



File-Sharing Networks Give Predators an Opening

Special Interest Articles

* Sexual predators are using peer-to-peer networks to approach kids.
Page 1

* How safe is your wireless Internet connection?
Page 1

* Three Arkansas students earn MVM honors.
Page 2

* Why isn't your community an i-SAFE city?
Page 2

Also in this issue page

Internet Statistic 2

i-SAFE Wants You! 2

Internet Safety Tip of the Month 3

Spammer Gets Jail Time 4

Important i-SAFE Resources 4

About i-SAFE 4

i-SAFE Contact Information 4

P2P: Porn 2 Peers?

Thousands of kids and teens are opening files of pornography every day. And they don't even know it until it is too late.

A recent study by the House Committee on Government Reform and the General Accounting Office (GAO) found a growing trend of hiding adult and illegal child pornography in peer-to-peer (P2P) file-sharing networks. According to the Recording Industry Association of America, students 12-18 years old make up 41% of P2P file-sharers. Inside these networks the P2P files containing pornography look just like any other file. The kids and teens think they are opening a music file of their favorite artist and *wham*, their computer screen is filled with a pornographic image.

For this study, the GAO used Kazaa, the most popular P2P network with around four million simultaneous down-loaders. They searched three keywords that are associated with child pornography and what they found is astonishing. More than three-quarters of the files contained pornographic material, with 57% of the files classified as child pornography or child erotica. The GAO also searched innocent terms kids and teens would use to search for files, like "cartoon characters" or "celebrities." The majority of those files were pornographic—56% to be exact! Those files were broken down into adult pornography, child pornography, child



Predators are using P2P networks.

erotica, and *cartoon pornography*. The latter being yet another method predators use to break down the barriers and blur the line between right and wrong among the youth of our nation.

The GAO sent their findings to the Department of Justice. The DOJ said they agree "that child pornography is readily available on peer-to-peer networks, that juveniles using such networks may inadvertently be exposed to child pornography as well as other pornographic material...." The DOJ went on to admit there is a technology gap between law enforcement in general and the offenders but said they are adding resources to help close this gap. This includes the creation of the High Tech Investigative Unit within the Criminal Division's Child Exploitation and Obscenity Section. In layman's terms it is a staff of

Continued on page 3

Criminals Hijack Wireless Internet Connections

Wireless Internet technology has revolutionized the way that computer users access the Internet. Wi-Fi technology allows computer users equipped with a laptop, PDA, or cell phone to access the Internet via high-frequency radio transmitters anywhere an open wireless connection is available.

Despite the benefits of Wi-Fi technology, it can also make your Internet

connection more vulnerable to unauthorized intrusion. Cyber criminals can hijack a wireless connection to gain access to networks where they can steal data and personal information, upload viruses or inappropriate material, and eavesdrop on computer activities. An unprotected wireless network also provides anonymous access to the 'Net.

Continued on page 3



Whitney, Jessica, and Erica promote i-SAFE in Georgia.

Internet Statistic

**80 percent
of students
spend at
least 1 hour
per week on
the Internet**

*Source: i-SAFE America
Assessments--2003-04
i-SAFE survey of 19,000
students grades 5-8*

**“As a member of a
Community Action
Team (CAT) in
your area, you can
be a leader
in making kids
safe online.”**

i-SAFE Wants You!
i-SAFE is putting
together a dream team
of 12 student mentors
from across the
country. [Find out](#) how
you can nominate a
student for the first ever
i-SAFE Student
Advisory Board.

Arkansas Students Earn MVM Award

Cara, Jade, and Jordan, students participating in the Environmental And Spatial Technology (EAST) program at Star City High School in Arkansas, recently joined the i-SAFE mission to promote Internet safety awareness in their community. Their superb efforts have also earned them the national i-SAFE Most Valuable Mentor (MVM) Award for November 2004.

On November 15th the EAST Lab students began a Cyber Safety Week for seventh and eighth grade students. The students chose a different Internet safety topic for each day of the week and planned morning announcements on the school PA system and hosted workshops. On the evening of November 18th, i-SAFE Youth Empowerment Manager, Steve Godwin and Officer Fells of the Arkansas State Police Dept. conducted an i-Parent Program at the Star City Civic Center to educate parents and community members about Internet dangers. Steve Godwin said “The presentation was well received



**Steve and Officer Fells congratulate
MVMs Jordan, Jade, and Cara**

and all those attending acquired a renewed sense of responsibility and awareness of the dangers facing the youth in their community.”

