

## Faculty Insider—i-SAFE Assessments

### Table of Contents

Faculty Insider.....	1
Internet Safety Tip.....	2
i-SAFE at the X Games.....	3
Peer Pressure and Cyber Bullying.....	3
Tech Tip.....	4
Site Spotlight.....	4
Curriculum Bonus.....	5
NAC Corner.....	5
Most Valuable Mentor.....	5
Cyber Security Awareness Month.....	6



*“What ruins mankind is the ignorance of experts.”*

—GK Chesterton

The online student assessments are a vital component of the i-SAFE program. New training offerings are developed and existing ones revised based on what we learn from them. Another important role of our student assessments is to identify and describe the behavioral impacts of i-SAFE training for educators as well as for existing and potential partners and sponsors of our programs.

The participation of your students in i-SAFE’s National Assessment Center (NAC) survey process is not currently required. It is, however, strongly encouraged so that the uniqueness of your location and its student population are represented in NAC findings, which enhances the statistical reliability and validity of the analyses. With a high level of participation in the assessment process, findings on what students are doing online and what works to reduce their online risks can be generalized to American students as a whole with a high degree of confidence.

Students in kindergarten up through grade 12 should take the assessments. In most cases they should be given three assessments each year: (1) a pre-assessment, to be administered prior to any i-SAFE lessons; (2) a post-assessment, to be given shortly after the last i-SAFE lesson of the year; and (3) an outcomes assessment, to be administered approximately three to six weeks after the completion of all training for the year. Students in grades K-2 are the only exceptions. For them, only a post-assessment is used to explore basic computer and Internet use patterns.

The pre-assessments for grades 3-12 focus on Internet use patterns, attitudes, beliefs, and behaviors prior to i-SAFE training. The post-assessments explore changes in attitudes and beliefs about



Internet safety following i-SAFE training. Outcomes assessments identify specific changes in online behavior as a result of i-SAFE training. Topics of exploration, depending on grade level, include cyber citizenship, predator identification and personal safety, cyber bullying (online threats, insults, or harassment), cyber security issues, social networking, intellectual property theft, and cyber-related public health issues (e.g., visiting online sites that support or assist self-injury, or using the Internet to obtain drugs, steroids, cigarettes, alcohol, or pornography).

*continued on page 2*

## NAC Tracks

Which of these terms are your students least likely to know?

- A: Spam
- B: Spim
- C: Computer virus
- D: Trojan horse
- E: Spyware

Vote here


*i-SAFE Assessments* continued from page 1

Administering the pre-assessment typically takes no more than 20 minutes. The post-assessment and outcomes assessment process take only 10 to 15 minutes each. For the first time this year there are separate assessment forms for students in grades 5-8 and 9-12, moving i-SAFE toward a less global and more lesson-focused assessment approach. The change also assesses differences in delivery mode, which varies from middle school (classroom instruction) to high school (webcasts).

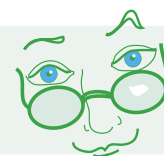
Both middle- and high-school students will be randomly given one of three pre-assessment forms with a different (but overlapping) set of questions on each form. There is only one post-assessment form for grades 5-8; likewise, 9-12. There is also only one outcomes-assessment form for each group. As in years past, there is one pre-assessment form for grades 3-4 and one post- and outcomes assessment form. The outcomes forms for all grades are especially short this year, consisting mostly of checklists, in order to encourage more participation than we obtained in the past.

The Internet is a fast-changing environment. Therefore,



we anticipate replacing several pre-assessment questions in January with new questions to address emerging issues not yet on anyone's radar screen (e.g., MySpace.com a year ago), and to delve deeper into particular issues of interest. Again, please support these vital assessment activities by having your students participate fully. 

## Internet Safety Tip: Carefully Select Your Usernames and Passwords



If you are like most other Internet users, you use a select few usernames and passwords for all of your online activities. While the thought of creating and remembering multiple usernames or passwords can be daunting, it is important that you are thoughtful when creating your accounts online.

Here are a few tips to help you ensure computer and personal safety when using the Internet.

- **NEVER select your password to match your username.**

- **NEVER use passwords that contain info about yourself, family, pets, significant dates, or other personal info that someone could figure out if they knew anything about you.**

- **NEVER use the same password or username on all of your accounts.** If you have used the same password over and over and a hacker acquires it, that person would have no problem accessing the rest of your accounts. Criminals can figure out where you have accounts, or get lucky by trying a number of banking, credit card, or other Web sites with your usernames or passwords.

