidence in the homes that something unsavory was going on. Shirey says parents might have been able to identify these clear signs had they been more aware of how computers and the Internet work.

How do sexual predators persuade children to meet them offline—children who otherwise would never consider going off with a stranger they encountered in a shopping mall or on the street? Online, there are no physical behavior clues to alert the child, such as shifting eyes, tense posture, or strange demeanor. "There are no nonverbal cues on the Internet," Shirey says. "A sexual predator starts talking in the chat rooms, then moves to e-mail, gradually initiating sexual conversations on the computer and then phone calls, with the ultimate goal of the meet."

When the police investigate these crimes, she says, they generally find evidence that parents would have questioned had they known how to recognize the signs. "The clues are there—secretive behavior, additional e-mail accounts, e-mails that should have been questioned, the websites visited, even photographs of the child with the suspect."

---

[1] Finkelhor, David, Kimberly J. Mitchell, and Janis Wolak, *Online Victimization: A Report on the Nation's Youth,* conducted by the Crimes Against Children Research Center at the University of New Hampshire, for the National Center for Missing and Exploited Children and the Office of Juvenile Justice and Delinquency Prevention, June 2000.

[2] Cyveillance (www.cyveillance.com).

[3] eMarketer™ (www.emarketer.com).

The Internet and Your Child

The Internet and Your Child class is organized into modules. Each section builds on the next, so it can be used in any setting, from a PTA meeting to a law enforcement group, or for a 5-minute talk or an hour-long briefing. The class is interactive and hands-on.

Offered at no cost, the class begins with the basics. It discusses the issues of managing technology in the home and provides a guide and forms for parents to use in creating their own Internet rules. One obvious rule is to require that the computer be in a public room in the house with the screen turned toward the center of the room. Class participants learn how to set the toolbar so they can observe what children are doing online and to use the browser history or drop-down menu. "If the drop-down menu bar is empty, you have to ask why," Shirey says.

Another rule for children is never to provide personal information such as names, addresses, or phone numbers on the Internet. Predators are patient and keep carefully gathered information about their chat room contacts. For example, children who sign off a chat room saying they have to go because their mom is home or because it is time to go to baseball practice are providing clues to the predator. A child may inadvertently give another child's name or mention when the family vacation will be. Predators save this seemingly innocuous information and use it to search the many sources of personal information on the Internet to identify potential victims.

Class participants also learn to search chat rooms, read an Internet address, deal with issues of property rights and ethics, and identify scams and schemes. They learn how to use monitoring and filtering software programs and how a child could get around the software. Filtering software, Shirey says, is used to restrict access to adult Internet sites, while monitoring software runs behind the computer operating system and is activated when the computer is turned on. It records all websites visited in any browser and extracts text from Internet applications. It records all keystrokes, including instant messaging and chat room conversations, without slowing or changing computer performance.

As part of the class, the instructor, posing as a teenager, goes online and into a chat room to demonstrate how quickly predators approach their young targets. "They always do," Shirey says. "In every class."

The Internet and Your Child class does not focus solely on children as victims. It also looks at the problem of children as perpetrators and the signs that a child may be involved in online criminal activity.

Fighting Electronic Crime on All Fronts

Sponsoring The Internet and Your Child train-the-trainer courses has not been the National Law Enforcement and Corrections Technology Center (NLECTC)–West's only involvement in fighting computer and electronic crime.

NLECTC–West has assisted in electronic crime issues since its early days. The center has developed tools to recover data from computer media that guarantee the integrity of the data recovery process while providing the information investigators need to solve crimes.

Robert Waldron, director of NLECTC–West, says his center has assisted in more than 40 computer forensic examination cases. "These cases," Waldron says, "have involved identity theft, fraud, child pornography, and homicide. In one case, 500 victims of identity theft were brought to light by data recovered from a suspect computer."

This forensic casework has naturally evolved into the center's work with electronic crime issues and the task forces that have been created to deal with this burgeoning problem. Because the availability of training is a continuing problem for task force investigators, Waldron says his center has taken the initiative to host various training opportunities.

NLECTC–West arranged for the National White Collar Crime Center to offer a weeklong course on the basics of computer data recovery to investigators from seven western States at The Aerospace Corporation, NLECTC–West's technology partner, in Los Angeles, California. The class was so successful it was repeated at two other NLECTC system facilities.

Following the success of this class, Waldron says, the Federal Bureau of Investigation (FBI) asked NLECTC–West to host a 2-week class for Internet investigators. His center provided classroom space and high-speed Internet access that the FBI did not have, and his staff were able to build relationships with investigators from various agencies in the region.

