

Cyber Bullying Awareness Tip Sheet

Cyber bullying is verbal harassment that occurs during online activities. It can take many forms, including:

- a threatening e-mail
- a nasty instant-messaging session
- repeated notes sent to the cell phone
- a Web site set up to mock others
- “borrowing” someone’s computer and pretending to be them while posting a message
- forwarding supposedly private messages, pictures, or video to others

i-SAFE Inc. has created this list of Internet safety tips (please copy and distribute) to help your family recognize online danger and take appropriate steps to protect yourselves.

• Don’t open/read messages from cyber bullies.

Your child can’t be intimidated by messages from cyber bullies they never open. Teach your child to curb his or her curiosity to read and respond to a message if he or she suspects or knows it’s from a cyber bully.

• Block messages from the bully.

Utilize the blocking features in e-mail programs, chats, and instant messengers to block communications from a bully.

• Encourage your child to tell an adult.

For some children, their reaction to being bullied is not only fright but confusion about how to react appropriately. Coach your child to tell a trusted adult if he or she is being bullied.

• Report cyber bullying.

Internet service providers (ISPs) can often block a cyber bully, and schools have specific procedures and rules to handle bullying. Save the bully’s message and screen name, then contact these sources and report it.

• Don’t chat while angry.

Sending angry, hostile, or taunting messages attracts cyber bullies. Make certain your child is not using e-mail messages or chat rooms to vent his or her anger in a way that hurts others.

• Save the evidence.

Save e-mails or instant messages, or print out the communications; they may be needed to take action.

• If you are threatened with harm, report it!

Even if you don’t know how to identify the individual who has made the threat, law enforcement often has access to the information and may be able to track down and arrest bullies before they do more harm. If it is school-related, tell the school. All schools have bullying solutions.

• Be part of your child’s online experience.

It can be a fun journey to explore the wonders of the Internet as a family. As computer-savvy as kids and teens are today, they may even teach you a thing or two!

• Get involved with i-SAFE Inc.

These are only some of the measures you can take to ensure your child has a safe and enjoyable Internet experience.

Remember the 4 Rs.

RECOGNIZE “flaming” and cyber-bullying techniques, and 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 or with the letter unopened.

REPORT cyber bullying to the ISP, the school, or law enforcement to stop it immediately.

E-mail Threats Tip Sheet

Spam

Spam is any unsolicited message or posting that is sent to multiple recipients, or multiple postings of the same message sent to newsgroups or listservers. Spam is the electronic equivalent of junk mail.

Different studies show that roughly half of all spam mail is related to money—advertising get-rich-quick schemes, debt-reduction plans, and gambling opportunities. A third of spam mail is porn-based, and this figure is set to increase. About 10 percent is health-related, and the remainder covers a wide variety of topics.

i-SAFE Inc. has created this list of tips to help you respond appropriately to spam.

• **Protect your e-mail address.**

- Avoid giving your personal e-mail address to anyone other than family, friends, or business associates.
- Create and use a separate e-mail address for public use (i.e. for posting on Web forums, or registering or purchasing online, etc.).
- Before registering on a Web site, read the site's privacy policy to ensure that your e-mail address will not be shared or sold to a third party.
- Never display your e-mail address openly online, such as on public forums, in chat rooms, or in profiles.
- When forwarding e-mails to others, copy and paste the text into a new e-mail before sending. Simply clicking "Forward" also forwards the e-mail address(es) of the prior recipients of the e-mail. Remind friends and family to use this technique to avoid having your e-mail address forwarded to a person(s) you do not know.

• **Use technology to block spam.**

- Check with your Internet service provider (ISP) to see what spam-blocking utilities it offers and how to activate them.
- E-mail clients, such as Microsoft Outlook Express, have spam-blocking features and message rules that can block e-mail from unwanted sources. Check the "Help" tab to determine how to activate these features in your e-mail client.

• **Never respond to spam.**

- Ignore the "Unsubscribe" links in spam e-mails. If the e-mail you received didn't require a subscription, there is little probability that you will stop the spam e-mails by unsubscribing. Instead, by responding to the e-mail, you are essentially validating that your e-mail address is active and being read. Professional spammers will often subsequently sell your e-mail address to other spammers.

• **Report spam e-mails.**

- The United States has the CAN-SPAM ACT (Controlling the Assault of Non-Solicited Pornography and Marketing Act). To report any spam e-mails, forward a copy of them to spam@uce.gov.

