EDTECH™ FOCUS ON K-12

Brought to you by:

CDW-G

CASE STUDIES

TACTICAL ADVICE

RESOURCES

Classroom

Infrastructure Optimization

Security

Storage

Networking

Mobile

Hardware & Software

Management

CURRENT ISSUE

Subscribe

SIGN UP FOR

EdTECH

E-NEWSLETTERS

Follow EdTech K-12

Follow RSS Feed

Connect With CDW

LinkedIn YouTube Spiceworks

Like 3k

ADVERTISEMENT

Cyber Safe

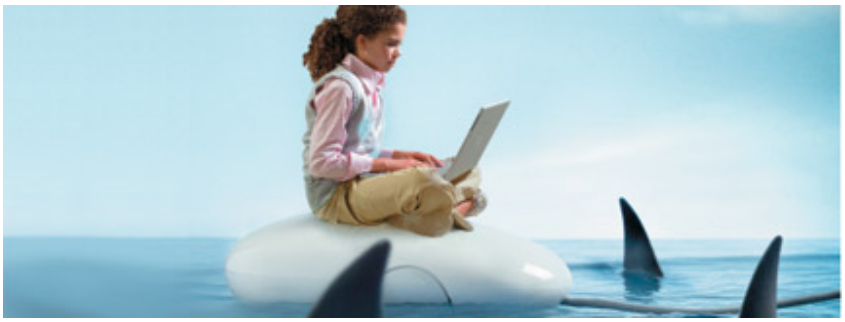
Chat rooms. Instant messaging. Social networking. Unfortunately, these fun and popular Web 2.0 pastimes are a predator's paradise. Crafty technology practices, evolving usage policies and safety education help schools keep kids secure online.

Lee Copeland And John Pulley

posted April 10, 2007

Like Tweet 0 Share Spice

ADVERTISEMENT



Related Articles

- *Saved by the Bell*
- *Safe Zone*
- *Serious About Security*

From Beowulf — the oldest-known English text — to Little Red Riding Hood, we've warned our children of evil lurking in the world. In modern tellings, the monster is a sexual predator, a faceless sociopath who lurks undetected on the Internet. Like the Brothers Grimm red-hooded heroine, who naively talks to a wolf in the woods, unsuspecting young people today are still being duped into letting down their guards online.

Kacie Rene Woody, a 13-year-old girl, was sexually assaulted and killed in 2002 by a man she met in an Internet chat room. Friends of murder victim Kayla Reed reported that the 15-year-old girl was active on MySpace until the day she disappeared last year. According to the U.S. Department of Justice, one in five children ages 10 to 17 has received unwanted sexual solicitations online.

Social networking sites, instant messaging, blogs and other permutations of Web 2.0 provide modern-day monsters with an easy path to their victims, and schools are emerging as ground zero in the fight to keep kids safe online. Yet there are no easy fixes. Administrators in Massachusetts, Virginia and beyond are responding to the challenge of protecting students without isolating them from emerging technologies with a multipronged strategy that includes content filtering tools, crafty technology practices, constantly evolving acceptable use policies (AUPs) and safety education.

Lockdowns and Spot Checks

How do you keep 30,000 notebook-toting, wireless-Internet-surfing, middle and high school students safe online? Lloyd Brown, director of technology for Henrico County (Va.) Public Schools, asks himself that question every day.

While Henrico relies on education and policies to help keep students safe, technology rounds out the defense. Most students carry notebooks equipped with wireless Internet access on campus and away from school. Henrico

blocks access to inappropriate Web content and also locks down computers when administrator-defined thresholds for accessing inappropriate Web sites are exceeded.

“We have full access and full control of every laptop” and that control extends past the school district’s walls, says Brown. When students access the Internet away from school, the content filter forces them onto a remote filtering device. Henrico’s system regularly lists the 100 sites most visited by students. On any given day, the system sends up a red flag if a Web site gets an unusual number of student hits.

To further help officials keep abreast of students’ online activities, notebooks issued by the district contain complete histories of surfing activity that cannot be deleted by students. “We do computer spot checks and look at the history to see what’s going on,” says Brown. “It’s just like the drug dogs.”

System lockdowns are a popular deterrent at school districts across the country. Take Township High School District 113, for instance. The Highland Park, Ill., school system locks browsers from the network side to prevent students from bypassing the district’s security measures to create Internet proxy servers or change history settings. “We use Group Policy to lock down Internet Explorer on all computers, so that students cannot change proxy settings or history settings,” says Ron Kasbohm, system support manager at District 113, which enrolls 3,800 students.

Group Policy, an administrative management tool created by Microsoft, also provides a means to prevent students from running executable code, Kasbohm explains. If the district didn’t take this measure, students could launch proxy servers off USB drives, CDs or network drives.

