

## ***AN AGE BY AGE DESCRIPTION OF WHAT TO KNOW***

### ***Internet Safety 1-2-3: The Quick Guide***

This will give you a quick guide on the risks that most children and teens face at certain ages. **Read the description of their activities, not just the age ranges.** How they are using the technologies and which they are using is more important than their age in determining the risks they face. This can be very helpful when you want to know where to start. Reviewing these will help you know what to look for, especially when you want some quick help.

#### **Under 8 years of age:**

The children are lap-surfing and just beginning to use the Internet. Some are pre-readers, and others are new writers and slower readers. That means they can easily make a mistake when typing in their favorite website name or searching for their favorite topics in a search engine. Most are not using interactive communication technologies (e-mail, instant messaging, etc.) without parental screening and supervision. They may or may not be allowed to access the Web without their parents standing over their shoulder.

These children play lots of games, online and offline, but most of the ones they play are not interactive (meaning, they don't usually involve them playing against other people). They spend most of their time on favorite sites that usually involve their favorite offline and television characters and brands, such as Disney, Children's Television Workshop, Nickelodeon and Cartoon Network.

Children under eight years of age are very concerned about doing something to break the computer (downloading viruses and spyware applications). It's a good age to get them started with secure surfing and using an anti-virus program if downloading anything or accepting any attachments. It's also a good time to get them to start using spyware and pop-up blockers (perhaps by using a customized toolbar, such as Google's or Yahoo's ). They are not yet involved with stranger communication or the risks of meeting people offline.

They need to learn good netiquette and how to respect others online. They also need to learn how to find new sites without risking full-sized search engines. Being able to communicate with large numbers of friends and have them be able to reach you is less of a problem at this age. The most restrictive parental control technologies work well here. They don't need millions of websites to do their homework at this age. It's less about opening up their access and more about limiting it.

Some children of this age are using mobile phones and handheld gaming devices with networking capability, but most aren't. Prepaid calling cards for their mobile phones are a good decision, to keep them from running up high phone bills. Text-messaging shouldn't be permitted at this age. And the most restrictive settings for all networked handheld technologies is your best bet, if you buy them at all.

And if you are allowing them to play video games, check the ratings and choose one that is appropriate in violence, language and sexual content for your child. Check and make sure that they can't install new video games on their mobile phones without your approval. Keep them from using any interactive game devices, such as X-Box Live or Sony PlayStation Network, or other voice chat games or devices.

Less is more when you are dealing with children of this age. They still believe that their parents are in charge, know everything and are there to protect them. (It's a magical age...Enjoy it,

it won't last! ☺) Also, are you using babysitters? Remember what I suggested about password protection and turning off the Internet when you are not home.

- Use filtering or parental control technologies. Block everything that isn't pre-approved, rather than just filtering out the "bad" sites.
- Think about whether they really need e-mail or IM, and if you determine they do, block all communications from anyone other than pre-approved senders.
- Make sure that the buddy list is no longer than the age of the child, and that you know (in real life) everyone on it.
- Bookmark their favorite websites so they won't mistype them and end up at a "bad" site.
- Use kid-sized search engines: Yahoorigans and Ask Jeeves for Kids.
- Limit their online time to no more than ½ hour a day, unless they have a special project for school.
- Check with their teachers and librarians for suggested websites and for recommendations for good resources online.
- Don't let them use interactive games, such as X-Box Live or Sony PlayStation Network yet. You should use our safe gaming award winning Disney's Toontown.com instead.
- Sit down with them as often as possible and find out where they go online, what they like and ask or answer any questions they may have.
- Don't allow them to set up websites, profiles, blogs or away messages or use other public posts without your direct supervision.
- Control their passwords.
- Look for safe site lists you can trust. Check out WiredKids.org approved safe sites list and the other safe sites listed in my "Green Light" section.

## From 8 to 10 years of age:

They are beginning to use instant messaging, e-mail and other interactive communication tools. They are also surfing more and spending more time online. They need to learn more about what information they can and can't share with others online, how to choose their passwords and with whom they can be shared. (Parents tend to worry most at this age, as their children do from surfing to communication tools.)

They may be engaged in interactive gaming (playing against strangers, sometimes with voice chat), spending more time playing video games (including more violent and adult-themed games) and be more likely to use adult-sized search engines to find the sites they are looking for. Because of their visiting gaming related websites, like code and cheat sites (to improve their game play), they are prime targets for spyware. And as they learn to flex their cyber-muscles, they are often cyberbullied or cyberbullying others and frequently hacking into, and sending malicious codes to, each other.