E-mail Threats Tip Sheet

Phishing

Identity thieves often “phish” for information by sending e-mail spam or pop-up messages that appear to be legitimate businesses or organizations (i.e. bank or online payment services that you may deal with). These phishers lure their victims to counterfeit Web sites that appear to be the legitimate sites. However, they are intended to trick you into divulging information needed to steal your identity or perform fraudulent acts. Viruses or malicious programs often accompany e-mails and are secretly downloaded onto your computer to gather your personal and financial information.

Recognizing phishing e-mails is not always easy. Here are some tips to help you.

- **Watch for bad spelling and grammar.**

A careless scammer often makes spelling and grammar mistakes that would otherwise be caught by a legitimate company’s proofreaders.

- **Be aware of generic greetings.**

Most companies will address you by your name or Web site username when corresponding with you. Generic greetings, such as “Dear Valued Customer,” should raise a red flag. Companies are not likely to send e-mails requiring urgent requests for personal information.

- **Look out for account suspension or cancellation warnings.**

Scammers often use these scare tactics to trick their victims into disclosing personal or financial information.

Here are some helpful tips and reminders that can be used to avoid and respond appropriately to e-mail threats.

- **Never directly respond to pop-up messages or e-mails asking for personal or financial information.**

Contact the organization via telephone, or go to the organization’s Web site to verify your updated information. Legitimate companies never ask for customer information by way of pop ups or e-mails.

- **Never click on links within e-mails.**

Open a new browser window, and directly type in the organization’s Web site address—never copy and paste the link from the e-mail into the address bar. Phishers create links that look like legitimate Web site URLs and then redirect their victims to phony Web sites.

- **Be cautious about opening e-mails or attachments, or downloading files from e-mails, even if they appear to be from someone you know.**

Scammers often spoof e-mail addresses to trick victims into believing they are receiving e-mails from someone familiar. Best advice: If you receive an e-mail with an attachment or file, contact the sender to see if they actually sent you the e-mail. If so, save it to your hard drive, and run a virus scan before opening it.

- **Never use e-mail to provide personal or financial information to an organization.**

E-mail is not a secure method of transmitting personal data. If you must provide your personal or financial information online, go to the organization’s Web site and look for the lock icon, which is on the browser’s status bar on the bottom left-hand corner or the “https” in the URL address bar, to ensure it is a secure Web site.

E-mail Threats Tip Sheet

- **Use antivirus, spam filters, pop-up blockers, and antispyware software to further protect your system.**

Antivirus software is essential to protect your computer from malicious codes that might accompany spam. Using spam filters and pop-up blockers will reduce the amount of spam you get and lessen the number of phishing attempts. Install antispyware software to detect programs that have unknowingly been installed to track your online activities or gather information without your knowledge. To ensure that new threats are recognized, enable your software programs to regularly update via the manufacturer's Web site.

- **Install a firewall.**

A firewall creates a barrier between you and the Internet, providing a further layer of protection against computer threats. A firewall is especially important if you have a broadband or other high-speed Internet connection.

- **Act immediately if you believe you have been hooked by a phisher!**

Notify your account holders immediately. Don't forget to contact the credit bureaus and request a fraud alert on your credit files.

Internet Frauds and Scams Tip Sheet

The Internet has become a widely used method of selling and purchasing items. Many legitimate companies sell products and services online. However, because it is inexpensive and affords a level of anonymity, there are also many fraudulent companies and individuals using the Internet as a vehicle to lure and scam people.

Here are some of the most common scams and frauds you may face when using the Internet.

“Get-Rich-Quick” Schemes

The Internet is full of claims to get rich quickly and easily. If it sounds too good to be true, it most likely is!

Business Opportunities/Work-at-Home Offers

These offers promise quick, maximum income for minimal labor at no risk—and the convenience of working from home. Often you are enticed to send money for products to sell, or instructional materials, but you never receive the goods. You may also be required to pay hidden costs to place newspaper ads, make photocopies, or buy supplies, software, or equipment to do the job. Once you complete your assignment, you may find that your employers refuse to pay you, claiming that your work isn't up to their “standards.”

Foreign Lotteries

Foreign lottery e-mails boast incredible odds and large payouts. The e-mail may even claim that you've already won, and all you must do is pay to collect your winnings. It's illegal for a company to require you to buy something or pay a fee in order to win or claim a prize. Besides being terribly risky, participating in a foreign lottery violates U.S. law.