“We’ve already busted two or three kids who tried to do that,” says Kasbohm. The steps for creating a proxy server with an external Internet protocol address to bypass content filtering tools are easy to find through any search engine, such as Google.

Numerous CIO and information technology administrators at school districts told EdTech that battling proxy servers built by tech-savvy students is a continual challenge. Suspicious sites tend to routinely change server names, Web site and IP addresses after landing on blocked site lists. “As soon as they find out they’re on the filtering list, they relocate and make new names to get by the filter,” Brown says. “MySpace changes URLs so much. It’s hard for us to stay 100 percent on it.”

Ford Greene, chief of information systems and technology at Rochester School District in New York, which runs two content filtering tools, likens shutting down proxy servers to a never-ending chess match. “We block them as fast as we identify them,” he says. “Don’t assume for a minute that these kids don’t understand the technology. Even in the fifth and sixth grades they are very, very sophisticated.”

Like Township High School District and Chicago Public Schools, Rochester School District runs a closed e-mail and instant chat system for its 40,000 students and 7,000 staff members. That makes it easier to prevent students from launching inappropriate Web sites and stores all communications be-tween students and staff, while reducing the potential for unauthorized access via e-mail or instant chat.

“We have to stay diligent to ensure that nothing inappropriate happens from within our district and from the outside world,” says Greene.

In Illinois, Kasbohm’s district monitors all communications within its closed system as well. “All chatting and e-

mail communications are logged in our system," he reports. "We archive them forever."

Online Safety by the Numbers

- **25%** of children have been exposed to unwanted pornographic material online.
- **75%** of children are willing to share personal information online about themselves and their families in exchange for goods and services.
- Only **25%** of children who encountered a sexual approach or solicitation told a parent or adult.

The Three R's and Computer Safety

"I spoke to a parent about cyber safety and our acceptable use policy recently, and she said, 'I hope you're not relying solely on the honor system,'" recalls Rochester's Greene. His answer: No. Students must review and sign the acceptable use policy they receive with their registration packets, and teachers, administrators and librarians receive about 10 hours of training each on Internet safety and popular, but problematic, Web 2.0 tools.

But crafting an AUP that's backed by computer safety education is the last and sometimes trickiest piece of the security puzzle.

"It's our duty," says Felicia Vargas, acting director of TechBoston, a Boston Public Schools program that promotes and supports advanced technology. "This technology exists in the schools, and if we're not doing anything to educate students about it, it's negligence on our part. It's really basic: reading, writing, arithmetic ... and computer safety."

Boston's public schools are taking a multistep approach to keeping students safe online. The city was a stop on last year's 12-city Get Net Safe Tour, sponsored by i-safe.org, a nonprofit foundation dedicated to making the Internet safe for children. The school system provides stipends for teachers to become tech contacts in the schools. To date, some 220 teachers have completed the training.

"The tech-support teachers are the first-line approach," says TechBoston's Vargas. But backing them up is the expertise of the Boston Police Department, school police, the District Attorney's Office, the Massachusetts Attorney General's Office and Bunker Hill Community College, which received a grant from the National Science Foundation to establish a program of study in computer forensics, with a focus on Internet safety for youths.

Technology can help to keep kids safe online, but the crux of the issue is behavior modification, says Patrick Plant, director of technology and information services at the Anoka-Hennepin Independent School District in Minnesota.

"There's no easy silver bullet," Plant says. "The challenge is making students discerning individuals." Seeking to give students the skills they need to make smart choices, the school district has integrated a program called TOOLS (Technology Opens Opportunities for Lifelong Skills) into its curriculum. The initiative exposes kids to a range of issues from acceptable use of resources to strategies for validating the accuracy of information found on the Internet.

"The best thing we can do is educate," says Robert Runcie, CIO of Chicago Public Schools. "We work to make education a priority, to invest in resources and time to protect our students and staff." The school district of 420,000 students and 46,000 staff locks desktops and runs a closed communication system. It continually updates its acceptable use policy and provides policies for students, educators and administrative personnel. Like Boston Public Schools, Chicago's 300 technology coordinators help preach the message about appropriate behavior and how to protect one's identity online.

"We cannot control what our students do outside of school," Runcie says. "That's why education is very important, and helping the students to understand the risk associated with Web-based communications."

Quick, what's the most popular Web site in the country?

For those who answered Google, congratulations, you came in second. Ask the nearest teen and they are more likely to give you the top answer — MySpace.com, which receives 80% of social networking traffic. Almost 6% of U.S. Internet hits went to the social networking site, while the search engine got 4.5%. Facebook and YouTube.com also made the top 20.

Two music-oriented sites, Buzznet and iMeem, are showing the fastest growth within the social networking category, with visits increasing 148% and 146% respectively from January to February 2007. Source: LeeAnn Prescott, Research Director, Hitwise, February 2007

Rick Woody's Mission

Rick Woody has lived every parent's nightmare. His daughter, 13-year-old Kacie Rene Woody, was kidnapped and murdered by a California man she met in an Internet chat room. Ask the Greenbrier, Ark., police officer about the role of technology, schools, parents or even the police in online safety. His answer remains the same: Education is the most important element.