Student Mentor Cara said, “It was a huge success and we also learned a great deal, too. We are so excited. We cannot wait until we reach the high school and elementary schools.”

**By Lisa Cunningham
i-SAFE Youth Empowerment**

Help Make Your Community an i-SAFE City

In communities all across America volunteers work with law enforcement and organized programs to make their neighborhoods safe from drugs, crime, violence and predators. As we work to make the real world safe, so too we must endeavor to make our communities safe in the virtual world. That is why i-SAFE America created the i-SAFE City program—to educate community members, parents, and students about the dangers online and offer solutions on how to make certain our kids are safe.

As a member of a Community Action Team (CAT) in your area, you can be a leader in making kids safe online. CATs partner with i-SAFE to make their town an i-SAFE City by educating leaders and parents about the dangers online and the i-SAFE solution. There are four ways a CAT can work to have their community designated as an i-SAFE City:

Outreach Team—A group of volunteers that attends community events, staffs booths, provides presentations, distributes materials and recruits other members.

Advocacy—The CAT can sign-up to speak at a local school board or council meeting about Internet safety, and they can enlist the elected officials to support the i-SAFE program in schools and the community. CATs can also write letters to their elected officials or set-up a meeting to discuss Internet safety education.

Earned Media—CAT members can write letters to the editor, call local talk radio shows and submit Opinion-Editorials to the local newspaper on Internet safety.

Parent Nights—CAT members can contact the local PTA or other community groups and provide a speaker to talk about Internet safety.

Once a CAT has conducted these outreach events, they will be designated as an “i-SAFE City” by i-SAFE America. i-SAFE stands ready to help you succeed in making your community an i-SAFE City. We have brochures, sample Opinion-Editorials, letters to the editor, scripted PowerPoint® presentations and tips on how to recruit more volunteers. To learn more, e-mail us at CAT@isafe.org.



Internet Safety

Tips of the Month

Contact your wireless provider to obtain specific information on how to strengthen the security of your particular wireless network.

Install a firewall on your wireless network.



Michigan students pitch the message of Internet safety.

“Parents should know there are currently no filters designed to work within P2P file-sharing networks.”

Criminals Hijack Wireless Internet... continued

Theft of service is an increasing problem within the wireless community. Unauthorized tapping of a wireless signal, even if only to access the Web, might constitute a felony. It's like running a coaxial connection to your neighbor's home to steal cable TV service. Wi-Fi hitchhikers can access illegal material or pornographic images, hack, send spam, or initiate numerous other illegal activities through your wireless Internet connection. And you or your business could be held liable.

In an activity known as “wardriving,” computer users seeking open wireless connections drive through neighborhoods and cities using a wireless-equipped laptop to detect and log open Wi-Fi computer access. Wardrivers eager to share their findings with others often leave chalk symbols, called “warchalking,” on building walls and sidewalks indicating open computer connections. (This low-tech method of advertising open access points was inspired by homeless persons who would leave chalk messages on sidewalks or buildings to indicate locations where free meals or shelter was available during the Depression in the 1920s.) While the act of wardriving is in itself quite legal, unauthorized use of a computer connection is illegal, as are many of the activities that Wi-Fi hitchhikers partake in while using these connections.

In November 2003, in Toronto, Canada, police arrested and charged Walter Nowakoski, 36, with access, possession and distribution of child pornography and theft of telecommunications. Nowakoski acquired the pornographic images via an unauthorized access to a wireless



Criminals are tapping wireless access. computer network in a nearby home.

Open Wi-Fi access also offers e-mail spammers a way to distribute unsolicited e-mail cloaked in anonymity. In a California case, Nicholas Tombros pleaded guilty to charges of unauthorized computer access and distribution of spam e-mails advertising pornographic websites. He acquired his Internet connection by driving around his California neighborhood searching for open access points.