Online Auctions

You can find almost anything at an online auction. However, sellers may not hold up their side of the bargain, or merchandise may have been misrepresented.

Charity and Disaster-Related Scams

Fraudulent charities often appeal to your patriotism and take advantage of disasters to trick people who want to help victims. Some crooks try to fool people by using names similar to those of well-known charities to tug at your heart strings and convince you to help the less fortunate.

Nigerian E-mail Scam

These e-mails are from crooks in Nigeria, or another country, who claim they need your help accessing money being held in a foreign bank. Their purpose is to steal your money or commit identity theft. If you assist them in accessing their money, they will transfer lots of money into your bank account in payment for assisting them. Inevitably, emergencies come up requiring more of your money and delaying the “transfer” of funds to your account. Ultimately, the scam artist vanishes with your money.

Medicare Rx Drug-Coverage Scam

Con artists are trying to cash in on the new Medicare discount drug card program by offering phony Medicare prescription plans. Their main objective is to steal your money or personal information.

Medical Scams

E-mails claiming that a product is a quick and effective cure for ailments or diseases, and that there's a limited availability, require payment in advance and offer a no-risk, money-back guarantee. Most include testimonials from customers or doctors verifying its effectiveness. All are intended to steal your money or identity.

Credit Card Fraud

Fraudulent credit card offers often promise to repair credit reports for a “fee” or to get credit cards for persons with credit problems. If your credit history is bad, your best bet is to use a well-known bank and get a “secured” credit card to rebuild your credit rating. You can correct inaccurate data on your credit report by contacting the credit-reporting agencies.

Travel Fraud

Fraudulent companies often offer free or low-cost trips to lure people into buying their products or services. A “free” or incredibly cheap trip may have hidden costs or restrictions, require you to use a specific company whose costs are higher, or take your money and never actually place the reservations for your travel.

Internet Frauds and Scams Tip Sheet

i-SAFE has created this list of tips to help you avoid and respond to Internet fraud and scams.

- **Never respond to unsolicited e-mails.**

To stop communications from a company or charity, contact the sender by phone or by going directly to the web page to request that you be removed from their contact list. Never click on links within e-mails or hit reply. Replying often verifies that your e-mail is valid and results in even more unwanted messages from strangers. The best approach may be to delete the e-mail.

- **Beware of imposters.**

Fraud e-mails often pretend to be connected with a business or charity, or have a Web site that looks just like a legitimate company or charitable organization. Contact the legitimate company or charity directly if you are interested in the offer or request.

- **Guard your personal information.**

Never provide personal information, including credit card or bank account numbers, to anyone unless absolutely necessary. Revealing your social security number should never be necessary unless you are applying for credit. Businesses with whom you already have an account will never request information that they should already have. They should not have to verify any information from you via e-mail.

- **Be cautious of file attachments.**

Opening file attachments and downloading files puts you at risk for viruses, spyware, and identity theft. Fraudsters often use spyware to obtain your personal information or download code that connects your modem to a foreign telephone number, resulting in expensive phone charges.

- **Know with whom you're dealing.**

Do your homework: Check out the company or charity by contacting the consumer-protection agency and the Better Business Bureau. Try to get the physical address and phone number in case there is a problem later. Check with Medicare to make sure that the plan you're considering is approved. If buying on an auction site, read the buyer feedback responses to gain useful information about other people's experiences with particular sellers.

- **Stay on guard.**

Be aware that "no complaints" does not mean that a business is legitimate. Fraudulent companies often don't stay in business under one name for long. The fact that there has been no complaint made against a company does not mean it is legitimate.

- **Resist pressure and time-sensitive appeals.**

Legitimate companies and charities don't use pressure or scare tactics to force you to make a decision. If a company or charity demands that you act immediately or is too persistent, it is most likely a scam.

- **Think twice before entering contests.**

Fraudulent marketers sometimes use contest entry forms to identify potential victims.

- **Do not believe promises of large sums of money for your cooperation.**

Why would a total stranger want to make you rich?

- **Monitor your credit report!**

Periodically, check your credit report for accuracy. Maintain a list of all your credit cards and account information along with the card issuer's contact information. If anything looks suspicious or you lose your credit card(s), you should contact the card issuer immediately.

To determine where to report specific Internet crimes, visit <http://www.cybercrime.gov/reporting.htm>, and forward all suspected fraud e-mails to spam@uce.gov.

