



Internet Safety Day

9.28.14

Parent Guide

Developed By:
Family Safe Computers
www.FamilySafeComputers.org

www.InternetSafetyDay.com

WHY INTERNET SAFETY DAY?

Internet Safety Day

Internet Safety Day or ISD is a day to create awareness about Internet and technology safety. This event is purposely chosen to coincide with millions of children and teens getting back to school and spending more time online while doing homework and socializing.

What can I do as a parent during Internet Safety Day?

Take this opportunity to sit with your child or teen at the computer for just 30 minutes and learn about their Internet activities. It's also important to talk with them about their cell phone activities as well. For example, ask about the social networking profiles they might have on sites like [Facebook.com](https://www.facebook.com) and see what personal information they include as well as their privacy settings and list of friends. Do they use twitter and who's tweets do they follow. Find out whom they chat or IM with and what their friends do online. Talk to them about each name in their buddy list and ask how they know that person? Do they know how to spot a predator and how to respond? Do they understand the dangers of cyber bullying? Do they use file sharing services to download songs illegally? What video websites do they like to use? Discuss your reservations about the Internet and learn how they feel about staying safe. Explain your expectations for their behavior online and why it is important to be safe.

Make sure you use this time as a learning tool and show a legitimate interest. Listen to their ideas and insight because after all, they are experts about what they do online. Just showing an interest in what they do will go a long way. Even if they know more than you about computers they still need parental guidance and involvement.

What if I don't understand enough about technology to feel confident when discussing Internet safety with my child?

That is why we created this guide. It provides a brief summary on most of the popular technology activities among children and teens. In order for your discussion to be productive you don't need to be an expert, but it helps to have a general awareness so you can ask the right questions.

TABLE OF CONTENTS

WHY INTERNET SAFETY DAY?	2
INTRODUCTION	4
INSTANT MESSAGING & CHAT ROOMS	6
IM CODE	10
CELL PHONES / SMART PHONES	12
SOCIAL NETWORKING	15
PREDATORS	18
CYBER BULLYING & SEXTING	20
WEB VIDEO	22
E-MAIL	23
FILE SHARING	26
SEARCH ENGINES	28
PROXY SITES	28
ONLINE GAMES	29

This guide contains excerpts from *The Family Computer Handbook* © 2006 Brian Rice (Practical Press 2006).

The Family Computer Handbook is available at: www.Amazon.com and www.BarnesandNoble.com.

Limits of Liability and Disclaimer of Warranty

The author of this guide has used his best effort in preparing the information and suggestions contained in it. The information in this guide is distributed on an "As Is" basis, without warranty. While every precaution has been taken in the preparation of the guide, the author shall not have any liability to any person or entity with the respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this guide or by the computer software and hardware products described in it.

It is not the intention of the author to infringe on the rights of any copyrighted material. If you feel material listed in this guide is an infringement of your copyright please contact us at contact@InternetSafetyDay.com

Updated: 03/13

INTRODUCTION

Computers, phones, and the Internet have come a long way in a short amount of time. As a parent, you likely have memories of a society that was much less technology dependent. Unfortunately, your children are growing up in a much different world and they need adult guidance to make proper choices about online activities. Without such guidance, they are forced to maneuver through the online world alone, which can be very dangerous.

For example, most parents would never drop a teenager off at the local mall known as a hangout for registered sexual predators or allow some random adult to visit their son or daughter's bedroom. However, many of those same parents wouldn't think twice about allowing their child to sit in their bedroom using online chat rooms with complete strangers or hanging out in social networking sites known to have registered predators.

The majority of adults and parents are still predominately invested in the face-to-face world where they communicate with friends in person or on the phone, watch television for entertainment, and use the Internet as a tool for looking up things like directions or the weather. They completely underestimate the power and danger of the online world. Their children, however, are largely invested in this world where they strike a balance between a real and virtual existence. Many times, both are equally important to them.

As a parent you must first accept the fact that you will probably never totally share the fascination with the online world and will likely never match your child's technical ability. With that out of the way, you can begin to focus on your true role by serving as their mentor and guide. To be effective in this role, you must have a basic idea of how things work. After seeing the "Big Picture" you can begin to understand how it relates and thus be more effective in your efforts. This guide will hopefully serve as a first step in that journey for you.

Please also understand that as a parent you might find it overwhelming to think your child is involved in every topic listed in this guide. Most children and teens are typically drawn to a few. For example, one teen might just use [Facebook.com](https://www.facebook.com) and Instant Messaging while another prefers playing online games exclusively. It is all about their interest and once you learn you can begin to focus on those areas. The name of the game is to get involved. If your child uses Yahoo Messenger then setup an account and start using it. If they spend hours on [Facebook.com](https://www.facebook.com) then signup for an account and build your own profile. It might even be smart to ask your child for help, they might enjoy introducing you to their online world and showing you around.

START FROM THE BEGINNING

To start developing the “big picture” concept of Internet safety we must first examine the idea of technology devices and how they connect to make what is referred to as the “Internet.” For simplicity, let’s focus on a computer and the fact that it is merely a piece of electronic equipment storing and displaying information. In order for computers to share this information we have developed ways of connecting them with wires - known as networking. Without networking, all computers would be stand-alone devices unable to exchange information.

If we expand this concept to a worldwide scenario, where millions of computers are connected to one single network, we have what is known as a **World Wide Web** also known as the Internet. All web site addresses start with **www** to tell the computer to browse to this network in order to find the information on this web of connected computers and servers. This is considered a web due to the millions of connections resembling a spider’s web.

When a member of your family is “online” they are plugged into the same network as the sexual predator in the next town or the identity theft operation in another country. It’s just one more wire connecting a computer to the larger network that spans the entire globe and allows instantaneous communication with any other computer or connected device. With the use of “smart phones”, the phone is just another form of a technology device wirelessly connected to that same network.

It's very important to understand this Internet network because it serves as the backbone for all other functions. When discussing activities that use the Internet, for example, instant messaging, file sharing, and social networking, these activities are piggy backing on the already established network to function. Such services have flourished due to the Internet allowing that instant communication between two computers or two Smart phones across any geographic location.