- **AVOID using words that are in the dictionary.** The best passwords consist of six to eight random alpha-numeric characters using both upper and lower case (ex: 2voNj89!).


- **AVOID adding a number in front, behind, or simply reversing a word** (such as angell1 or l1egna).

- **NEVER give your password to anyone.** No one, including your ISP, bank, or online retailer should ever need you to tell them your password. If you've forgotten your password, use the password retrieval tool present on the Web site.

- **BE AWARE of "shoulder-surfers" who may be watching as you are logging in to accounts or Web sites.**

- **CHANGE passwords frequently.**

- **STORE your passwords securely where passing traffic cannot see.**

- **ERASE the hard drive of your computer completely, using a file-wipe utility when you sell it, give it away, or replace its hard drive.** Simply deleting the data will not completely remove it from your hard drive and criminals could use a data recovery tool to access the data hiding on your hard drive. 

## iSAFE at the X Games—Bob Burnquist, Skateboarder

The Internet is a new way for professional athletes to interact with fans, promote sponsors, and publish their latest feats. With that in mind the iSAFE video production team packed its gear, which did *not* include a skateboard, and traveled to X Games 12 in Los Angeles. Without exception, the athletes we interviewed were enthusiastic about our technology questions, especially the questions about the Internet.

We asked veteran skateboarder and X Games 12 silver medalist, Bob Burnquist, about the Internet's impact on action sports.

"I think it brings the world together. I have 12 sponsors and it's a full-time job to stay in communication and make sure that I'm making all of them happy. The Internet allows me to do that. Now everything is instant. Now something happens, I can post it up on my Web site and I can tell people all around the world that they can get the news first at my Web site without waiting for the magazine articles to come out."

Burnquist has a young daughter, so we asked if he has concerns about the Internet.

"In the world of today, you definitely have to be private with your information. You've got to watch out; don't believe everyone and everything that you see. It's almost like you're stepping outside in public. You're inside your room, but you're really outside and you're in communication. Don't be dumb about it, just be smart and use good sense."



According to Burnquist, technology like the Internet and skateboarding Web sites are helping young, passionate skateboarders achieve success.

"Now everyone can have a hand-held camera that has a really nice look, a professional look. As an amateur skateboarder you can go out and make your own 'sponsor-me' skate video, put it together and upload it to a sponsor, or burn a DVD and send that to a sponsor. It's like, Wow, that's awesome!"

## Peer Pressure and Cyber Bullying

How mean can teenage girls be? A recent episode of the ABC news magazine *Primetime* set out to answer that question in a special hour-long program titled, "Cruel Intentions." The program focused on the potential dangers of cyber bullying. iSAFE President and CEO Teri Schroeder provided host Diane Sawyer with Internet safety expertise, and she assisted in the development of a unique role-play experiment that helped expose bullying among groups of teens using cell phones, instant messaging, and personal Web sites.

During the experiment, different groups of high school students quickly developed rivalries—mercilessly putting down other individuals and groups—in the hopes of being accepted by a popular group of boys. What made being mean so easy? It was the anonymity of the Internet. We learned from the program that the teenagers who participated in the experiment later admitted that the anonymity encouraged them to bully one another, behaving online differently than the way they act in person.

To avoid cyber bullying remember "The 4 Rs":

**RECOGNIZE** "flaming" and cyber-bullying techniques, noting the bully's screen name or address.

**REFUSE** to open or read any message from a cyber bully.

**RESPOND** assertively by leaving the chat room without responding.

**REPORT** cyber bullying to the ISP, the school, or law enforcement and request they help stop it immediately.



## Tech Tip—*Watch Your Wireless*

Many of us are now wireless. It's convenient. It's easy. Just set up your laptop or handheld device and access the Internet to shop, pay bills, read e-mail, do homework, play an online game, or just chat. Right?

Not so fast! Think security first. Wireless surfing—whether at home or in public—can make you an easy target. Savvy wireless hackers don't even have to attack your computer to break into it through a wireless connection. They can just sit and wait for you to provide your information to them.