Identity Theft Tip Sheet

Identity theft is the fastest growing crime in the United States!

A Federal Trade Commission (FTC) study reported that nearly 10 million people were victims of identity theft in 2003.

Don't become a victim!

i-SAFE Inc. has created a list of helpful tips and reminders that can be used to help recognize potentially hazardous situations and to teach you how to respond appropriately.

- **Monitor your credit card situation regularly.**

Obtain your credit report at least once a year from at least one of the three major credit bureaus (Equifax, Experian, and TransUnion), and look carefully for any unusual or fraudulent activity.

- **Beware of all requests for your personal information online.**

Legitimate companies will not send unsolicited requests for personal information (addresses, account numbers, passwords, social security numbers). A good rule of thumb is to never give out this type of personal information unless you have a trusted business relationship with the requestor and you initiate the correspondence.

- **Do not respond to unsolicited e-mails, links within e-mails, or pop-up ads.**

Fraudsters often use spam, spyware, and adware to acquire information from potential victims.

- **Never reveal personal information in e-mails, on instant messages, in profiles, on bulletin boards, or in chat rooms.**

Con artists often intercept personal information sent electronically over the Internet to steal their victim's identity.

- **Use a firewall to further protect your computer from intrusions.**

Firewalls offer an extra layer of protection against hackers trying to gain access to your computer and the information stored within.

- **Shred all documents that you plan to throw away.**

These documents include bank statements, preapproved credit card offers, utility bills, and any other documentation with your social security or account numbers.

- **Protect and store personal information at home.**

Ensure that files and documents are safely stored and inaccessible to visitors to your home (i.e. repair persons, casual acquaintances, etc.).

- **Don't carry your social security card (unless absolutely necessary).**

Any item containing your social security number can be an inviting target to identity thieves.

- **Take your outgoing mail to your local post office.**

Send bills, checks, or other personal correspondence from a secure location. Residential mailboxes without locks are open targets to identity thieves.

- **Install a locking mailbox at your residence.**

Criminals often obtain the information they need by intercepting mail in unlocked street mailboxes.

- **Notify law enforcement if you see someone "dumpster diving."**

People rummaging through garbage may be looking for unshredded documents that contain valuable personal information.

- **Beware of "shoulder surfers."**

These people look over your shoulder as you fill out forms or provide passwords and secret codes. Hide from others any papers, receipts, notes, or any other documents with passwords, personal identification (PIN) numbers, social security numbers, account numbers, and other personal information.

- **Place a fraud alert on your credit.**

This is a first line of defense if you have lost your wallet, purse, social security card, passport, or if you suspect you may be a victim of identity theft. Contact each of the three credit bureaus for assistance.

Internet Safety Tips for Parents

Online predators are out there!

They can infect your computer with viruses; they want to steal your personal information and possibly your identity; and they may be out to harm you or the people who use your computer.

i-SAFE Inc. has created this list of tips and reminders to help you recognize potentially hazardous situations and teach you how to respond appropriately.

- **Have the family computer in an open area.**

Never place it in your child's bedroom.

- **Keep the lines of communication open.**

Rather than "policing" your child's online behavior, keep the lines of communication open. Talk to your children about online predators, identity theft, viruses, and other online dangers. Let them know that they can come to you if they are ever in an uncomfortable situation.

- **Become a part of your child's online experience.**

It can be a fun journey to explore the wonders of the Internet as a family. As computer-savvy as kids and teens are today, they may even teach you a thing or two!

- **When using e-mail, beware of opening unsolicited attachments.**

Viruses, worms, and Trojan horses can be activated by unsuspecting e-mail users opening infected attachments to e-mail messages. Viruses can "spoof" the sender of the e-mail, making it look like someone you know sent the message. Use updated antivirus scanning software regularly to monitor your computer.

- **User names and profiles can provide a wealth of personal information.**

Ask your child about his or her online user name, profile, and downloading activities. Having too much information in user names and profiles can attract predators. Examples of dangerous user names are surfergirl15 or hiphopboy14. We suggest creating a family profile, not an individual profile for your child.

- **Know intellectual property and copyright regulations.**

Downloading music and movies illegally can result in lawsuits and heavy fines against parents. If your child is using file-sharing programs for downloading music, it can also open up your computer to identity thieves by giving access to your personal information. Talk to your child about the consequences of this type of behavior, and emphasize that intellectual-property theft is a crime, not just an inconvenience.