INSTANT MESSAGING & CHAT ROOMS

Instant Messaging (IM) and Chat Rooms utilize the Internet network to operate. This allows for instant communication between two computers anywhere in the world. With this principle, services like IM and Chat Rooms have flourished.

INSTANT MESSAGING

Instant Messaging (IM or IMing) is a service allowing users to send typed messages, pictures, files, and live video with sound to a recipient based on their screen name. This exchange can go back and forth as long as both parties desire. It provides a personal way of communicating with friends and other known contacts and is very popular among teenagers as well as many adults.

In order to use this service a user must download a free program and install it on their computer. There are several available with some of the more popular ones being Yahoo Messenger, Windows Live Messenger, and AIM (America Online IM). The program handles all the communication and provides a window for the user to type and receive messages. (See Figure A)

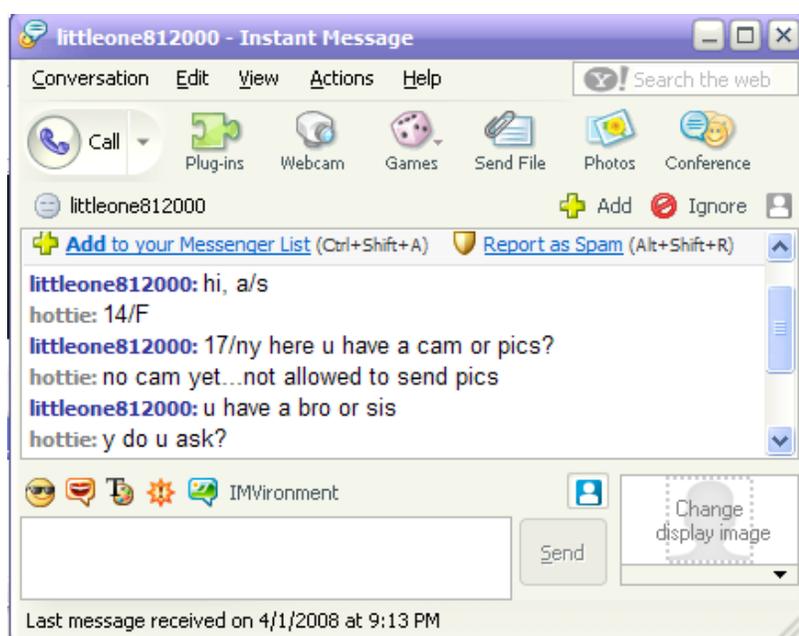


Figure A

Web sites like www.Yahoo.com and www.Google.com offer membership "ID" accounts that allow a user to register and build a simple profile in exchange for THE use of many web services such as free e-mail, game playing, and online shopping for example. Part of these offerings also includes Instant Messaging and Chat Room services. Once logged into the site, a user can seamlessly maneuver through all application options. The web site also keeps track of user's activities in order to provide a personalized experience on future visits. There are no verification efforts to make sure the person who creates an account is who they say they are. This allows for the anonymity many predators desire when they can pose as a much younger person in order to meet others.

In reference to the multiple web services concept, let's say a teenager registers for a free Yahoo e-mail account and instantly has access to all the other features. The personal information listed during the initial registration becomes part of the teen's online profile for that website service. This is another reason it is important to think twice before entering personal information within online profile registration pages. Keep it all generic.

A "buddy list" or "messenger list" is a small active window inside an IM program that lists screen name contacts a user wants to consider as a friend. It allows for quick communication by clicking the name and typing a message. Lists also indicate if that user is signed on to the service by placing some type of icon next to the name. It is very common for teenagers to have multiple names in their list. For safety reasons teens should set options in their account to only allow contacts from users on their buddy or messenger list (referred to as block or ignore people not on list). They should also never allow files to be accepted on their computer to reduce potential virus threats from a friend's computer.

CHAT ROOMS

A chat room is very similar to Instant Messaging (IM) but instead of one-to-one communication, users log on to a themed based virtual room and communicate with several people only known by their screen name. By sending typed messages to the room, all connected users can read and respond like a big online get together. There are numerous chat topics to choose from such as: hobbies, television shows, boy bands, sports, politics, health issues, and relationships. (See Figure B) Basically if there is an interest, there is probably a chat room available. While watching chat room dialog, users will likely notice most postings are just typed advertisements for other web sites and similar things with very few legitimate conversations taking place. It is more of a place for users to post their name and then wait for someone to invite them into an Instant Message session also known as "going private."

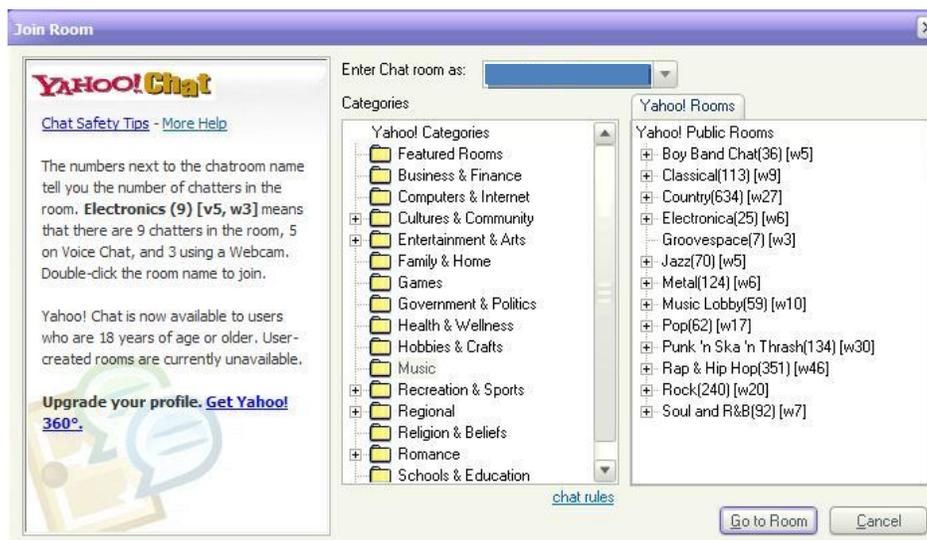


Figure B

As mentioned in the previous section, many chat rooms are seamless with IM services in regard to certain web sites. Once a user has an account they can travel between both worlds with the click of a mouse. "Yahoo Chat" is one example. While using "Yahoo Instant Message" a user can simply drop down a menu and select "Yahoo Chat" and instantly be presented with

a list of available topics and corresponding rooms. (See Figure B) Other examples are “AIM Chat” and “Google Talk.” There are, however, many other chat room web sites that focus on chatting exclusively and are not tied with major search engine web sites.

