

## Family Insider—Deleting Digital Data

### Table of Contents

- Family Insider ..... 1
- In Action ..... 2
- Site Spotlight ..... 2
- Internet Safety Tip..... 3
- Get Involved ..... 3
- i-SAFE at the X Games ..... 4
- Peer Pressure and Cyber Bullying ..... 4
- Tech Tip ..... 5
- Most Valuable Mentor ..... 5
- Cyber Security Awareness Month ..... 6

You've researched new computers and decided to make a purchase. The community center needs a computer, so you decide to donate yours. Much to your surprise, you may be donating more than just the computer to the community.

Do you think that digital data just goes away? It doesn't. In fact, it is startlingly durable and accessible to others. By not taking the proper steps to erase your digital history you may be putting yourself and your family at risk.

Completely removing the information on your computer is not as easy as it seems, either. Vital data, such as your financial or medical information, sensitive personal information, private e-mails, or photos can be easily retrieved even after purging it from your computer's trash bin. Special recovery tools can allow even hidden data to be retrieved, if necessary.

While this may be wonderful news to someone who has accidentally deleted important information on the computer, it can be devastating news to the user who has data recovered by a criminal. For this reason, if you intend to donate or resell your computer, you may want to consider using one of the many software products designed to erase the hard drive completely. Only then can you be sure that your information is not on your computer waiting to be recovered.

Cell phone users also appreciate the convenience and privacy of using their hand-held device for calls, e-mail, photos, and text messaging. New reports, however, reveal that digital data you keep on your cell phones could also put you at risk once you dispose of it – even if you believe that you've erased all of the data stored on it.



Cell phone upgrades and resale of old phones and PDAs are frequent. But if you sell your phone or PDA back when you upgrade to a newer model you could pass along any information that you've communicated via phone to the new owner. Sensitive information such as phone numbers, bank account information, and private text messages remain on your cell phone even after you reset it.

Trust Digital, a mobile security software provider, conducted a test that recovered “nearly 27,000 pages of personal, corporate, and device data from nine of 10 mobile devices purchased through eBay for the project,

*continued on page 2*



*“It is difficult to give away kindness. It keeps coming back to you.”*

*~ Cort Flint*

### NAC Tracks

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

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




**Vote here**

**Deleting Digital Data** *continued from page 1*

including a smartphone sold by an employee of a major corporation.” Corporate records and personal information were obtained – including banking and tax information, business secrets, even embarrassing details of extra-marital affairs.

So, what can you do to protect yourself if you decide to upgrade to a new cell phone or PDA? Simply deleting the information will not completely erase it from the

memory of the device. Ask your cellular carrier for advice on how to protect your information and how to “hard-wipe” the data from your phone or PDA before you trade it in or resell it.

Living in the digital age requires consumers to be alert, educated, and proactive. Log on to [www.isafe.org](http://www.isafe.org) to get the most up-to-date news on sensitive issues that affect you and your family. 

**In Action—Get Net Safe Tour in Chicago**

I’m David Leingang. As an i-SAFE Professional Development Manager, I meet with groups of parents around the country who are concerned for their children’s welfare while online. In September, I was privileged to address more than 100 parents at John Whistler Elementary School in Chicago, and Montini Catholic High School in Lombard, Illinois. These i-PARENT presentations were part of the national Get Net Safe Tour.

My work regularly introduces me to parents across America who are seeking good answers to the growing challenge of Internet safety. I am a parent of teenagers who spend a lot of time online, so I know how concerned those parents feel. I found the i-PARENT Program from i-SAFE to be an essential method of educating parents about risks their children face online and I presented it to the parents I met in Illinois. They specifically wanted to know:


- How can I protect my child from Internet predators?
- How can I tell if my child is being cyber-bullied (harassed online) and what should I do about it?
- How can I minimize the chance a virus will infect my personal computer?

These self-appraising parents readily admitted their kids were more cyber-savvy than they were. That did not, however, deter them from actively participating in their

children’s online experience.

The i-PARENT Program from i-SAFE addresses these vital issues and much more. For now, here are some short answers:

- **Children should not reveal personal information since their online “friends” may have lied about their true identity.**
- **Follow this FBI safety tip: Be sure your children understand to never arrange a face-to-face meeting with someone they first met online without telling you.**
- **Children should tell their parents or teachers whenever they encounter anything that makes them feel uncomfortable while online. This includes, of course, being harassed or bullied. If it reaches the point your child is afraid to go to school, inform your local law enforcement agency promptly.**
- **The best defense against cyber attacks is an integrated protection suite of software including a computer firewall, anti-virus, anti-spam, anti-spyware, and anti-adware (also known as pop-up blockers).**

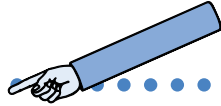
I strongly recommend that parents watch the i-PARENT Online modules. Viewing the modules gives parents more information about how to protect children from online dangers. You can find the i-PARENT modules at <http://ilearn.isafe.org>. 

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>.



## 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 and/or name 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 files/accounts. Criminals could figure out where you have accounts, or get lucky by trying a number of banking, credit card or other Web sites with your usernames and 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 angel1 or 1legna).
- **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, give 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.

## Get Involved—Learn About Internet Safety at Our New Virtual Training Academy

Parents are gradually realizing that they need to learn more about Internet safety in order to protect their children from online predators, cyber bullies and other Internet dangers. Today's students are technologically very savvy and keeping one step ahead of our children is often challenging. As parents, we must not only ensure that we are well educated about the dangers online, but that we continue to learn about emerging Internet safety issues.

i-SAFE understands the time constraints parents live with. This is why we offer versatile methods to educate parents such as the Virtual Training Academy, i-LEARN Online, and live i-PARENT trainings in the community.