Most Wi-Fi freeloaders are just looking to surf an open Internet connection, but some may break in to read your hard drive, plant malicious software, or commit criminal activity using your computer address. Worry less about going wireless by following a few basic security steps.

### 1) Secure your system

When you buy a router for wireless surfing at home, its security may not go on automatically. Make sure you enable the router's security. Use a firewall, keep your software and operating system updated and turn off file-sharing.

### 2) Disconnect

When surfing in a public place, like a cyber café, or an airport, don't simply turn off your laptop and leave. Remember to click on the icon that disconnects your computer from the wireless network.

### 3) Be careful shopping

Avoid sending sensitive information when using a wireless network. If that's not possible, make sure the Web site you are using supports a secure connection. A padlock symbol appears in Web browsers when you communicate with a secure Web site.

### 4) Pick a good password

Your login information may be available to the public, unless you change it often. In a recent survey a researcher was able to uncover the default login and passwords for three of




his neighbors with a simple Google search.

### 5) Check webmail security

Is the security for your webmail turned on? Check with your webmail service provider to make sure it's operating.

### 6) Turn off

You should turn a laptop's Wi-Fi function off when it's not being used in order to avoid accidentally connecting to a non-secured network.

Of course, no network is 100% secure. That's the nature of wireless. But even if complete security is an unreachable goal, taking a few simple steps is far better than doing nothing at all. 



[www.connectforkids.org](http://www.connectforkids.org)

The Connect for Kids Web site offers parents, grandparents, educators, and community members tools and information to improve the lives of children, youth and families.

Log on to <http://www.connectforkids.org>. 



## Curriculum Bonus—Preview Certified Mentor Curriculum



Your curriculum bonus this month is a special preview of our new Certified Mentor Training curriculum for i-Adopt-A-School. For those who don't know about this program, middle- and high-school certified i-MENTORS can select from a variety of enrichment or service-learning programs and receive coordinating materials to carry out their projects. **To access the curriculum bonus, go to [www.isafe.org/bonus](http://www.isafe.org/bonus).**

To help i-SAFE certified i-MENTORS as they tackle teaching Internet safety to other students, we've designed a special curriculum on the hot topics that they are most qualified to teach. The lesson plans are designed to coincide

with the mentor's development level and ability. They are laid out in a simple step-by-step formula that includes coordinated activities and resources. i-SAFE supplies everything your students need for success. So take a look at material that will soon be available only to certified i-MENTORS. This month's bonus lesson is designed for older students to teach to students in grades 3-5.

Get your students involved in the i-Adopt-A-School, either as students or teachers. Students can find out more and become i-MENTORS by visiting the X-BLOCK Web site at <http://xblock.isafe.org>.



## NAC Corner—Cyber Security Threats



Most American children today enjoy Internet access at home. According to an i-SAFE National Assessment Center (NAC) survey of 93,661 students in grades 3-12 conducted during the 2005-06 academic school year, 84% now have online access from home. With such a high percentage of our children online and with so many well-known threats to cyber security (e.g., computer viruses, worms, Trojan horses, and spyware) lurking on today's Internet, one might predict that a majority of American parents have at least discussed cyber-security issues with their own children. But, that is apparently not the case. In another survey conducted in 2005-06, the NAC found that, among 2,790 students in grades 5-12, a majority (54%) had never discussed cyber security with their family members. The survey also found that a mere 12% had ever discussed the

need for using anti-virus software or a firewall with their parents.

For students in grades K-12, i-SAFE offers training on a host of cyber-security issues. Depending on grade level, the topics covered may include: what to do with e-mails and e-mail attachments from strangers; how to recognize e-mail hoaxes; the role of anti-virus and anti-spyware software in protecting computers; the importance of a firewall; and, keeping your computer's operating system current by downloading the latest updates and security patches. Specific threats that may be covered in cyber-security lessons include: malicious code, spam, spim, hacking, cracking, phishing, steganography, and much more. Cyber security is considered by i-SAFE to be a core lesson, intended for all students.



## Most Valuable Mentor September 2006

Jamie and Staci, this month's Most Valuable Mentors, are Wyoming sisters and Future Business Leaders of America (FBLA) students. Jamie was i-SAFE trained at an i-SAFE workshop at the 2005 National FBLA Conference, while Staci was trained online by watching the i-MENTOR training videos at <http://xblock.isafe.org/mvm.php>.