A chat room window basically combines people who will only know each other based on their profile and registered screen name. (See Figure C) If a person decides they want to “go private” with someone in the room, they can click that person’s name and ask to send an Instant Message. At that point, both users are simultaneously still in the room while engaging in a private IM session in a separate pop up window. (See Figure D) Predators use this feature to target users they meet in chat rooms. Additionally, once a predator has a screen name written down, he or she can send future Instant Messages directly by opening the IM service, typing in the name, and then typing a message. Many also send requests to be added to the potential victim’s buddy or contact list.

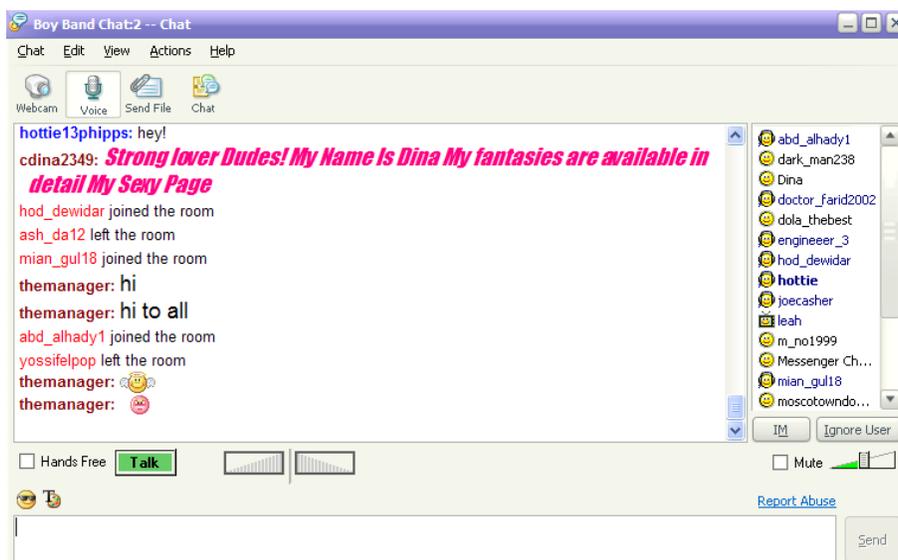


Figure C

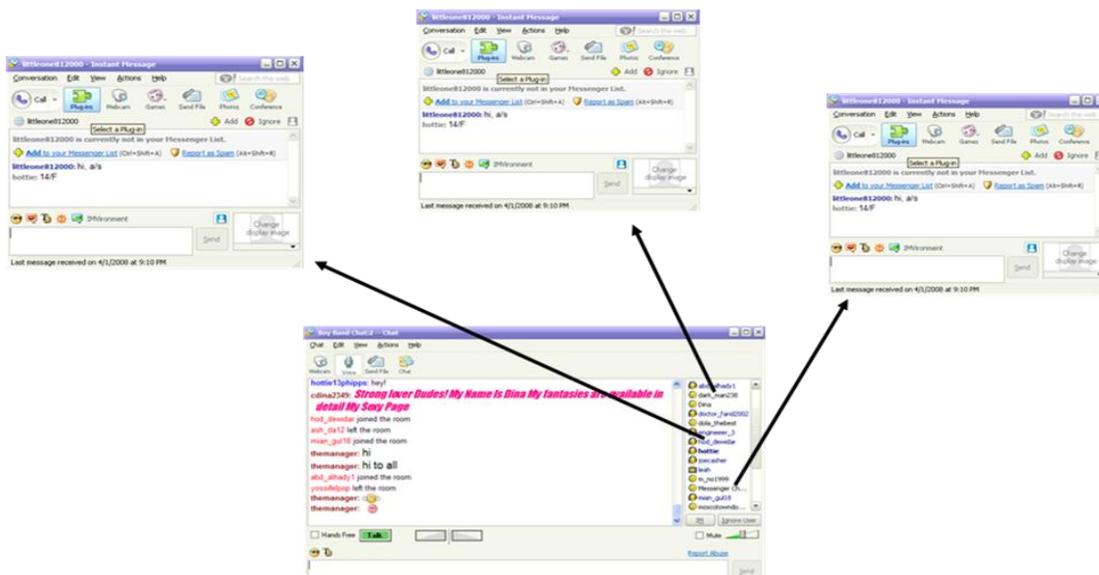


Figure D

IM AND CHAT ROOM Do's AND DON'TS

- Try it yourself (learn what it is about) – use the service to communicate with your children
- Use generic screen names and profile information so predators cannot use it to gather information. For example screen names like “**boytoy17**” or “**soccrgrl13**” are very inviting to predators because the name itself provides an image into that user’s life (soccrgrl13 it likely a soccer player and either 13 years old or it’s her jersey number)
- Require children to save IM and chat history for parent review
- Monitor child use (stay involved)
- Set preferences to only allow IM’s from Buddy or Messenger List, this blocks messages from users you do not know – especially predators who may try to send an IM while in a chat session
- Ask your child about each screen name on their list at least once a week to see how they know that person. If they only know them through online correspondence delete the name.
- No Web Cam. Almost all Instant Messaging services allow video and audio to be sent through the connected session. If there is no camera on your computer it can’t be used. If you have a laptop with a built in camera, run the program that controls the camera and look for settings that will disable it.

PARENT FYI - If you don’t know how to manipulate the above settings ask your children or a friend for help. Anyone with some basic computer experience will likely be able to help you locate where to go. If you still can’t find it, look for words like “preferences”, “privacy”, or “options” within the program windows.

