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

- **Have the family computer in an open area –** Never in your child's bedroom.
- **Respect your child's privacy –** Rather than "policing" your child's online behavior, keep the lines of communication open with your child. Talk to your child about online predators, identity theft, viruses, and other online dangers. Let them know that they can come to you if they ever find themselves 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 anti-virus scanning software regularly to monitor your computer.
- **Usernames 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 is illegal and 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, emphasizing 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 America –** Make a difference! Talk to other parents about online hazards, and help raise Internet safety awareness by joining an i-SAFE Community Action Team.

Remember the 4 R's

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 or local law enforcement.

REPORT, to law enforcement authorities, any suspicious or dangerous contact that makes you or your child feel uncomfortable.

i-SAFE America Cyberbullying Tip Sheet

Boys are as likely as girls to be targeted on the Internet by threats or efforts to humiliate them.

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

- ***Don't open or read messages from cyber bullies***
  Your child can't be bullied if they don't open or read messages from cyber bullies. Teach your child to curb his or her curiosity to read and respond to a message once he or she recognize a cyber bully has sent it.
- ***Encourage your child to tell an adult***
  For some, their reaction to being bullied is not only fright, but also embarrassment and confusion of what the right thing is to do. Coach your child to tell a trusted adult if they are ever being bullied.
- ***Report chat bullying to the ISP***
  Internet Service Providers (ISPs) can often block a cyber bully. Save the bully's message and the screen name, then contact and report it to your ISP and request they be blocked.
- ***If it's related to school, inform an administrator***
  Schools have specific procedures and rules to handle bullying of all types—including cyber bullying. Use the school as a resource to resolve conflicts between students before they cause greater harm.
- ***No chatting while angry***
  Sending angry, hostile or taunting messages attracts cyber bullies. Make certain your child knows netiquette and is not using email messages or chat rooms to vent their own anger in a way that hurts others.
- ***If you are threatened with harm, tell the police***
  Even if you don't know how to identify the individual who has made the threat, law enforcement has access to information and may be able to track them down and arrest them before they do harm.
- ***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 America***
  Raise Internet safety awareness by joining, creating, or supporting an i-Parent Board in your school or community organization and informing other parents what they can do to keep their families safe online.

Remember the 4 R's

RECOGNIZE techniques used by identity thieves to obtain people's personal information.

REFUSE to become a victim! Protect your personal information and only provide it when absolutely necessary.

RESPOND assertively if you suspect you may be an identity theft victim. Contact the three U.S. Credit Bureaus and put a fraud alert on your credit.

REPORT any unusual or fraudulent activities you notice on your credit report, "dumpster divers," or e-mail scams that you encounter, to local authorities.

Caution is the key to eluding Internet predators.

Only 1 in 4 youth who received a sexual solicitation reported the incident to an adult.

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

- *Keep Usernames and profiles generic and anonymous*
  Discuss your child's online screen name(s), profile(s), and activities. Many provide too much personal information. Ensure all screen names and profiles are nonspecific and purposely vague.
- *Avoid posting personal photos*
  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.
- *Respect children's privacy*
  Respect your child's privacy but make certain they know personally everyone on their e-mail "buddy" list. Work to generate parent and child trust that support 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!
- *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 America*
  Raise Internet safety awareness by joining creating or supporting an i-Parent Board in your school or community organization and informing other parents what they can do to keep their families safe online.

Remember the 4 R's

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 or local law enforcement.

REPORT, to law enforcement authorities, any suspicious or dangerous contact that makes you or your child feel uncomfortable.

i-SAFE America Intellectual Property Tip Sheet

Protecting intellectual property is everyone's responsibility.

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

i-SAFE America has created this list of helpful tips and reminders that can be used to help recognize what is and what isn't protected materials and to avoid violating the law. recognize these potentially hazardous situations and how to respond appropriately.

- **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 such as KaZaa, iMesh, and Gnutella, users can unknowingly be allowing others to share files illegally—as well as your personal files—with everyone 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 to copy or download and use, even for your own personal use. Free doesn't mean legal.
- **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 America**
  Raise Internet safety awareness by joining, creating or supporting an i-Parent Board in your school or community organization and informing other parents what they can do to keep their families safe online.

Remember the 4 R's

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 or local law enforcement.

REPORT, to law enforcement authorities, any suspicious or dangerous contact that makes you or your child feel uncomfortable.

i-SAFE America Identity Theft Tip Sheet

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

A Federal Trade Commission study reports that nearly 10 million people were victims of identity theft in 2003. Don't become a victim!

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

- **Monitor your credit situation regularly.** Obtain your credit report at least once a year from at least one of the three major credit bureaus (Equifax, Experian, and Trans Union) 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 ((SSN)). 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.
- **Shred all documents that you plan to throw away.**
    These documents include bank statements, pre-approved credit card offers, utility bills, and any other documentation with your Social Security or account numbers.
- **Don't carry your Social Security Card (unless absolutely necessary).**
    Any item containing your SSN 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 info they need by intercepting mail in unlocked mailboxes on the street.
- **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 your passwords, PIN numbers, Social Security Number, 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

Remember the 4 R's

RECOGNIZE techniques used by identity thieves to obtain people's personal information.

REFUSE to become a victim! Protect your personal information and only provide it when absolutely necessary.

RESPOND assertively if you suspect you may be an identity theft victim. Contact the three U.S. credit bureaus and put a fraud alert on your credit.

REPORT any unusual or fraudulent activities you notice on your credit report, "dumpster divers," or e-mail scams that you encounter, to local authorities.