Everyone "needs to know the things that put [children] in danger and the ploys these predators use. They always have the same interests the kids have," says Woody. "They will always have the same problems. And they always

want to keep it secret."

The typical predator ploy is summed up in the acronym SITS (similar interests, trust and secrecy).

"Cyber predators are out there looking for children to meet offline or to do things online that are inappropriate," says Ben Halpert, a nationally recognized security expert and parent in Atlanta. It always starts with a grooming period, Halpert says. "Over the course of time measured in months, the predator wears down the child's defenses until they move into online solicitation."

But education shouldn't end with the kids, Woody cautions. "No matter how much you educate the kids, you can't rely on them to make the right decision all of the time," he says. "You've got to get to the parents. They think they already know how to keep their child safe online, but they don't understand how predators work."

To promote awareness of online safety, he established the Kacie Woody Foundation (*www.kaciewoody.com*). Through the foundation, Woody disseminates information about predators in the news, works with an Internet Predator Awareness Team of students each year and makes presentations at schools and conferences in the area.

Five Smart Ideas

1. Don't put computers in the corner. Place computers that students use where teachers, librarians or administrators can pass by and see what the students are doing. Besides, you want technology to be an integral part of learning. — Ford Greene, chief of information systems and technology at Rochester (N.Y.) School District
2. Educate your faculty and staff on how to respond when a teen does report a concern. One gossiped-about misstep could turn students off and keep them from reporting inappropriate behavior if they're made to feel embarrassed in front of their peers. — Nancy Willard, executive director for the Center for Safe and Responsible Internet Use in Portland, Ore.
3. Encourage parents to Google their child's name and visit their child's social networking page. Parents should also check their child's blog and buddy list. Rather than leaving these open, most sites offer the capability to keep posts and buddy lists private. Some parents, however, are concerned about invading their child's privacy. "They put these pictures and information out there for potentially millions of people to see — why not you?" — Lisa Hicks-Thomas, Virginia's senior assistant attorney general
4. Invest in a real-time identification system, which automatically searches the sexual predator databases. This ensures that all school visitors are documented and makes it easier to identify those who don't belong on school grounds. — Marge Wessel, executive director of Doctors Charter School in Miami Shores, Fla.
5. Communication from cyber predators isn't the only concern. Many colleges and employers check social networking sites prior to admitting students or hiring employees. Photographs or posts with drinking, drug use, nudity or inappropriate language could create dire consequences down the road. — Cathy Cratty, director of student and employee assistance programs at Township High School District 113 in Highland Park, Ill.

Related Articles

- *Saved by the Bell*
- *Safe Zone*
- *Serious About Security*

Like

Add New Comment Login

Showing 0 comments Sort by newest first

Subscribe by email RSS

Trackback URL http://disqus.com/forur

Security

3 Strategies for Preventing Notebook Theft

Schools have a variety of options at their disposal to combat device loss, including...

A Firm Foundation: Bringing Google Apps into the Classroom

Google Apps facilitate communication and collaboration in classrooms, but the right...

...more

Storage

5 Next-Level Data Consolidation Tips

An IT expert offers five data consolidation tips.

Making the Most of Power and Cooling Management

Using equipment strategically ensures continuity of operations while also generating big...

...more

Infrastructure Optimization

5 Next-Level Data Consolidation Tips

An IT expert offers five data consolidation tips.

Modular Data Centers Let Schools Add Capacity Easily

Modular strategies let schools add capacity easily

...more

Networking

Tidy Up with Iogear's KVM System

Iogear's KVM console gives your data center a professional appearance.

Getting Ready for the BYOD Revolution

School IT leaders reveal how they're readying their networks to support the additional...

...more

Classroom

Teachers Bring Text Messaging to the Classroom

Social media and smartphone-based learning help typically shy students find their voice.

Video Conferencing Takes Education to the Next Level

How schools are using video conferencing to bolster interactive learning.

...more

Hardware & Software

Review: Adobe Premiere Elements 10

Students and teachers can create their own Hollywood movie magic with the latest version...

Review: Lenovo ThinkPad Tablet

This business-minded tablet will put a charge in students' productivity.

...more

Classroom

Infrastructure Optimization

Security

Storage

Networking

Mobile

Hardware & Software

Management

Home

Contact Us

About the Editors

Sign up for E-Newsletters

Subscribe

Site Map

Terms and Conditions

Copyright © 2012 CDW LLC | 230 N. Milwaukee Avenue, Vernon Hills, IL 60061

cdw.com

cdwg.com

biztechmagazine.com

edtechmagazine.com

fedtechmagazine.com

statetechmagazine.com