IM CODE

When using IM and chat rooms it is common to use abbreviations for words or phrases that take too much time to type. This type of abbreviating almost becomes a cryptic language of its own preventing unfamiliar users from understanding what is actually being typed. This puts parents at a disadvantage even if they are watching over their child's shoulder. There are even codes for telling others a parent is watching.

This is a small list of some of the more common codes with their associated meaning. **More can be found by searching the Internet or using the following web sites:**

www.noslang.com

www.netlingo.com/acronyms.php

www.chatslang.com

<u>IM Code</u>	<u>Interpretation</u>
2NITE	Tonight
ADR	Address
AEAP	As Early As Possible
ALAP	As Late As Possible
ASL	Age/Sex/Location
AWGHTHTGTTA	Are We Going To Have To Go Through This Again
B4YKI	Before You Know It
BOHICA	Bend Over Here It Comes Again
BRB	Be Right Back
BRT	Be Right There
CP	Sleepy
CWYL	Chat With You Later
CYT or SYT	See You Tomorrow
E123	Easy as 1, 2, 3
EM?	Excuse Me?
EOD	End Of Day
F2F	Face To Face
FOAF	Friend Of A Friend
GYPO	Get Your Pants Off
HAK	Hugs And Kisses
ILU or ILY	I Love You
IMNSHO	In My Not So Humble Opinion
IWSN	I Want Sex Now
J/C	Just Checking
KFY	Kiss For You
KOTL	Kiss On The Lips
KPC	Keeping Parents Clueless
L8R	Later
LD	Long Distance
LMIRL	Let's Meet In Real Life
LMK	Let Me Know
LOL	Laugh Out Loud
MOOS	Member(s) Of the Opposite Sex

MorF	Male or Female
MOSS or MOTSS	Member(s) Of The Same Sex
N-A-Y-L	In A While
NALOPKT	Not A Lot Of People Know That
NAZ	Name, Address, Zip
NIFOC	Nude In Front Of Computer
NM	Never Mind or Nothing Much
OLL	Online Love
OSIF	Oh Sh** I Forgot
OTP	On The Phone
P911	Parent Alert
PAL	Parents Are Listening
PAW	Parents Are Watching
PIR	Parent In Room
POS	Parent Over Shoulder
QT	Cutie
RN	Right Now
ROTFL	Rolling on the Floor Laughing
RU	Are You...?
RUMORF	Are You Male Or Female
SITD	Still In The Dark
SMEM	Send Me an E-mail
SMIM	Send Me an Instant Message
SO	Significant Other
SOHF	Sense of Humor Failure
SorG	Straight or Gay
SWDYT	So What Do You Think?
TDTM	Talk Dirty To Me
TOM	Tomorrow
TS	Tough Sh**
TTFN	Ta-ta For Now
U-R	You Are...?
WFM	Works For Me
WTH	What the Heck
WUF	Where Are You From?
WYCM	Will You Call Me?
WYRN	What's Your Real Name?

CELL PHONES / SMART PHONES

Several years ago, cell phones were simply used as a mobile way to make phone calls. With advances in technology over the past several years, the cell phone has evolved into what's known as a "smart phone." Although traditional cell phones are still around, smart phones are essentially the standard now and basically serve as a portable pocket computer capable of texting, viewing and downloading music and videos, taking and sharing pictures, surfing the Internet, and many other applications at very fast speeds. This type of personal device can complicate parental efforts in monitoring a child's use of social mediums. The old adage of ensuring the family computer is located in a high traffic spot to prevent improper activities can be thrown out with respect to smart phones. The sheer processing power and applications (apps) available for such devices, along with societal demand for a more mobile internet experience has changed everything. This is yet another example of why parents must remain engaged in their children's technology activities.

Another thing to consider with smart phone use is how most are equipped with GPS (Global Positioning System) technology. Pictures taken with such phones typically imbed GPS coordinates or "geotag" the physical location where the picture was taken within the data of the picture. When such pictures are posted online it can create a safety issue. A simple picture of your dog in the backyard can provide the GPS location of where you live.

For more information visit - <http://icanstalku.com/how.php>

Linda Criddle, President of LOOK**BOTH**WAYS, Inc. has listed the following information on her website concerning cell phones. <http://ilookbothways.com>

There are very simple phones for the youngest users that can essentially do only one thing – place calls – and those calls can be restricted to certain numbers. On the other end of the spectrum are the 'smart phones' that are likely to include photo and video filming and viewing, GPS (location tracking) functionality, the ability to chat and use social networks, conduct financial transactions, have removable memory, and more. Think through the safety and privacy implications and responsibilities that come with each feature and select a phone that you and your child/tween/teen can both be comfortable with.

1. **Choose the carrier that best fits your needs.** Consistent coverage is always the first concern for phone purchasers, but for youth you want to also consider what safety features the carrier offers. Verizon has the most comprehensive family safety/parental control options (<http://parentalcontrolcenter.com>) (see also Verizon Safeguards) among mobile service providers, but all the major carriers have at least some safety features. (see comparison chart below)
2. **Pick the phone plan that provides only the functionality you want for your child.** You can choose to purchase a plan that allows text messaging, photo sharing, and internet access – or not. Add these as you feel your child is ready to take on the greater responsibility for appropriately using these features. Talk to your carrier's sales personnel to learn more about

the safety functionality they provide, and, if you feel anxious about your ability to set the controls on your child's phone yourself, ask the sales person to set these up for you.

1. Another consideration when choosing your child's phone plan is whether you want your child to have a prepaid plan, a monthly independent plan, or include your child on your family plan. Selecting a plan that allows you to review the bill each month gives you a strong method for monitoring their use and safety. The phone bill should show you what times of day calls/texts are made or received, how much time is spent on the phone, who your child is interacting with, what websites they're visiting, etc. This helps you to see where there may be concerns like texts/calls during school hours or late at night or calls to numbers you don't know.
3. **Have the 'Talk'.** Before your child gets their first phone, talk about each type of functionality they'll be able to use, and what is – and isn't – appropriate behavior, what types of information are ok to share and what isn't, what times of day and with whom it is suitable to communicate, and how to treat others with respect. Talk about how to report trouble and assure your child you'll help if they need you, learn together how to block callers, and use other safety features. Based on your child's age, talking about talking/texting and driving, cyberbullying via cell phones, and sexting may be appropriate. Discussing *in advance* your family's safety rules, and being up front about the technologies you will employ to monitor behavior is crucial. Though many programs allow you to spy on your kids using a stealth mode, doing so will break down the trust between you and is likely to cause serious harm to your relationships.