Law-abiding citizens using legal wireless connections provided in public establishments, such as Starbucks, should also know the dangers they face when connecting in a publicly used access point, or “hotspot.” Because they are traveling on an Internet connection open to many other users, their own computer is vulnerable and the information they are transmitting or receiving could be intercepted. Those using public wireless connections should therefore take precautions to secure their own computers prior to accessing public hotspots.

By Lisa Cunningham
i-SAFE Youth Empowerment

P2P: Peer to Porn? continued

computer forensic experts who's only goal is to prosecute those involved with Internet-based child pornography and adult obscenity.

The DOJ also agrees “that those who engage in the production of and trafficking of child pornography are consistently early adopters of emerging technology.” Currently the emerging technology of distribution is an old favorite among kids and teens. Parents should know there are

currently no filters designed to work within P2P file-sharing networks. The best method of protection is good old-fashioned education. It is not the easiest of subjects to discuss with students, but it is not nearly as difficult as dealing with the consequences of an innocent victim exposed to illegal images.

By Kevin Storr
i-SAFE Director of Communications

News Flash!**Spammer Locked Up**

For the first time ever in the U.S. a spammer has been convicted of felony spamming. Jeremy Jaynes was sentenced to nine years in prison under Virginia's tough new spam law. Jayne's sister, Jessica DeGroot, was fined \$7500 for her involvement in Jayne's spam operation. According to court papers, Jayne and company repeatedly sent over 10,000 spam messages over a twenty-four hour period—and those were only the ones reported by irate recipients. The Register of Known Spam Operations rated Jaynes as the eighth-most prolific spammer in the world.



We welcome your input!

If you would like to submit an article for the newsletter or tell us your story, please contact us at:

i-SAFE Times Editor
5963 La Place Court
Suite # 309
Carlsbad, CA 92008
(760) 603-7911
Editor@isafe.org

We're on the Web! See us at:

www.isafe.org

i-SAFE AMERICA

Educator's Corner: i-SAFE Vs. the Mac

We know some of you have been experiencing difficulties in using our materials with the Mac. Please know we are hard at work to alleviate these problems. We have reformatted the PDP CD; the videos are no longer embedded but are hyperlinked. This is immediately available for your presentations. And we are in the process of creating a hybrid Curriculum CD that will allow graphic-user interface rather than through the html page. The auto-run will be applicable for PC use only. Our minimum system specification are listed on our website in several places, including http://www.isafe.org/channels/system_reqs.htm.

What this all means in non-tech terms is, these revised CDs will work on your Macs! Similarly, all Outreach materials have been tested to ensure compliance. If you have been struggling with your CDs, please contact us at Education@isafe.org. We will be happy to provide you with a replacement.

i-SAFE Resources

Educators! If you are interested in bringing the i-SAFE Curriculum to your school, contact us at education@isafe.org or call us at (760) 603-7911.

Parents and Community Leaders! If you are interested in bringing the i-SAFE program to your community, contact us at outreach@isafe.org or call us at (760) 603-7911.

Students! If you are interested in becoming an i-SAFE Student Mentor, contact us at mentors@isafe.org or call us at (760) 603-7911.

Interested in attending an i-SAFE event? Click [here](#) for a full calendar of events coming to a location near you soon!

About Our Organization...

MISSION: i-SAFE is a non-profit foundation whose mission is to educate and empower youth to safely and responsibly take control of their Internet experience.

GOAL: The i-SAFE program provides students with the awareness and knowledge they need in order to recognize and avoid dangerous, destructive, or unlawful online behavior and to respond appropriately.

i-SAFE is dedicated to: 1) implementing a standardized Internet safety education program throughout the nation that provides kids and teens with essential tools to reduce the risk of their being victimized while engaged in activities via the Internet; and 2) launching an Outreach Campaign that empowers students to take control of their online experiences and make educated, informed, and knowledgeable decisions as they actively engage in cyber activities.

A Special Thanks from The i-SAFE Times Staff

Bronwen Matthews, Editor-in-chief; Eric Fairbanks, Editor; Teri Schroeder, i-SAFE President; Jonathan King, Outreach Director; Lee Taylor, Education Director; Paul Olson, Graphic Design, and contributing writers: Lisa Cunningham, Kent Gates, Steve Godwin, Kevin Storr.