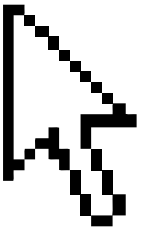
DO YOU KNOW WHERE YOUR KIDS ARE CLICKING?



Your kids aren't going to stop using MySpace and Facebook, but at least you can give them safety helmets and kneepads.

BY ALAN COHEN

Illustration by Asaf Hanuka

EVERY FEW WEEKS, DAVID FREY walks into a school cafeteria, pops open his laptop, and frightens a room full of parents. There's nothing particularly scary about Frey himself, a friendly 39-year-old with a wry sense of humor. It's all in his presentation.

An assistant district attorney of Staten Island, New York, and chief of his office's computer and technology investigations unit, Frey has seen practically every bad act that can happen via the Internet, from drug deals set up in AOL chat rooms to sexual predators targeting—and assaulting—minors. Almost without exception, the parents he speaks to have noticed nothing to be wary of. "Most parents are completely surprised when I show them this stuff," says Frey. "They have no idea what goes on online."

Although many parents are in the dark about their kids' online activities, there's nothing secret in Frey's laptop. And that, says Frey, is an even bigger problem. With social networking sites such as MySpace.com, Facebook, and Xanga exploding in popularity, teenage diaries are no longer hidden under the bed. They're posted online, often freely accessible to anyone, anywhere. Bits of information that seem perfectly innocuous—a first name, a school name, interests, and worries—can be seen and used by sexual predators, for whom the Internet has become, Frey says, "a target-rich environment."

Before visiting a school Frey will search for, and easily find, MySpace pages belonging to students at that school. These are what he shows the parents, and these are what shock them. "Here's one," says Frey, shaking his head as he pulls up a teenage girl's MySpace page in his conference room. "For a pedophile, this page is just perfect."

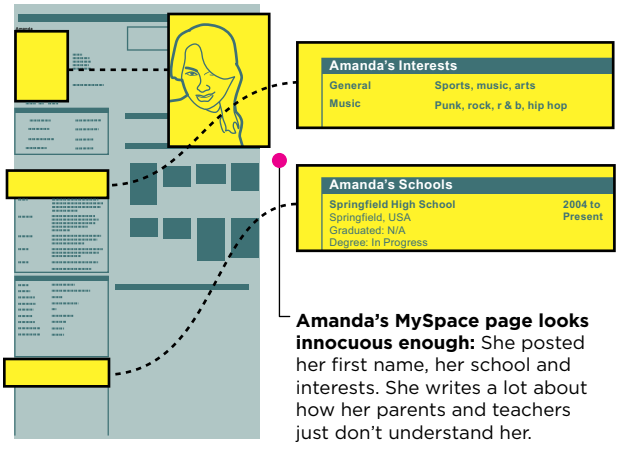
At first glance, there doesn't seem to be anything extraordinary about the page. A young girl writes about her struggle with bulimia, her drug use, and her lack of self-esteem. It's troubling stuff, to be sure, but no different from hundreds of other pages Frey has accessed on the Internet. That, too, says Frey, is the problem: "Kids don't think of the Internet as something everyone sees. They are completely trusting. They say things they'd never tell their parents." The irony is that although their parents may not know about any of this, online predators, who tend to target the most vulnerable kids, now do.

"Look at this," says Frey, pointing to the screen. "She posts her photo and gives her name. Then she posts the name of her high school, her e-mail address, her AOL Instant Messenger name, and all of her interests—the singers and movies she likes."

For a predator this is both a dossier and an opportunity. "If I'm a pedophile, I now know that she has a bad self-image, I know where she goes to school, I know the things she likes," says Frey. "I know that she's in drama class. She even says where she works." All of this, he says, creates easy pickings for a predator, who will know how to make contact with the teen and how to gain her trust. It's simple to say all the right things when you're practically handed an instruction manual.