Include in your discussion clear ground rules for using the phone and the consequences of failing to use the phone appropriately. Cell phones aren't a 'right' they're a privilege and failure to appropriately handle a privilege can result in the retraction of that privilege.

That said, I am not a proponent of taking away a child's cell phone as a punishment for things unrelated to cell phone use. For example, if you wouldn't take away pens and pencils from your child if they wrote mean notes, then taking away the cell phone of someone who writes mean texts doesn't really make sense. The punishment for bullying should be about the behavior, not the tool. However, if your child is making or accepting phone calls in the middle of the night, taking the phone away at bedtime and giving it back in the morning makes sense.

Be clear about your level of direct monitoring. If you feel that periodically sitting down with your child and reviewing their contacts, texts, photos, etc is appropriate – and it is based on age and the child's maturity – this expectation should be well understood by your kids up front so you avoid unhappy confrontations in the future.

4. **Continue having the 'Talk'.** Once your child has a cell phone, sit down periodically to discuss how well they're managing the freedom and responsibility the phone affords them. When they demonstrate that they can use the existing phone features appropriately, allow them to add additional features and functionality and step up their level of self management.
5. **Decide if your child needs additional safety or monitoring tools.** These tools break down into three primary categories: tools that filter content and contact, tools that monitor and block usage, and tools to track the child's location. Which tools will be appropriate for your situation

is something only you can determine, but you have a number of options. See <http://davidburt.us/parental-controls/> for an excellent overview of not only cell phone safety but all kinds of technology safety.

Your goal is to help protect your kids while helping them to become fully capable, independent, responsible online citizens on any device. As kids mature, the settings you use to monitor them need to be reevaluated. Ideally you do this 2-3 times a year, but at least do so once a year. You need to transition responsibility for their behavior, and for the content, programs and sites they use as they demonstrate they have mastered the skills needed, and accepted the corresponding responsibilities that new services and activities require.

SOCIAL NETWORKING

Another popular activity online is creating a profile on one of the many social networking web sites. Many sites offer this service but the most popular are Facebook.com , MySpace.com and the new Google+. Each site basically provides the same experience but has its individual characteristics along with rules and regulations. The way it works is users register and create a personal page called a profile on the site. Profiles can include pictures, personal information, opinions, online journals called blogs, music, videos and basically anything else a person feels represents them and their personality.

These sites offer various search tools to connect users with real life friends or find others with similar interests. This allows many people to also find lost acquaintances and other people from their past as well. Once found, they make contact by requesting “friend status”. Acceptance from the other party creates a new icon on both users friend list. Users typically post comments, web links, pictures, etc. to either their own profile “wall” page or their friends. Posting on their own “wall” also places it on all their friends “home” page. This creates a simple way for someone to quickly keep tabs on all their friends by just reviewing what they have posted on their own “home” page. The general rule of thumb is the more friends a user has the higher status they enjoy.

Replacing the need for face-to-face interaction, social networking has become a new addiction for many who spend hours cruising through endless profiles making connections with old friends or making new ones. In a sense, it allows users to have their own virtual “network” of people they use as a resource by sharing ideas as well as learning by reading what others post. Users can also send messages to their friends as well as Instant Message instantly after the service indicates their friend is online.

As with anything involving the Internet there are dangers to consider with social networking. For starters, it creates a place for online predators to gather information. This is a concern considering the number of teenagers who carelessly list personal information such as their full name, town, high school, and post pictures of their house or car. Some sites, like Facebook.com, prevent unregistered users from viewing profiles while others do not. MySpace.com allows anyone to browse and view profiles although certain areas are restricted to unregistered users. Another area of concern with MySpace.com is the browse and search features allowing searches based on such criteria as body type, sexual orientation, smoker, drinker, and relationship status (i.e. Single, Married, In a Relationship, Divorced, Swinger). Some users also post risqué, nude and sexually suggestive pictures of themselves or others although websites have rules against it listed in the terms of use agreement. Both sites also restrict users under the age of fourteen from registering and having a profile. The method of age verification is determined by the birth date the user lists which is easily defeated. There are other social networking sites developed specifically for very young children (weeworld.com).

MySpace.com has made attempts over the years to crack down on predators by implementing restrictions for adults having access to underage user profiles. Although with no age verification adults can easily pose as the age group they are targeting. Many social networking sites list safety tips for users to review and typically a safety link is available at the bottom of most webpages.

Social Networking profiles can be set to a private mode which only allows people to view it that have been accepted as a friend by the profile owner. This is default in Facebook.com. This prevents random users from viewing and is a great safety feature for protection. All profiles should be set to private but keep in mind this prevents parents from viewing their child's profile as well unless they have a profile themselves and have been added as a friend.

MICROBLOGGING

Microblogging sites like www.Twitter.com and www.jaiku.com are also considered a form of social networking because they allow users to create their own type of "people network" to be used as a resource. The act of microblogging basically allows a user to post small messages (140 characters or less) to an online profile which in turn is received by other users that have signed on to receive their messages. Many celebrities use Twitter.com to post "tweets" about their normal daily activities which provides fans with an insight into their life. Most tweets are done with cell phones as a user would text the information to the site which is then posted.

Users can also utilize their followers for assistance by sending out questions and getting responses. This is another example of the notion of a "people network" where everyone contributes and helps each other.

VIRTUAL WORLDS

When most people think of social networking they think of MySpace.com or Facebook.com. There is also a completely different type of social network infrastructure available now that has taken lessons from role playing games. Web sites such as www.secondlife.com, www.kaneva.com, and www.gaiaonline.com offer a virtual world/community that allow users to create a character of themselves known as an "avatar." Once created, they roam through this online world and interact with other avatars. The avatars represent other people sitting at their computers doing the same thing. Avatars allow people to be whomever they want. Men can become women and vice versa. Older adults can build their avatar to be 16 years old. Basically in a virtual world anything goes and no one can prove otherwise.