- **Learn about the Internet.**

The more you know about how the Internet works, the more you can be informed about how online predators and identity thieves work, and what you can do to stop them.

- **Get involved with i-SAFE Inc.**

Make a difference! Talk to other parents about online hazards, and help raise Internet safety awareness by joining an i-PARENT Board.

Malicious Code Tip Sheet

According to a study done by the Pew Internet & American Life Project, 68 percent of home Internet users, or about 93 million American adults, have experienced at least one computer problem related to malicious code, adware, or spyware in the last year.

Internet users with Internet connections that are always on, such as broadband, DSL, or cable connections, are at greater risk of becoming victims of malicious code.

Malicious code is a computer program that modifies, destroys, or steals data, allows unauthorized access to your computer, and exploits or damages a system.

A computer virus is a type of malicious code that infects or attaches itself to other computer programs to perform malicious or mischievous acts, such as erasing or editing files, or locking up systems.

Worms are self-propagating computer viruses embedded in a file that create copies of themselves, which in turn create even more copies as they travel through a computer network and/or across the Internet by various means, most frequently via e-mail.

Trojan horses, named after the wooden horse from Greek mythology in which Greek soldiers snuck into the city of Troy, are malicious codes that appear harmless, but when executed, can launch a virus or worm. Trojans may also be hidden inside another program, so when the innocent program is installed, the Trojan program also is installed. Once installed on the victim's computer, the other party is notified each time the victim is online. The remote attacker then has virtually unfettered access to most aspects of the victim's computer, allowing him to access personal information and files, and have control of the victim's computer.

Spyware refers to software that hides on your computer with the purpose of collecting your personal information and computer activities, and reporting them back to the one who distributed the spyware.

Adware, a close relative of spyware, is software that downloads to your computer to play, display, or download advertising material to a computer. In addition to being an annoyance, adware slows down your computer and often contains inappropriate content.

You may have malicious code, spyware, or adware on your computer if:

- pop-up ads appear when you are not connected to the Internet
- your browser home page has changed without your consent
- a new toolbar is present on your browser
- your computer takes longer than usual to complete certain tasks
- your computer is suddenly taking a long time to perform certain tasks, unexpectedly begins doing strange things, or crashes without warning

Remember to turn on your computer's firewall, keep the operating system up to date, and use up-to-date antivirus and antispyware software.

Malicious Code Tip Sheet

Malicious code can be spread through just about any computer medium, including e-mail, infected floppy disks, instant messages, file-sharing services, and pop-up ads.

i-SAFE Inc. has created this list of security tips to help you recognize, avoid, and respond appropriately to malicious code.

- **Install antivirus software, and update it regularly.**

Antivirus software only protects your computer if it is running. Set the program to auto-start when the computer is on. Set your software to auto-update from the manufacturer's Web site. If virus protection is out of date, it cannot detect the newest viruses, worms, and Trojan horses being created daily.

- **Do not open e-mails or attachments from persons or businesses you do not know.**

- **Always scan incoming e-mail attachments before opening them.**

Even if the e-mail is from someone you know, save attachments to your desktop, then scan with your virus-protection software before opening. Viruses can spoof the sender of the e-mail, making it appear that it was sent by someone you know.

- **Downloading files is risky business!**

This includes freeware, screensavers, games, and any other executable program (files with extensions like .exe, .pif, or .scr). File-sharing and downloading media is very risky. Always save files to your hard drive, and virus scan before opening.

- **Beware of the floppy disk.**

Scan all floppy disks before using. Never leave a floppy disk in the computer when not being used. If a floppy is infected with a boot sector virus and is in the floppy drive when the computer is rebooted, the infection will be transmitted to your system.

- **Keep your operating systems patched.**

Operating system vulnerabilities are discovered almost daily. Windows updates should be set to update at least weekly to make sure your computer is protected.

- **Never click "Yes" when prompted to install or run content from a web page that you are not sure you can trust.**

Just say "No," or if given the option, save to your hard drive, and virus scan before opening.

- **Install antispyware tools in addition to your virus-protection software.**

Spyware is designed to hide on your computer and monitor and report your personal information and Internet activity to the remote attacker. Antispyware software that can detect and remove spyware from your computer is available.

- **Always read the user agreements, privacy statements, or other disclaimers before downloading or installing programs.**

Programs that you install can contain spyware. By accepting the user agreement, you are giving permission to download spyware to your computer.