Fortunately, they are still too young to be engaged in face-to-face meetings with adults offline, and generally not looking for sexually-explicit content online. They are more interested in finding gory and shocking websites, where baby seals are being clubbed to death.

They often begin to use lewd and inappropriate language at this age too, even if they would never dream of doing this offline. Boys and girls are very different in how they use the technology at this age, as well. Boys tend to be less involved with interactive communications, even with their friends, and girls tend to surf less, spending more of their time chatting or IMing their offline friends. The people they talk with online are still the ones they know in real life. And more have mobile phones, but still need to have prepaid calling plans and restrictions on who can call them and who they can call.

Children begin to register at websites and fill out online forms at this age. Parents need to talk with them about what they can and can't do and which sites to trust. And their homework may require more websites than they can get with the most restrictive parental control settings or with some of the child-sized search engines.

Most of the children in this age group aren't downloading music or other copyrighted media online yet, unless they have older siblings. And they are still willing to tell their parents what they are doing online and when things go wrong online. Parents are still the "good guys" and are an important influence on their online activities. This may be your last chance to have an affect on their online activities. Don't waste it.

- Raise the bar on filtering or parental control technologies if you find they are complaining or are locked out of school-recommended sites. Or make sure that you use a product that will send you an e-mail at work to let you unblock a particular site. (MSN has this feature.)
- If you add IM or e-mail, make sure only pre-approved senders can send your child an IM or e-mail. Consider using a free web-based service with parental controls and spam blockers. That way, whatever they access online won't pollute their real e-mail address, or yours.
- Use a pop-up blocker or toolbar (like Google's or Yahoo's), an antivirus program and a spyware blocker and remover (this begins the age of dangerous downloads).
- Keep using the Yahoooligans! and Ask Jeeves for Kids search engines.
- Make sure that they understand what information can and can't be shared online with anyone.

- Practice chatting online with them so they know how to handle strangers they encounter online.
- Make sure that they know not to cyberbully someone or say or do anything online that they wouldn't do offline.
- Make sure they know how to use the "notify" or "warning" buttons, or consider using a monitoring software to be able to review what they are saying and doing.
- Watch for hacking, password and identity theft at this age. This is when they start stealing each others' passwords and locking them out of their own accounts.
- Also watch for their corrupting your files on your computer with spyware, etc. Back everything up!
- Limit online time (aside from special school projects) to under an hour a day (including all IM and text-messaging time).

## **Between 10 and 12 years of age:**

Cyberbullying is very common at this age. So are filling out forms, signing up for newsletters and registering for contests and giveaways online. More of the children at this age have mobile phones, which should still have a prepaid calling plan and restrictions on who can call them and who they can call. Many have text-messaging on their mobile phones, and if you don't use a prepaid plan, you may find yourself with very high mobile phone bills for their text-messaging use alone.

Some preteens are setting up profiles on social networking websites at this age, usually hiding them from their parents. They are more interested in communicating with their friends from school on these sites, and self-expression and being creative by creating "pink, pink, pink" profiles (how one of my Teenangels described her site). They are still usually chatting and IMing only people they know offline.

But some are starting to feel more confident and are willing to respond to a stranger's message or to engage in communications with a friend of a friend. (A sexual predator will often befriend one preteen to get to their friends.) And some of the younger Internet sexual predator victims engage in meeting strangers offline at this age. They usually think they are meeting a cute fourteen-year-old, but know it's someone they don't know in real life. A much higher portion of victims at this age are female than male.

Some of the boys may begin to seek out sexually-explicit content online. Many of the boys and girls are using lewd language and pretending to be more sophisticated than they are. "Cybersex" or ask the kids call it "cybering" usually begins at this age too. It is when they type sexual things online with someone else (similar to having "phone sex"). Sometimes they don't appreciate the seriousness of what they are doing, but do it anyway. Sharing their personal information and communicating with strangers are the most important issues they face at this age. Keeping them grounded at this age will payoff in the future. They are already starting to keep online secrets from their parents and don't share their passwords as readily. Some try and avoid their parents' supervision and use chat lingo to avoid their parents understanding their communication. They pretend a great deal at this age. Pretending to be older, more popular, richer, a better athlete, etc. is commonplace. They are experimenting all the time.