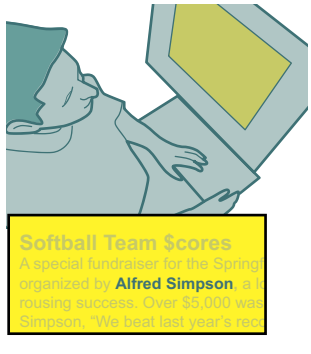
A PREDATOR'S PATH

An online predator can turn a little info into a lot of trouble.



Amanda's MySpace page looks innocuous enough: She posted her first name, her school and interests. She writes a lot about how her parents and teachers just don't understand her.

A predator draws a conclusion: Amanda just might be on the high school's softball team. He Googles the high school, finds a photo of the team—and recognizes her. He now has Amanda's last name.



The predator heads back to Google: He enters her full name and her school name, and finds a local newspaper story about a fund-raiser Amanda's father spearheaded for new equipment for the softball team.

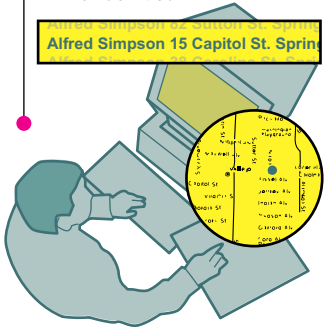
No joke. Assistant DA David Frey tells kids at Intermediate School 51 on Staten Island how easily online predators can track them down.

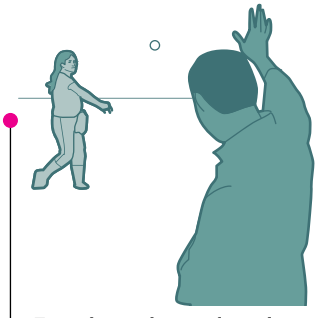
"Predators are very clever," says Frey. "They use the data you've posted to pretend to be a friend. They groom you; they get your trust. It's not sexual at first. But gradually they push a little bit, then they fall back, then they push—until it's completely sexual." Often predators will send pornography to the kids they are targeting to desensitize them to sexual activity, explaining that it's no big deal and that everybody does it. Then comes the final push: a suggestion to meet. "This girl," says Frey, looking at the profile on his laptop and shaking his head once more, "is the perfect victim."

Kids at Risk

The Internet may have broadened our view of the world and made our professional lives easier, but it has certainly complicated parenting. Of course, the problem is not exactly new. Even before social-networking sites came on the scene, parents had good reason to worry about their kids' safety online.

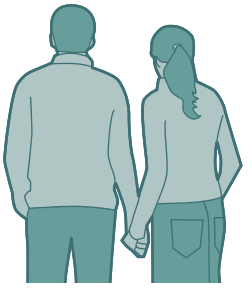
A new Web search: Google provides the predator with the addresses of all the Alfred Simpsons in the city. Only one of the dozen listings is near Amanda's school. The predator now knows where Amanda lives.





From here, the predator is home free: He knows where to find her. Striking up a conversation—say, on a softball field—won't be a problem. Neither will be gaining her trust. He can say all the right things—like how his parents never understood him, either.

In a short time, the predator has contacted Amanda: The e-mails and IMs are harmless enough, and Amanda's new friend is always so friendly and reassuring. Finally, Amanda thinks, there is an adult who understands her.



The messages are getting a bit explicit: Amanda says so, and the predator tones things down. He sends her a new softball glove, too. When the messages get sexual again, she figures he's right, everyone does talk about—and do—this stuff. So when he suggests they meet up, she thinks: Why not?