The sisters used their training to teach about 40 fifth- and seventh-graders about Internet safety at a local school in their community. They also completed the i-Adopt-A-School program.

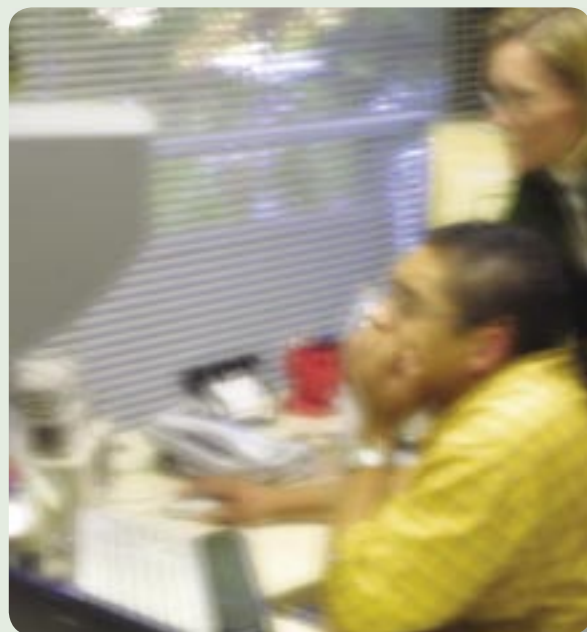
Jamie and Staci won first place at the FBLA State Conference in the community-service project competition, which earned them a trip to the National FBLA Conference. They recently spoke at the FBLA National Conference's i-SAFE workshop and did a press interview with the local Fox television affiliate.

Contact us at [mentors@isafe.org](mailto:mentors@isafe.org) to tell us what you're doing, and you might become the next MVM!



## Cyber Security Awareness Month

October is Cyber Security Awareness Month, a good time to learn to defend against and combat malicious code which can damage your computer. i-SAFE and the National Cyber Security Alliance (NCSA) have teamed up to offer schools a unique student assembly experience. Through the i-SAFE/National Cyber Security Alliance Assembly Experience, students learn how susceptible their computers are to infection and how vulnerable they are to scams and hoaxes while online. They learn best practices to protect themselves and their computers through a series of videos and true-life stories. Using the motto of the NCSA, students are advised to stop and think before they click. Just fill out an Implementation Plan for this assembly. 




## Team Up With i-SAFE

Currently, i-SAFE has reached more than two million students with Internet safety information. By providing free materials, programs, and educational videos, students are learning how to make positive choices when challenged with today's technology. Not only are students learning to protect themselves against predators, they are also learning how to make decisions regarding intellectual property, identity theft, and more.

i-SAFE strives to provide educators, schools, and students with the most current information regarding the issues they face today on the Internet. In order to bring our programs and materials to your school and community, we rely upon donations.

We would be grateful if you, or perhaps someone you know, could assist i-SAFE in reaching as many children as possible. Since i-SAFE is a 501(c)(3) corporation, your donations are fully tax deductible.

To donate, you can e-mail us at [donations@isafe.org](mailto:donations@isafe.org) or go to [www.isafe.org/donations](http://www.isafe.org/donations). 

## We Value Your Input

Do you have a question or a comment about an article? Perhaps you have a story you wish to share with other readers. Do you know somebody whose story will inspire others to get involved? We would like to know. Please e-mail us at [editor@isafe.org](mailto:editor@isafe.org) with questions, comments, or contributions. If snail mail is your preference, **send written correspondence to:**

**i-SAFE Editor**  
**5900 Pasteur Ct.**  
**Ste. 100**  
**Carlsbad, CA 92008**

## About i-SAFE

Founded in 1998 and active in all 50 states, i-SAFE Inc. is the leader in Internet safety education. i-SAFE is a nonprofit foundation whose mission is to educate and empower students, parents, seniors, and community members to safely and responsibly take control of their Internet experiences. i-SAFE provides knowledge that enables them to recognize and avoid dangerous, destructive, or unlawful online behavior, and to respond appropriately. This is accomplished through dynamic K through 12 curriculum and community-outreach programs to students, parents, law enforcement, and community leaders. i-SAFE is the only Internet safety foundation to effectively combine these elements. [www.isafe.org](http://www.isafe.org) 