As they are starting to grow up, they may be entitled to more privacy (when discussing young crushes and other private information). But balancing their privacy with supervision is something parents need to learn to do. They may want more privacy and freedom than they should have at this age. You'll have to decide that for yourself, based on your preteen. The more balanced their activities are (offline friends, sports, after school activities and hobbies) the safer they usually are online. But, trust needs to be earned on both sides.

School assignments may require more access to websites than the younger parental control settings would allow. And the more restrictive kid-sized search engines may not give them access to the sites they need, either. And, when they are upset and online, they are more likely to act out. So teaching them to Take5! and ThinkB4UClick are important lessons at this age.

They may start using peer-to-peer software to illegally download music at this age. Keep an eye out for their use of file-sharing software (like Kazaa or Limewire), since there is no good reason a child of this age should be using it at all. Consider buying them a music service subscription service, like Yahoo's or Napster's, or giving them an account at iTunes.

- Raise the bar on parental controls and filtering programs to allow them to access websites they need for school, or use a parental control software that allows you to unblock sites from a remote location, by e-mail override.
- Start using full-sized search engines with filters applied (check their advanced settings) or use a toolbar (Google's comes preset with a medium filter).
- Cyberbullying is a serious problem at this age, watch for the signs...
- Teach them about personal information and predators. Without going into details, they are concerned about people showing up at their house. Make sure they remember this when online or on text-messaging devices.
- Watch for "away messages" for their IM programs. Kids often post their cell phone numbers there.
- Websites and profiles they build should be reviewed carefully, as should screen names.
- Make sure that you control the family account password and have their passwords too. Expect some push-back.
- Give them privacy as long as it is with people you trust.
- Block all but pre-approved senders. (Expect push-back here too.)
- Make sure they can't share pictures online, or set up profiles, blogs or webcams without your okay.
- Interactive games should still be limited to Toontown.com and other kid-approved sites. They are still too young for X-Box Live, without direct parental supervision or parental controls. (X-Box won one of our safe gaming awards for its parental controls.)
- Watch early media piracy, teach them not to steal online or offline.
- Google their name, screen names, address, and telephone numbers at least once a week and create alerts to warn you of any new postings. Many kids post nasty things about others at this age. (Read about how to Google someone in Step Three, Implementing and Enforcing Your Choices.)
- Change their passwords often and make sure that they aren't using a provocative screen name.
- Search regularly on your computer for images (of porn or of your kids), and any music, movie or media files you don't know about.
- Spyware is a serious problem at this age, since they often access game sites riddled with spyware and malicious code.
- Lock your private files with a password they don't know.
- Get them started in online safety education, check out [wiredkids.org](http://wiredkids.org) or [internetsuperheroes.org](http://internetsuperheroes.org). Check out starting a tweenangel chapter at your local school. (For more information visit [teenangels.org](http://teenangels.org).)
- Watch cell phone gaming, porn and spending capabilities, and think about limiting their cell phone usage in a way that shuts it down when they exceed it, instead of just charging you extra. (Check into filtering products for cell phone Internet access.)

## Between 13 and 15 years of age:

The risk of Internet sexual predators and Internet sexual exploitation is highest at this age. They have the freedom to meet the Internet "friends" in the mall or in other public places and their being away from home (at the movies, etc.) isn't questioned as it would have been a few years ago. Their hormones are raging, and they are more sexually inquisitive at this age too. Our studies have shown that a surprisingly high percentage of girls at this age admit to engaging in cybersex (having graphic sexual communications online, typically with strangers they encounter.) In one of our studies 60% of the girls we polled between 13 and 16 years of age admitted to engaging in cybersex.

It gets tricky, as they need more privacy at this age than ever before, yet also need more supervision and guidance. Respect their privacy more and talk with them about their online experiences. If you use monitoring software, use it for emergencies - never accessing the reports until something goes wrong and you need to. Consider them the security video camera in the corner of the bank. No one reviews the tapes until there is a bank robbery. And then they are invaluable.

Their mobile devices are their lifeline at this point in their young lives. Text-messaging is crucial to their social life and if they are offline for a few hours, everything falls apart. ☺ Maintaining balance is harder too. And no one website or collection of websites holds their loyalty. In fact, they surf much less than ever before, spending their online time posting on social networking profiles, building their own websites, setting up webcams and instant and text-messaging their friends. Perhaps social networking websites and blog sites are more of a risk for teens in this age range for than for anyone else. And, since they have a huge influence on money spent offline and have lots of their own money to spend (from holiday gifts, babysitting and other jobs), they are targeted by marketing schemes and ads of all kinds. Unfortunately, everything they had practiced until now on safe and secure technology use is often thrown out the window in their quest for new thrills and to be treated like young adults. They will sometimes at this age engage in sexual discussions and intentionally meet adults offline for sexual purposes. At least one study reflected that 1 in 4 girls and 1 in 7 boys in this age range were meeting strangers offline.