Photograph by Scott Schedivy

10 ESSENTIAL TIPS FOR PARENTS

Here's some practical advice for keeping your kids safe online:

1. Don't forbid Internet use; in all probability, your kids will defy your ban on the sly.
2. Filtering software won't block all dangers your kids face on the Web, but it's a good start. Also visit sites with your child whenever possible.
3. Understand the technologies: Take a class, check out the Web resources listed on page 94, try the sites yourself. The more you know about the Internet, the better you can talk to your kids about it.
4. Place the computer in a common area of your home; kids won't expect privacy there.
5. Talk to the parents of your child's friends; most kids use computers at friends' homes.
6. Teach your kids the "embarrassment rule": They should never post anything they wouldn't want everyone to read.
7. Tell them to be careful about what they post regarding other people. Predator-friendly information is often left by friends posting comments.
8. Let your child know that it's important to tell you if he or she is ever approached online or receives inappropriate content.
9. Look for red flags that your child is in danger, such as minimizing a browser when you enter the room and getting phone calls from people you don't know.
10. If you think there may be a problem, report it to authorities and also to your Internet service provider.

Frey started giving his talks—to parents, kids, guidance counselors, and other prosecutors—in 2000, the same year that a study by the National Center for Missing & Exploited Children found that one in five children who use the Internet had been sexually solicited online.

Back in 2000 the main targets of concern were chat rooms and instant messaging. Now there are blogs and social-networking sites to worry about. For both parents and kids, these new technologies can be even more problematic. "In a chat room, a predator goes in cold," says Frey. "On these new sites, predators know about you, they know about your friends, they have all of this data about you." And they know how to use it.

The burgeoning popularity of social networking sites—MySpace has over 75 million users—means that even preteens are clamoring to use them. Although MySpace warns users that they must be 14 or older to register, the site has no way of verifying age. The same is true for almost all other social-networking sites. "We know that younger children are lying to get on the sites," says Nancy McBride, the national safety director at the National Center for Missing & Exploited Children.

Making matters worse: Online predators aren't the only danger parents have to fear. The ubiquity of broadband now makes it easier for kids to be exposed to pornography and other objectionable video and images. Cyberbullying, where kids are threatened via anonymous e-mail, instant messages, and even full-blown Web sites, is an increasingly common and worrisome problem.

Then there's all the personal information kids post online. Not only does it expose them to predators, it puts them at risk for identity theft. And even if there are no criminals reading your MySpace page, well, maybe there is a college admissions officer taking a look. "Kids think they're talking to other kids, but they have no idea who they are speaking to," says McBride. "They'll post pictures of illegal or inappropriate behavior and it will come back to haunt them when they apply to schools or for a job."

Advice to Parents: Learn This Stuff

Keeping all of these perils in check can be a full-time job for a parent, and it's a job they're not doing so well. One particular challenge is that most kids know a lot more about the Internet than do their parents, and they use the knowledge gap to win more time and less supervision online. "You find that a lot of parents are bullied," says Frey. "They don't want to look stupid in front of their kids, who tell them that everyone is doing it."