This is very dangerous because when children and teens are involved in this type of virtual reality world they are literally blind to who they are dealing with. They are mixed into a virtual world interacting with adults and potentially some predators. There are also several adult areas in Second Life including "rape rooms."

There are also virtual worlds targeted to grade school children. www.weeworld.com is one of those sites that allow very young children to make avatars referred to as a "wee mee." They use their avatar to play with other kids in the virtual world. A potential for danger is very prevalent in this world as well. Similar sites such as www.whyville.net and www.clubpenguin.com offer a safer environment.

SOCIAL NETWORKING DANGERS

- Adults use the site
- Inappropriate language, nudity, alcohol use, sexually provocative images, etc.
- Predators use it to gather information
- No real method of age verification
- Some Social Networking services allow people to view profiles without logging on; therefore teenagers and young children can access it easily

SOCIAL NETWORKING DO'S AND DON'TS

- Set profile to private
- Read safety tips on all SN web sites
- Ask teenager to show you their profile (all of them)
- Discuss online privacy
- No addresses, phone numbers, other identifiable information (license plate)
- Once posted online it is there to stay
- No Web Cam

PREDATORS

Sexual predators do exist and are a very real threat. They target both boys and girls of all ages and use the anonymity of the Internet to their advantage since they can be whomever they want. Many are master manipulators with skills that can cripple any child's sense of awareness. This is known as the grooming process and predators look for children that are more technically savvy than their parents. They look for children that are emotionally vulnerable which can be related to personal issues derived from problems at school or home. They use these issues to befriend the victim and empathize with them while building a pseudo friendship and trust. If a child indicates frustration with parents or teachers at school the predator might suggest the child's parents are way too strict or their teacher is being unfair and this plays right into the adolescent mind as they look for people to verify their feelings.

With the presence of searchable user profiles when dealing with Instant Messaging and Chat Rooms as well as Social Networking profiles, predators can easily find information about potential victims since many naive children list personal information with no regard for safety. Even simple statements listed on a profile such as school attended, sport played, or even what jersey number worn can allow predators to target them. A 16 year old girl who innocently posts a picture of her new car in front of her house for her friends to see is also providing information for potential predators such as what her car looks like, her license plate number, house address, what her house looks like etc.

Once a predator Instant Messages or Chats with a victim and gains their trust they often send pornographic pictures via the IM session or e-mail and sometimes gifts through the mail. They might even have a toll free phone number for the victim to call or mail a cell phone so it will not show up on their parent's phone bill. If the victim tries to cut off communication, predators will often convince them that they will tell their parents what they have been doing online and that they have viewed pornographic pictures, etc. and scare the victim into continuing the relationship.

The Internet is a worldwide network that stretches far beyond the grasp of the U.S. judicial system. Technology moves so fast the slow progression of our law making process will never fully address the problem. Therefore, parents must be on guard to protect their families. There are many organizations and government agencies designed to assist parents with issues such as these. Internet searching for information will also provide many links and web sites to help.

PREDATOR GROOMING

- Chat Rooms (based on interest)
- Look for child oriented screen names
- Search through Social Networking profiles
- Strike up a conversation
- Show interest and gain their trust
- Build them up (be their friend)

PREDATOR WARNING SIGNS

- Spends a lot of time online
- Find porn on the computer
- Receive phone calls, mail, gifts from people you do not know

- Withdraws from normal activity
- Switches screen quickly (Alt+Tab)
- Uses other accounts for e-mail or Instant Messaging

Other helpful web sites for more information:

www.fbi.gov/publications/pguide/pguidee.htm

www.ic3.gov

www.missingkids.com

www.netsmartz.org

www.microsoft.com/security/family-safety/kids-social.aspx

www.isafe.org/

www.homesecuritysystems.net/resources/internet-security-at-home-for-kids-teens/

CYBER BULLYING

When someone uses the Internet to threaten someone or treat them in a negative way this is known as cyber bullying. Such activity is commonly found with teenagers who allow these situations to be reinforced within social groups at school. Cyber bullying can be represented in many forms: such as a student building a webpage making fun of another classmate and spreading the web link at school for other students to visit or sending threatening IM's or e-mails to that student. Sometimes, a teenager will IM a fellow classmate and act like their friend in order to gather private information to spread around school for embarrassment. Cyber bullying is only limited by the creativity and technical ability of the bully.

Unfortunately sometimes the bully is hard to catch. For example, a student that builds a webpage remains anonymous and it is likely being hosted on a server in another state or even out of the country. The company hosting the webpage is not inclined to provide the name or remove it since Internet companies typically feel it is not their role to police the Internet.

If you or someone you know is being bullied make sure to keep as much documentation as possible. If it is in the form of e-mail or IM it should be saved and printed. Consult with the school administration to determine what can be done. Also, keep in mind that bullying can take the form of cell phone text messages.

Visit these web sites for more information about Cyber Bullying:

www.cyberbully.org

www.stopcyberbullying.org

www.wiredsafety.org

www.isafe.org

SEXTING

Becoming increasingly popular with the use of smart phones with embedded camera cell phones "sexting" is the common name for taking nude or provocative pictures of oneself and sending them through cell phone text service to another person. Most commonly done by teenage girls for their boyfriends, they never think about the legal issues of this practice. Often times, after a breakup the receiving party may retaliate by sending the images to other friends in an attempt to embarrass the sender. Several cases have risen over the past few years where teenagers have been charged for producing and sending child porn since they are underage. The image recipients are also liable for having the images on their phone and/or sending child porn. This is an increasing problem facing schools in dealing with this issue. Such images spread quickly throughout the student body creating an administrative hassle as schools must confiscate phones and work through the authorities. This can also take the form of bullying as students might take a picture of an unsuspecting classmate in the locker room and circulate it throughout the school.

An important note to parents and adults is to report situations like this immediately. An adult who may want to keep something like this quiet and just take a phone away and put it up for some time can potentially face charges of possessing child porn themselves. School

administrators must be very mindful of this and not place suspected phones in their desk to deal with later.