In addition, Waldron says NLECTC–West is an active member in the Southern California High Technology Task Force Steering Committee, serving as its Secretary. The steering committee is composed of industry representatives who provide insight and guidance to the task force on the state of electronic crime in the region. The center also has been attending the Governor of California's statewide monitoring group and was invited to give a presentation on the NLECTC system and its

Continued on page 3

"Children think computers are like video games," Shirey says. "They forget judgment and ethics and the safety rules they routinely follow in the physical world and think they don't apply to the cyber world. It is so important that children and their parents understand the ethics of the Internet and the concepts of privacy and ownership—that it's not all right to steal music from the Internet or hack into a company's website for fun. Kids will use a password they find on Internet hacker or gaming sites without considering whether they have the right to use it. This is no different from finding a key on the sidewalk and using it to open your neighbor's front door. When kids who are caught hacking a website excuse their behavior by claiming that they did no damage, I ask them if they would consider it excusable to break into a neighbor's house if they just were looking around."

An issue that comes up in almost every class is whether parents should have password access to their child's e-mail account. Shirey says they should. "You do things in the physical world to keep an eye on your children. Being aware of who's contacting your child online is not spying. You have to eliminate secretive behavior."

Training the Trainer

A problem soon developed with The Internet and Your Child class. The demand for the class was greater than the number of available instructors. So Shirey and her coworkers took the original material and made it part of an intensive, 4-day course that certifies individuals to offer the class to others. Although there is a $150 fee for the train-the-trainer course, the fee is waived when participants present the class in their communities. To participate in the course, all would-be trainers must provide a brief resume and be screened based on computer knowledge, prior training skills and experience, and people skills. The students in each train-the-trainer class are a blend of law enforcement officers and investigators, corporate and industry leaders, and private individuals.

In October 2000, Wilma Jolly, a program coordinator at the National Law Enforcement and Corrections Technology Center (NLECTC)–West, participated in one of the train-the-trainer courses. Jolly attended 3 days of classroom training that covered computer hardware and software basics, accessing the Internet, passwords, e-mail, newsgroups, chat rooms, Internet addressing, hacking, fraud, sex crimes, ethics, privacy, copyright and licensing issues, searching for personal information, and filtering and blocking software.

"I had never been in a chat room," Jolly says. "We went in as if we were a 14-year-old and immediately we were approached by a 27-year-old man. Another individual gave explicit detail as to what sexual acts he wanted to perform."

Fighting Electronic Crime *(continued)*

role in supporting law enforcement agencies working on electronic crime. Recently, NLECTC–West was asked to join the Los Angeles Electronic Crime Task Force, which is being organized under the aegis of the U.S. Secret Service under the USA PATRIOT Act.

Waldron says NLECTC–West currently is involved with five regional electronic crime task forces in California and recently held the first meeting of representatives from electronic crime task forces in five western States. "We were able to bring task force representatives to Southern California to meet and exchange information about their work and operating procedures. The importance of this interchange was highlighted by the participant requests for continuing meetings and the presence of senior FBI and Secret Service representatives."

For more information on electronic crime initiatives of the National Law Enforcement and Corrections Technology Center–West, visit JUSTNET at www.justnet.org, e-mail nlectc@law-west.org, or call 888–548–1618.

Jolly says on the fourth day, participants teamed up and presented The Internet and Your Child class as their "final exam." Their presentations were videotaped. After a review of the videos, participants were either certified—or not—as trainers for The Internet and Your Child.

Participants in Jolly's class included parents, a school safety and security officer, a PTA representative, a casino representative, and police officers and sheriffs from jurisdictions in Colorado, Kansas, and Texas. Following Jolly's training, NLECTC–West hosted train-the-trainer courses.

Since its inception, The Internet and Your Child has been offered in 16 States and is developing an international presence. Although Seattle Police Department officers started the class on their own time, the training is now part of the department's Internet Task Force and is used as a model in several other task forces across the country. Instructors are volunteer law enforcement officers, computer specialists from the community, and graduates who have been certified through the train-the-trainer course. Classroom space equipped with computers often is donated by corporations and schools. Participants receive a manual filled with references and additional information from the Federal Government, libraries, and Internet safety sites. Since 1999, law enforcement officers could attend a similar class offered through the Federal Law Enforcement Training Center's Small Town and Rural (STAR) program. Since September 11, 2001, however, funding for the class has been diverted to homeland security issues.

For more information about The Internet and Your Child class, log on to www.theinternetandyourchild.org or write to The Internet and Your Child, P.O. Box 5386, Kent, WA 98064.

The National Law Enforcement and Corrections Technology Center System

Your Technology Partner

www.justnet.org

800–248–2742

This article was reprinted from the Summer 2002 edition of *TechBeat,* the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center system, a program of the National Institute of Justice under Cooperative Agreement #96–MU–MU–K011, awarded by the U.S. Department of Justice.