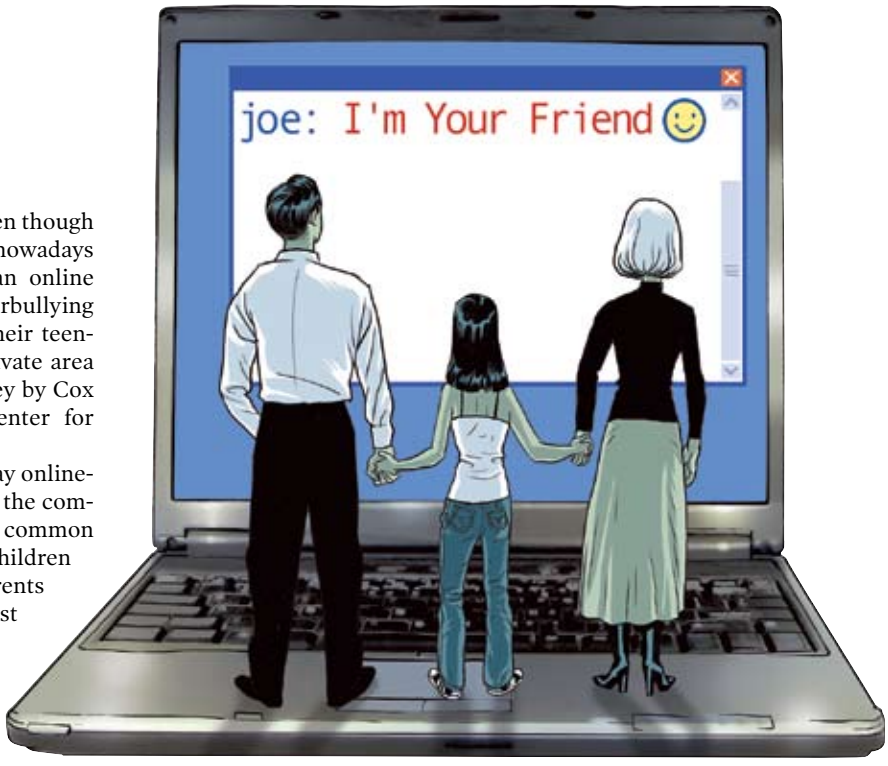
Bridging that knowledge gap is essential to understanding the risks your children face online and how you can help them. "If you're a parent, you better learn about this stuff," says McBride. "If that means taking a class, or getting a book, so be it. It's hard to protect your kids online if you don't know what they're doing." Once parents understand the technologies and the dangers, they can more easily talk to their kids about those dangers and how to avoid them.

Sadly, this common-sense solution—educating both yourself and your children about staying safe

If you're a parent, you'd better learn about this stuff. If that means taking a class or getting a book, so be it. It's hard to protect your kids online if you don't know what they're doing.

online—is in reality often neglected. Even though it's hard to read the daily newspaper nowadays without coming upon a story about an online predator or some cyberstalking or cyberbullying incident, 30 percent of parents allow their teenage children to use a computer in a private area of their home, according to a 2005 survey by Cox Communications and the National Center for Missing & Exploited Children.

That's exactly the wrong thing to do, say online-safety experts, who urge parents to take the computer out of the bedroom and put it in a common area, like a family room or den, where children have no expectation of privacy and parents can check in on what they're doing. Just a little bit of education, the experts say, and parents would quickly understand how necessary this rule of thumb is.



Filters: A False Sense of Security

If that little bit of education isn't getting through, the fault doesn't lie completely with parents. Criminal penalties, technological solutions such as filtering software that blocks inappropriate sites, and pressure on content providers to police their own sites are getting the bulk of media—and political—coverage. Not surprisingly, many parents have been lulled into believing that these approaches will take care of the problem—wishful, and dangerous, thinking.

"What parents have to realize is that there is no silver bullet," says Herbert Lin, senior scientist at the National Research Council of the National Academies, where he directed a 2002 study on protecting children from sexual exploitation and online pornography. "Filtering software has certainly gotten better, but do parents rely on it too much? In my opinion, they do. A filter is brittle. Even if it stops 90 percent of the bad stuff, what do you do about the other 10 percent? You still have to have a thorough educational process." (See page 96 for minireviews of filtering software, and visit *go.pcmag.com/parentalcontrols* for our comprehensive reviews.)

Four years ago, Lin emphasized the need for education in online safety in his report, and he's still waiting for legislators to pick up on the idea. "We said education was fundamental, but no one is taking that seriously," says Lin. "It's not sexy; it's not easy to do. You don't see any bills on education." The focus, instead, has been on criminal penalties and filtering software. These, say Lin, should be part of the answer, but not the answer itself: "Any solution that says you don't have to do the hard work of being a parent is not going to work."

Nor should parents rely on content providers to find predators and porn. To be sure, the sites are ramping up their own enforcement efforts. Both MySpace and Facebook recently hired chief privacy officers. MySpace runs public service ads to promote online safety and reviews all images on its site. Facebook warns users who may be abusing the system. "We'll look for things like the number of rejected friend requests they have," says Chris Kelly, Facebook's chief privacy officer.