- **Use a firewall to further protect your computer from intrusions.**

Predator Tip Sheet

Eluding Internet Predators

One in five children who use computer chat rooms has been approached over the Internet by a pedophile.

Only one in four youth who received a sexual solicitation reported the incident to an adult.

i-SAFE Inc. has created this list of tips and reminders that can be used to help recognize these potentially hazardous situations and to respond appropriately.

- **Keep user names and profiles generic and anonymous.**

Discuss your child's online screen name, profile, and activities. Many provide too much personal information. Ensure all screen names and profiles are nonspecific.

- **Avoid posting personal photos online.**

Pictures can be altered to embarrass or humiliate. They also provide personal information that can help an Internet predator act familiar by pretending to know you, your children, and/or their friends.

- **Always keep private information private.**

With just three pieces of personal information, specialized Internet search engines can be used to locate someone anywhere. Internet conversations should never include any personal information.

- **Place the family computer in an open area.**

A responsible adult should always accompany minors while they access the Internet to provide support and direction should they be confronted with an aggressive solicitation or inappropriate materials.

- **Remind children that online "friends" are still strangers.**

Predators trick their victims into believing that they have similar interests and groom children to desire a more intimate relationship. The reality is that online friends are still strangers, and your child can never be sure that the person is who he or she says.

- **Respect children's privacy.**

Respect your child's privacy, but make certain he or she knows everyone on his or her e-mail or instant messenger "Buddy" list. Work to generate parent and child trust that supports open and honest Internet use.

- **Become a part of your child's online experience.**

It can be a fun journey to explore the wonders of the Internet as a family. As computer-savvy as kids and teens are today, they will certainly teach you a thing or two!

- **Be aware of phone calls or mail deliveries from unfamiliar persons.**

Predators often call or send gifts to their potential victims in their process of grooming.

- **Learn about the Internet.**

The more you know about how the Internet works, the better prepared you are to teach your children about how online predators operate and what you can do together to identify and elude them.

- **Get involved with i-SAFE Inc.**

Raise Internet safety awareness by joining, creating, or supporting an i-PARENT Board in your school or community, and informing other parents what they can do to keep their families safe online.

Social Networking Tips for Parents

i-SAFE Inc. has created this list of social-networking tips and reminders that can be used to help avoid potentially hazardous situations and to respond appropriately.

- **Set rules concerning social-networking sites.**

Never reveal personal information online. Educate your child on the dangers of revealing personal information online. Ensure that your child knows not to post any personal information in his or her profile or in the content of his or her Web space. Other than the obvious, this includes e-mail address, instant-message (IM) contact information, sports teams, places frequented, or any other information that could allow a stranger to identify or contact them.

Follow Web site age restrictions. Most sites require users to be 13 and older. If your child is younger than the age limit, do not allow them to use the site.

Activate security settings on the Web site. Have your children password-protect their web pages and set permissions to allow only persons they know to view and post to their bulletins.

- **Discuss the dangers of communicating with strangers online.**

Online friends are strangers, not “real” friends. Remind your child that he or she is never to meet an online friend in person, and if asked to do so, to notify you immediately.

- **Evaluate the Web site.**

Read the Web site’s privacy policy and code of conduct. Find out if the site monitors and removes inappropriate content posted on user pages.

- **Spend time online with your child.**

Ask your child to show you his or her social-networking page. Unfamiliar friends and inappropriate content can factor into a dangerous equation.

- **Establish rules for posting pictures online.**

Posting photographs openly online is dangerous. Details in photos could provide predators with identifiable information, such as street signs, license plates, and school or city locations. Photos can also be inappropriately altered. When sharing photos online, use password-protected online photo sites, and only reveal the password to persons you actually know.

- **Talk with your children about the power of words.**

Remind your child that anything posted online has the potential of being read by anyone, including parents, principals, bosses, school officials, or friends. The things they say could be copied and passed around, or discovered by someone using a search engine. Cyber bullying often starts and continues on social-networking sites. Businesses and universities often perform Web searches on potential employees and students.

- **Restrict children from joining public groups.**

Public groups require identifiable information, such as specific interests like groups of students that go to a specific school or live in a specific city.

- **Report cyber bullying, or inappropriate or dangerous content.**

Notify the Web site by clicking on the “Report Abuse” link. If there is no link, look for a “Contact Us” link to obtain contact information. If you suspect someone is a criminal or predator, print out a copy of the communication and Web site address, and report it to your local law-enforcement agency.