The revolutionary i-SAFE Virtual Training Academy (VTA) allows parents to receive live instruction conducted by i-SAFE staff in a virtual classroom with other parents, all from the comfort of their own computers. The Virtual Training Academy is the ideal way for parents to learn about Internet safety in a setting where they can ask questions, discuss issues with other parents, and learn how to raise awareness in their own community.

#### Attend a Virtual Training Academy Parent Training or Parent Program and Get Involved! Here's how:

1. **Log into the i-SAFE Web site at [www.isafe.org](http://www.isafe.org) with your username and password.**
2. **Click on the "Virtual Training Academy" link.**
3. **Click on "Calendar."**
4. **Choose the event you would like to attend by clicking the date under the "Sign Up" column.**
5. **Click on "Confirm".**

You will receive an e-mail with the information you need to join the VTA session and information on how to download materials to be used in your session.

Upon completion of your session you can submit an Implementation Plan enabling you to conduct your own i-PARENT Trainings or i-PARENT Programs in your community to educate other parents about Internet safety issues. It's that easy!

## i-SAFE at the X Games—Bob Burnquist, Skateboarder

The Internet is a way for athletes to interact with fans, promote sponsors, and publish their latest feats. With that in mind the i-SAFE 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 handheld 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. i-SAFE 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

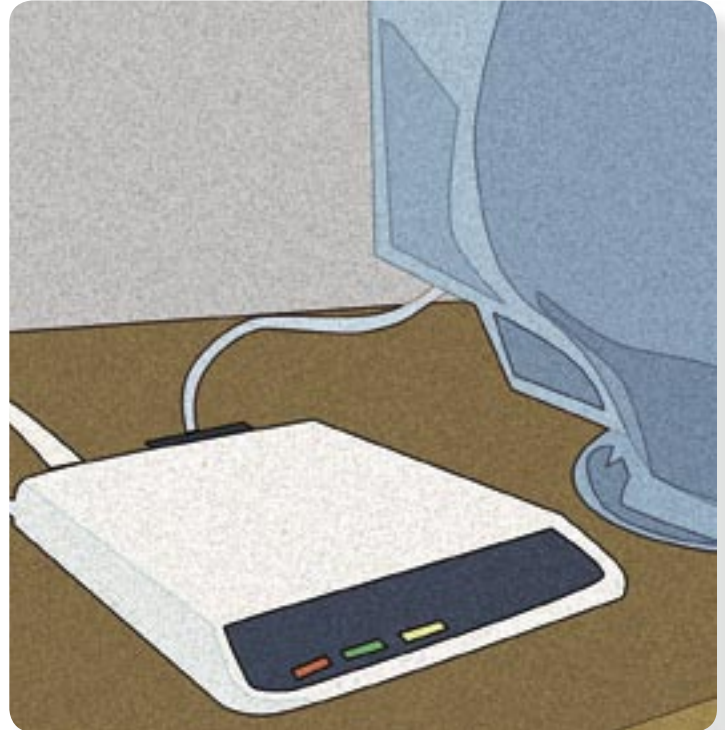
When surfing in a public place, like a cyber café or an airport, don't simply turn off your laptop and leave. Remember to click on the icon that disconnects your computer from the wireless network.

### 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 to avoid accidentally connecting to a non-secured network.

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

## Most Valuable Mentors September 2006

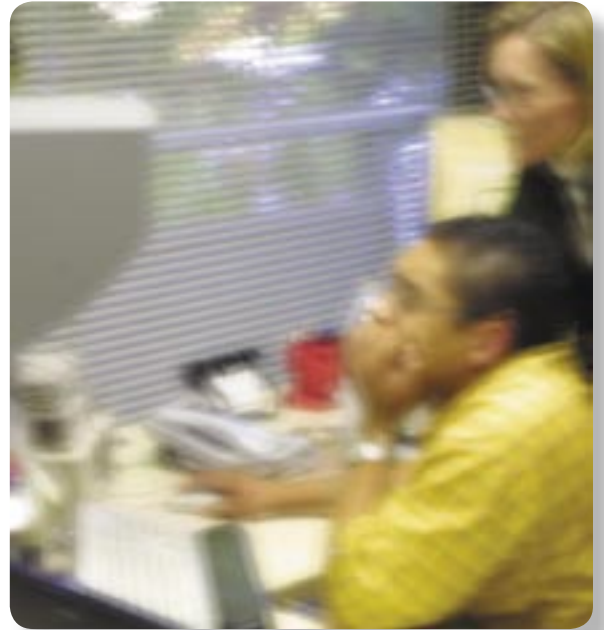
Congratulations, Jamie and Staci, this month's Most Valuable Mentors.

Jamie and Staci are not only certified i-MENTORS, they are sisters. The sisters took first place while attending the Wyoming FBLA Conference in the community-ser-

vice project competition. They won by teaching 40 fifth- and seventh-graders how to practice Internet safety in their school and community. Click <http://xblock.isafe.org/411.php> for more, or e-mail [mentors@isafe.org](mailto:mentors@isafe.org) and tell us what you're up to. *You* could be the next MVM. 

## Cyber Security Awareness Month

October is Cyber Security Awareness Month, a good time to focus on combating 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 your family with the most current information regarding the issues they face today on the Internet. In order to bring our programs and materials to your community and your home, we rely upon donations.

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

To donate, e-mail [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**

The series of i-SAFE newsletters also includes the *i-EDUCATOR Times* and *Kewl Timez* (for students). We encourage you to read the others and ask you to use the main article to initiate discussion and action with your students and your community.

## 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)