But with social networking sites growing so rapidly, inappropriate content and behavior is bound to slip through the nets. MySpace may be reviewing images, but it receives two million of them each day, and keeping an eye on all of them is a tall order.

Parents need to understand what can and does happen online, but just as important is their need to develop a line of communication with their children. This is crucial not only to prevent harm, but also to take action should inappropriate activity take place.

The good news is that even as the technologies get more sophisticated, so too have police and prosecutors. "Law enforcement is much better trained about this now," says McBride of the National Center for Missing & Exploited Children. Internet investigation units are also better staffed and funded. The Department of Justice finances 45 Internet Crimes Against Children task forces, and many local police departments now have units dedicated to investigating Internet crimes. Even cyberbullies hiding behind anonymous e-mail accounts, proxy servers, or a neighbor's Wi-Fi network can usually be tracked down quickly.

THE BEST WEB SITES

These Web sites offer an abundance of tips for keeping your kids safe.

The CyberTipline:
www.cybertipline.com

NetSmartz:
www.netsmartz.org

Microsoft Safety Tips:
www.microsoft.com/athome/security/children

SafeTeens.com:
www.safeteens.com

Net Family News:
netfamilynews.org/index.shtml

WiredSafety:
www.wiredsafety.org

NetSafeKids:
www.nap.edu/netsafekids

Illustration by Asaf Hanuka

64%
of parents with online teens say that there are rules in their home regarding the timing and duration of Internet use.
Source: Pew Internet & American Life Project, 2004

71%
of teens received messages online from someone they don't know.
Source: National Center for Missing & Exploited Children and Cox Communications, 2006

64%
say they do things online they don't want their parents to know about.
Source: Pew Internet & American Life Project, 2004

14%
of teens have met face-to-face with a person they had known only through the Internet.
Source: National Center for Missing & Exploited Children and Cox Communications, 2006

MySpace has pulled more than quarter of a million profiles believed to be for children under fourteen years old.
Source: MySpace, 2006

One out of five teens reported that it is safe to share personal information on a public blog or social-networking Web site.
Source: National Center for Missing & Exploited Children and Cox Communications, 2006

45%
of teens have been asked for personal information by someone they don't know.
Source: National Center for Missing & Exploited Children and Cox Communications, 2006

79%
of online teens say teens aren't careful enough when sharing personal info online.
Source: Pew Internet & American Life Project, 2004

87%
of teens age 12 to 17 use the Internet in some aspect of their lives.
Source: Pew Internet & American Life Project, 2004

Defn.: "Cyberbullying" is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet.
Source: Stopcyberbullying.org

20%
of 8- to 18-year-olds have a computer with Internet access in their own room.
Source: Kaiser Foundation, March 2005

KIDS ON THE WEB: RISKY BUSINESS KIDS ON THE WEB: RISKY BUSINESS

"They may be clever, but we're more clever," says Frey. "A lot of times they'll leak a tell. They'll target people they know; they'll use their pet's name, or their ZIP code, or their school in their screen name. You look for a guy with a pit bull named Randy. It isn't hard. We'll get 90 to 95 percent of the people we're looking for if it's reported."

And there's the rub. The best detective work in the world is of little use if kids and parents don't report inappropriate activity in a timely fashion. ISPs usually can't trace activity back to a specific user after a certain time period. "If we send a letter asking them to preserve data, they'll preserve it," says Frey. "The problem is when someone doesn't make a report in time, and we lose the path."

House Rules

Though Frey's presentation is intended to scare parents, he doesn't want to scare them *too* badly. Then they might pull the plug on the Internet altogether, and that, he and other experts say, probably does more harm than good: It deprives children of a remarkable resource and can breed defiance. "Kids are always going to find a way to use it," says McBride.

The better strategy is to give kids access—but set some rules. Keep the PC in a place where there is little privacy, and visit sites with your child when possible. Let your kids know that it's important to tell you if they are ever approached online or receive inappropriate content. Don't delete any messages or images, either; they can help law enforcement trace the activity back to its source.