WEB VIDEO

The ability to use the Internet to share videos is now very popular due in large part to the increased use of high-speed Internet service for home users. Videos are large files therefore they take a lot of time to transfer across a network and that includes the World Wide Web network. Therefore dial-up customers just a few years ago would not have been as eager to wait for videos to download.

Smart phones

The fact that anyone with a video camera can record something and post it online for millions to access is very appealing to amateur actors and directors who traditionally had no large outlet for their creative talents. By using the Internet as their distribution vehicle they have leveled the playing field with many of the television and movie networks. Simply put, people are turning to their computer for entertainment and customize their experience based on what they want to view. Many amateur videos posted online receive pop culture status and are viewed by millions of people, which sometimes garner big breaks for these struggling amateurs.

Many videos consist of stupid human tricks, comic parody commercials, clips from music videos and television shows and anything else you can imagine. Unfortunately, many videos also contain sexuality and nudity as well as alcohol use and violence. Some of the web site video services try to remove this type of material but videos are being posted at such a rapid rate it is almost impossible. Many also employ mechanisms to prevent underage users from seeing such content but with no real form of age verification it is not practical.

Web videos have also become part of social networking profiles where profile holders place videos for others to view. This has created a direct link between social networking and web videos and increased the popularity of both.

Out of all the video web sites YouTube.com is by far the most popular, but there are many others. Search engines such as Google.com and Yahoo.com also recognized the need to diversify and now offer video services.

Here are some examples of other Web Video web sites:

www.veoh.com

www.metacafe.com

www.stupidvideos.com

E-MAIL

E-mail (Electronic Mail) has become a popular way of communicating over the Internet. It enables messages to be sent instantly anywhere in the world. Instead of writing a letter and paying postage why not send it electronically? Using e-mail requires an e-mail address that is either provided by an Internet Service Provider (ISP) or a free service web site. Free addresses are popular due to their availability.

SERVERS

This is a good time to discuss the existence of servers and how they play a crucial role in Internet communications. A server is a fast, high-powered computer or bank of computers with large amounts of data storage. The basic function of a server is to store data and then serve or deliver that information to users when requested. Servers are specifically designed for their function and there are many types such as e-mail servers, web servers, ISP servers, and DNS servers to name a few. They work together to make up the backbone of the Internet and permit our communications with it. These servers are typically found in an ISP office or many large web site search engines will have them as well.

E-MAIL FUNCTION

It is important to understand that e-mail travels over the Internet from server to server. For example: I send an e-mail to a friend living in Florida. I log on to my e-mail server, type my friend's e-mail address in the "To:" box and then type the message. Once I select "Send" my server uses the address to forward the e-mail to my friend's server. My friend then retrieves the e-mail during his next log on to his server.

ISP BASED E-MAIL

As mentioned before, e-mail is available through either an ISP or a free service. The provider's name is typically part of the address revealing what type it is. All ISP's assign at least one e-mail account per customer but some people decide not to use it. They prefer instead to use a free e-mail account. It is common to access ISP e-mail with a client program installed on the user's computer. Programs like Microsoft Outlook Express (included with Windows), Microsoft Outlook, QUALCOMM Eudora and Mozilla Thunderbird, as well as many others are designed for this purpose. When a client program is opened, it contacts the ISP e-mail server and synchronizes to receive new e-mails or updates. The client program has all functions related to e-mail like composing and deleting. After making changes, the user can close the client program or manually click a Send/Receive button to update the server. Once updated, the server will replicate the changes and send e-mails accordingly. ISP's commonly provide web based access on their web site allowing users to access e-mail from any web connection. This can be for users who either do not want to use a client or are away from their normal computer.

FREE E-MAIL

Many search engines and web sites like www.yahoo.com, www.hotmail.com, and www.gmail.com offer free e-mail service. Such e-mail accounts are completely web based and popular despite the advertisements users must endure. Such popularity also creates a breeding ground for spam. Web based e-mail is accessible through web browsers. The web site supplies a web interface for users to gain access. Mail is never stored on the user's computer unless they purposefully save it there. This creates a safety zone from malware and other undesirable items that might be hiding. However, if an attachment is opened or a link

selected, it will use a program on the user's local computer therefore opening the potential for infection.

Take note when signing up for free e-mail; it requires personal information during registration. The provider uses this for target advertising. Some people use fictitious names as well as other fake information. Users who plan to use the e-mail address for professional correspondence should consider using their real name or initials. This name will be attached to all e-mails sent and might confuse recipients. Some free e-mail services do allow the sent name to be changed making it different from the registered name.

Here are some examples of web sites that provide free E-mail:

www.hotmail.com
www.mail.yahoo.com
www.mail.lycos.com
www.mail.com
www.hushmail.com
www.bluebottle.com
www.cooltoad.com

SPAM

Spam is basically junk e-mail from advertisers, companies, or people you don't know. It is similar to junk mail sent to your home. Many times it contains inappropriate words in the subject line as well as suggestive phrases. Most people ask me how they get Spam when they use antivirus protection software on their computer. Well for starters, Spam is not a virus it is just unwanted e-mail. In addition, it is typically stored on the server, not the user's computer. For users with a client e-mail program installed locally, Spam would only flag antivirus software if an attachment was infected. Some antivirus programs also have Spam filtering included.

Many e-mail providers scan for Spam but are typically overwhelmed and miss some. Setting filter parameters is also tricky when discerning between Spam and legitimate e-mail. If a user checks e-mail with a web interface, there is no concern with Spam prevention on the local computer since it stays entirely on the e-mail server. Usually there is a way to designate e-mail as Spam which will attempt to block future e-mail from the same sender. Chain e-mails are also known to cause Spam. Chain e-mails have cute pictures, graphics, jokes or encouraging stories. Recipients like them so much they forward them to all of their friends. Many times the e-mail also includes instructions to send it to other people to keep it going. Most users never realize their address and their friends' addresses become part of the chain history. A Spammer will use these e-mails to extract addresses. Ask your friends not to send such e-mails and you should never forward them to other friends. If you must participate in receiving such e-mails, create a junk account with a free e-mail service. Tell your friends to forward them to that account so your real address is not as susceptible to Spam.

