

Student Tip Sheets

Online Music Tip Sheet

Isn't it great that so much music is available on the Internet? You can listen when you want, and download music files to add to your music library. i-SAFE encourages you to do all of that, as long as your online music experiences are legal from Web sites that are appropriate for students.

The American Society of Composers, Artists and Publishers (ASCAP) has provided the following list of Web sites where you can access and enjoy music legally. However, before visiting these sites or purchasing any music online, i-SAFE encourages all students to discuss with a parent or a trusted adult whether these sites are appropriate for you.

Legal Music (Download Stores)

- www.rhapsody.com
- www.iTunes.com
- www.emusic.com
- www.napster.com
- music.yahoo.com
- www.zune.net
- www.broadjam.com

Free Legal Music

- www.myspace.com
- music.download.com/2001-1_32-0.html
- music.podshow.com/
- www.amazon.com
- www.purevolume.com
- www.thedelimagazine.com
- hype.non-standard.net/
- www.oddioverplay.com

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.

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.

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.

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.