Teach your kids the "embarrassment rule": They should never post anything they wouldn't want the whole world to read, because once they post it, the whole world *can* read it. Tell them to be careful about what they post about friends, too. Some of the most predator-friendly information (names, telephone numbers, employers) isn't left by the author of a MySpace page, but by friends posting comments.

The Best Parental Control Software

With these applications you can restrict the Web sites your kids visit and limit their time online. For a walk-through of the parental-control features in Windows Vista, visit **go.pcmag.com/vistaparentalcontrols.**

OTHER OPTIONS

iShield
By analyzing skin tones, textures, faces, limb shapes, and a variety of other cues, iShield does a good job of blocking pornographic images. It's very easy to install and use. Each time your browser (Internet Explorer, Netscape, Firefox, or Mozilla) loads a Web page, iShield analyzes the images found on that page. It can block images or entire pages, and it offers an option either to warn users or to record porn-surfing silently. If necessary, the parent/administrator can whitelist specific sites that get blocked in error or blacklist sites that are definitely unwanted.
$24.95
go.pcmag.com/ishield
●●●◐

ACCESS CONTROL PC Moderator
PC Moderator is a hardware device that disables the monitor when children have used up their allotted time on the computer. It's extremely effective, but a one-trick pony.
$79.95 analog, $89.95 digital
go.pcmag.com/pcmoderator
●●●●

ContentProtect
Strong on content filtering, this full-featured parental-control app analyzes Web page text in real time, offers time-based access control, sends e-mail notification of blocking events, and includes an abundance of surveillance reports. You can apply settings to all users or to individual user profiles, which you can tie to Windows user accounts so that no separate ContentProtect log-on is needed. You can let kids send an override request to the administrator. On the downside, the software requires too many passwords, and the remote management feature can't quickly push changes back to the protected computer.
$39.99 per year
go.pcmag.com/contentprotect
●●●○○

SAFE EYES 2006

PC MAGAZINE EDITORS' CHOICE

Keep your kids away from bad sites and control how much time they spend online. If they go wild on the Web, Safe Eyes rats them out so you can take control from wherever you are. It's tough; we tried circumventing it but failed to access blocked sites or get access outside scheduled hours. One license allows installation on three PCs or Macs that share the same online user profiles. That's great for the multicomputer family. And filtering happens at the server level, so it works with any browser. Add logging of Web and IM activity for even stricter parental control.

$49.95 per year for up to three computers
go.pcmag.com/safeeyes2006
●●●●○

Recognize the Red Flags

Keep in mind, too, that while preventive steps like these can reduce the risks, they can't eliminate them completely. So watch for red flags. Is your child minimizing or changing a browser window whenever you walk into the room? Is he using instant message lingo like "POS" (parent over shoulder)? Is he getting phone calls from people you don't know or wearing new clothes? They could be gifts from a predator. Is your child reluctant to log on or go to school? Those could be signs he's being cyberbullied. And if you think there is a problem, report it.

The National Center for Missing & Exploited Children runs a hotline, both on the Web at *www.cybertipline.com* and via telephone at 800-843-5678. Someone will review your report and forward it to the proper authorities. Let your Internet service provider know, too. ISPs face fines for failing to report child pornography on their systems—fines that the Bush Administration is seeking to raise under the proposed Child Pornography and Obscenity Prevention Amendments of 2006.

Most important of all, you want to educate yourself and your child on the risks that exist online. That way you can reap the benefits of the Internet while skirting the dangers.

"The Internet is a great thing but it's also dangerous—like a swimming pool," says Lin. "Do you want to have fences? Sure. Do you want to have locks? You do. Do you want to have laws that make people liable? Yes. But the safest kid is the kid who knows how to swim."

Alan Cohen is a freelance writer and frequent contributor to PC Magazine.