They are also listening, accessing and downloading music online and sometimes accessing movies and software through peer-to-peer websites, illegally. (Although most of the movie, software and gaming piracy occurs when they are in university, not middle or high school.)

Online gambling, eating disorders, bomb-building and other more dangerous websites hold their greatest appeal to kids in this age group. They experiment often and push the envelope, challenging your rules. Even if you remain consistent in your rules and use of parental control technologies, they are more likely to use handheld devices and their friend's Internet access to circumvent them.

Cyberbullying becomes cyber-sexual-harassment and more mean-spirited. Hacking, malicious code attacks and cyber-stalking become more common place when their tech skills improve and their access to higher powered technologies increase. Posing and password theft is a serious problem too. Sadly, the typical culprit is a close friend or former friend.

They are buying things online at this point, often bidding for things they collect on eBay and other auction websites. They may have their own e-commerce accounts and credit cards they are using online. That means that ID theft and financial credential theft are more prevalent at this age too. And scammers and con artists often target young teens, knowing that they may be less careful than they should be and may be conned into giving away your banking information.

- Filter sites that are inappropriate for young teens, instead of blocking all but approved sites. Some bad ones will get through, though. So talk about it beforehand.
- Give them more leeway on people they can accept IMs or e-mails from. But check and account for everyone, in real life, on their buddy list. No friends of friends.
- Make sure you filter or block image searches (a way around many filters).
- Block peer-to-peer technologies and get your kids an account with iTunes or another legal music download site, or even better, one of the new subscription services, like Yahoo!.
- Teach them to guard their passwords. Password theft is a serious problem at this age.
- Teach them not to pirate or illegally download or share software, games, music or motion pictures.
- Have them Google themselves often, screen names, telephone and cell numbers, addresses, full names, nicknames, etc. (all in quotation marks to search the whole phrase).
- Try and limit their use of chatrooms to monitored chatrooms or themed chatrooms on safe topics.
- Limit their online use (including text-messaging) to under 1-1/2 hours a day (aside from a special school project).
- Keep them out of social network or online dating sites (like xanga.com, friendster.com or match.com).
- Talk to them about not meeting strangers offline, and agree to go with them or teach them large group safe meeting tips (see "Step 3- Implementing and Enforcing Your Choices")
- Get girls (and boys) a copy of Katie Tarbox's book "A Girl's Life Online" (formerly known as "Katie.com") to read. (Katie founded Katiesplace.org, a website for young victims of Internet sexual exploitation and their families and friends.)
- Try to keep the computer in a central location, if it has Internet access, and watch new interactive devices, like cell phones, text messaging devices and interactive gaming devices, like X-Box Live. Use parental controls if they come with them. (X-Box Live got an award from us for their safety devices and parental controls.) But note that even with parental controls, these games are risky for young teens when they chat with strangers.
- Consider setting up a teenangels.org chapter, or starting an online safety club at their school. (Visit Marvel comic-themed Internetsuperheroes.org for available free materials.)
- Pick your battles! Not all risks are created equal online. Let things like their use of inappropriate and even sometimes lewd language go, understanding it's how kids talk online, and focus on their sharing too much personal information or meeting strangers.
- Talk to them about protecting their friends' privacy too.

### **For 16 years of age and over:**

All bets are off. If they have earned your trust, give it to them. If not, unplug the computer and take away their cell phones and interactive gaming devices. And pray often and hard. ☺ If you haven't taught them what they need to know by now, we're all in trouble.

- Focus on teaching them to be responsible cybercitizens and to use the filter between their ears.
- Emphasize the risks of sharing personal information and meeting strangers offline.
- Make sure they Google themselves often and report what they find. Have them set an alert on themselves as well.
- Teach them to use anti-virus programs, not believe everything they read online and to respect others. Check for adware or spyware often, use a firewall and teach them to come to you if anything goes wrong online. (Maybe they will.)
- And get their help in keeping their younger brothers and sisters safe online.
- Remind them that you're still around if they need your help.
- Pick your battles! Not all risks are created equal online. Let things like their use of inappropriate and even sometimes lewd language go, understanding it's how kids talk online, and focus on their sharing too much personal information or meeting strangers.