Intellectual Property Tip Sheet

Protecting Intellectual Property

Reproducing and/or distributing digitized copyright-protected or licensed materials without permission is a violation of federal law.

i-SAFE Inc. has created this list of tips and reminders that can be used to help recognize what is and isn't protected material to avoid violating the law.

- **Don't copy or download commercial computer software.**

With the exception of shareware, "borrowing" a CD from someone and downloading computer programs or games onto your computer for your own use constitutes theft even if you return the CD.

- **Be careful when using "sharing" software.**

By using software programs like Kazaa, iMesh, and gnutella, users can unknowingly be allowing others to share files—as well as personal files—illegally with everyone on the Internet. Additionally, viruses are often hidden in files being shared on the Internet.

- **Always cite the information source.**

Copying written materials from the Internet without citing the sources is plagiarism. Students should avoid the temptation to submit research papers purchased on the Internet as their own.

- **Get permission before downloading copyrighted materials.**

Books, magazines, videos, computer games, and music require the permission of the author, publisher, or artist when copying, downloading, and using, even for personal use. Free doesn't mean legal.

- **Download media legally.**

There are a growing number of free or "pay for" sites available where you can legally acquire media. Research the site before downloading to ensure that the site is legal and has permission to distribute copyrighted materials.

- **Become a part of your child's online experience.**

It can be a fun journey to explore the wonders of the Internet as a family. As computer-savvy as kids and teens are today, they may even teach you a thing or two!

- **Learn about the Internet.**

The more you know about how the Internet works, the better prepared you are to teach your children about how online predators operate and what you can do together to identify and elude them.

- **Get involved with i-SAFE Inc.**

Raise Internet safety awareness by joining, creating, or supporting an i-PARENT Board in your school or community organization, and informing other parents how to keep their families safe online.

Online Personal Safety Tip Sheet

The Facts!

- One in five children who use computer chat rooms have been approached on the Internet.
- A study by the NOP Research Group in 2002 found that of the four million children aged seven to 17 who surf the 'net, 29% would freely give out their home address, and 14% would freely give out their e-mail address if asked.
- According to the U.S Department of Justice, there are 250,000 to 500,000 pedophiles in the United States. This equates to approximately one pedophile for every 100 to 200 Internet users.
- According to the National Telecommunications and Information Administration, there are two million new Internet users per month. Do you know with whom you are chatting?

Consider This!

Thirteen-year-old Kacie Woody liked to play soccer, sing, and chat online. On December 3, 2002, she vanished from her home in Holland, Arkansas. Police found her body, along with that of her abductor, 19 hours later in a storage facility. She had been murdered by 47-year-old David Fuller of La Mesa, California, who then committed suicide. Kacie's friends told police that she had had an ongoing online relationship with some boy named David, whom she believed was another teenager. Signs of a struggle at her home indicated that she was unaware that he was coming to see her and unwilling to go anywhere with him.

Online Social Networks

MySpace, Xanga, Facebook, TagWorld—which site are you on? And on which sites are online predators? The answer may be all of them, at least for predators. Think about it: A profile is free, and anyone can lie about his or her age, or post a fake picture. Who are you really talking to?

- *Connecticut – In a span of a few weeks, nine girls reported sexual abuse from adults they met on MySpace.*
- *Texas – A 15-year-old was lured from home and assaulted by an adult met on MySpace.*
- *California – A 12-year-old was sexually assaulted by an adult met on MySpace.*

Rules of the Road

- *Don't give out identifying information on the Internet, such as your full name, address, age, school, and phone number.*
- *Review your screen name and see if it reveals too much information about you.*
- *Check your profile. You may be displaying information about yourself that predators can use.*
- *Screen your buddy list. Do you really know who's on it?*
- *Tell a trusted adult or police officer if you or a friend gets into a dangerous situation.*
- *Be aware of strangers asking too many personal questions and trying to become friends quickly.*

Remember the 4 Rs

RECOGNIZE techniques used by online predators to deceive their victims.

REFUSE requests for personal information.

RESPOND assertively if you are ever in an uncomfortable situation while online. Exit the program, log off or turn off the computer, and notify your internet service provider (ISP) or local law enforcement.

REPORT to law enforcement authorities any suspicious or dangerous contact that makes you uncomfortable.