PHISHING

Phishing is an e-mail appearing to be from a legitimate company. The purpose is to trick recipients into providing personal information such as credit card, bank account, and social security numbers. The e-mail uses the legitimate company logo and other identifiable marks to

gain the trust of the victim. With claims of “During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information” or “If your account information is not updated within 48 hours then your ability to purchase will become restricted” it is tempting for recipients to respond. Typically users respond by selecting a link in the text of the e-mail. The e-mail originator knows many recipients will not have an account with the company and realize it is a trick. However, phishing a large group might hook a few people who actually do.

FILE SHARING

File sharing has become a major problem for the entertainment industry. With the use of file sharing web sites such as www.kazaa.com, www.bearshare.com, and www.bittorrent.com many people are stealing music and movies by downloading them for free. The process works by users connecting to an Internet based peer-to-peer network and making their files available to others connected to that same network. For example, a user logs on to the network and searches for a particular song. In turn, the network searches through all logged on computers and displays who has it. The user initiates the download and a copy of the song is transferred to their computer. If a user's computer holds songs that others want, the same process is repeated in reverse. This is the file sharing process. The network makes everyone's files available in order to share.

The potential for viruses and other forms of malware from this activity is a major concern since users literally download files from unknown computers. In fact, some files are simply viruses disguised as songs or movies. Many times entertainment companies purposely dump placebo files in the mix to cause frustration and prevent users from downloading the real thing.

It is illegal to copy or share copyrighted material over the Internet. A friend of mine who works in the file sharing prevention industry told me he is surprised how many people play ignorant about what is copyrighted and what is not. His statement to me was "If it is not a home video of your family or a song you recorded yourself then it is probably copyrighted and you shouldn't be sharing it. In addition if you're not paying for it, and you can download it onto your computer for free, your copy is most likely obtained illegally." This is the bottom line.

The federal government has been working with music and movie executives to create new ways to crack down on illegal file sharing. Many legitimate web sites have been created that charge a fee to download music that is paid to the appropriate party. Obviously the free sites are more attractive and the apparent anonymity of the Internet makes it seem okay for many people.

Recently the Recording Industry Association of America (RIAA) has been targeting college students who have downloaded illegal music from campus networks across the U.S. They are mailing pre-litigation letters requesting the recipient to either settle out of court by paying a fee or face a civil lawsuit.

Here are some additional web sites with information about File Sharing:

www.riaa.com

www.respectcopyrights.com

Popular File Sharing Services (used for illegal sharing):

www.kazaa.com

www.bearshare.com

www.bittorrent.com

Web sites that Allow Legal Purchases:

www.apple.com/itunes/

www.rhapsody.com

www.emusic.com

www.walmart.com

SEARCH ENGINES

The Internet is commonly used to search for information which is performed with the help of web sites called search engines. There are numerous search engines available but some of the more common ones are www.google.com, www.yahoo.com, www.bing.com, and www.msn.com.

In order to remain competitive, search engines have diversified and now offer things like image and video searches. Microsoft's www.bing.com actually plays portions of the videos when a user hovers over the thumbnail picture of the search results.

Image and video searching is very popular with students doing school projects. It is also a way to look up inappropriate images and not be detected by filtering programs. The search engine shows the images within its own results page therefore it does not flag filtering software. If the user selects the picture the corresponding web site address would attempt to open and then be subject to filtering. However, the original picture shown is large enough to cause concern. In addition, many search engines restrict results based on filters but offer customizable filter settings for a user to quickly turn them off. Parents do have the ability to set the preference options when using the search engine that keeps all searches in "safe filtering" mode and require a password for changes to be made.

Here are some great search engine computer safety resources:

www.google.com/familysafety/resources.html

www.google.com/familysafety/advice.html

safely.yahoo.com/

PROXY SITES

A "Proxy Site" is a web site that provides visitors with a way around security blocks and is very popular with teenagers in schools or other areas where computer restrictions are in place. By providing a separate address bar on the webpage a user can surf the Internet within the proxy page bypassing the local security.

When a proxy site is used the only Internet activity history to be found will be the proxy site itself because as far as the computer is concerned the user only visited that site. The remaining activity was done within the site.

Here are some examples of Proxy web sites:

www.proxisurf.info

myninjaxproxy.info

ONLINE GAMES

Online games come in various forms from simple quick games (addictinggames.com) to intense role-playing games also known as RPG's. When it comes to online game safety RPG's are the most to be concerned about.

ROLE PLAYING GAMES

Role Playing Games also known as RPG's have been around for many years. Many people are familiar with the original tabletop Dungeon's and Dragon's game that was developed in the 1970's. The basic function was to let players take on the identity of a character and play against other players that assumed their own identity. The players work their way through various scenarios of the imaginary world.

As computers and the Internet have evolved, RPG's have gone virtual and are now online. There are many types to choose from based on themes and they are just a click away. In fact, there is a new acronym to explain the online version - MMORPG (Massive Multiplayer Online Role-Playing Game). Just typing RPG or MMORPG in any Internet search engine will return more results for games than you would ever care to know. One of the more popular ones is RuneScape, www.runescape.com.

Like other online activities, such games are very addictive and will occupy players for hours. One area of concern is unlike the tabletop RPG's from the 70's, people playing RPG's are playing against people they do not know.

VIDEO GAME SYSTEMS

Many parents consciously make an effort to keep computers out of their children's bedrooms but never consider the video game console.

Units like Microsoft's XBOX 360 and Nintendo's Wii do more than just play games – they are computer systems with network capabilities that can access the Internet. Even if you do not connect the unit to your home Internet connection via a network cable, some systems can still access wireless networks. That's right – little Johnny can potentially sit in his bedroom using his game console and connect to a neighbor's unsecured wireless network and surf the Internet without anyone knowing.

Additionally, these units have the potential to connect to an online Internet service allowing online communities in order to play against other players with the same equipment. Players can message each other or install a webcam and headset or microphone for players to see and talk to each other. Yes, there are adult predators in these communities as well. Microsoft's service is called LIVE and can be accessed for a yearly service fee. LIVE service is also available for players using their computer to interact.