



Ask Parry:

The Three Steps to Internet Safety: Internet Safety 1-2-3! adapted from cyberlawyer and Internet safety expert, Parry Aftab's upcoming book.. To read more by Parry, visit WiredSafety.org or Aftab.com and her featured blog here at Yahoo!.

Over the years, most of us in Internet safety have been making this much too complicated. We thought that you needed to know everything about the Internet, all risks and all solutions. We taught parents of young children everything they needed to know about meeting strangers offline even though they are not at risk for this until their preteen years.

We expected that you would appreciate how much we know about the subject and how hard we have worked to provide this information to you. We, in short, ignored your real needs and what you were telling us. You don't want to be Internet safety experts. You don't want to devote your life to learning about the technologies and their abuses. You just want to learn how to keep your children safe online, as quickly and easily as possible.

So, I have now approached the subject differently. I have devised three easy steps that help you learn what you need to know and how to implement your informed choices for your children.

1. Find out what your children are doing online and understand the risks posed by the technologies and services you and they are using.
2. Determine what choices you have to address those risks and make the choice that works for your family.
3. Understand what technology and parental control tools exist to help you enforce those choices.

It's that simple. These three steps will help you keep your children (and your entire family) safe, secure and private online. Using this program you understand the risks *your* children face, not *all* children, set rules that work for *your* household and then enforce *your* rules. It's easy and it works.

The first step (finding out what your children are doing online) involves taking an inventory of the kinds of interactive technologies they are using and how they are using them. Once you do that, I can help you spot the particular risks you and your children face. The second step (setting your rules) involves analyzing the risks posed by you, your children or your family's particular technology use and making choices and setting rules to minimize those risks. The third step involves implementing and enforcing those choices and rules, by guiding your children and using parental controls, anti-virus software and spyware blocking tools and family-friendly services.

Taking an inventory and spotting the risks

Understanding what your children are doing is crucial to designing a program that keeps them safe and secure online. While I can give you some basic guidance that will work pretty well for most families, every family is different. And, I'm willing to bet that no two of your kids are alike either. So your rules may have to be adjusted for each child in your household.

Even though some rules may change from family to family, there are a few that all families need to follow. Every family should use spyware and adware blocking software, a firewall, an automatic updated anti-virus and a SPAM blocker, and update them often. Start there. Check and see what you are using and if the subscriptions for updates are still current. Check your settings and make sure that they update automatically and often. Each product works a little differently, so contact the manufacturer for tips on the best way to use your product. If you don't have one, and are looking for suggestions, drop by WiredSafety.org for our latest reviews of security applications and technologies.

I can give you guidelines on what other parents are doing, but you know your child best. The fit has to be right for your child and for you. The more you know about what technologies you and your children are using, the features included with those technologies and how the technologies are being used, the better you can customize a plan that works for your family. Things to look for are: computer games (ratings and interactivity), content issues (such as hate, pornography, violence, misinformation), contact technologies (that allow your children to communicate with strangers), sharing too much personal information online (creating commercial and stranger danger risks), malicious code (including viruses, spyware and hacking programs), harmful and illegal activities (such as sites that sell drugs, have gambling or encourage eating disorders or suicide) and intellectual property abuses (including piracy and illegal downloading of music, movies, software and games).

Some of your children may have special risks. They may already have an eating disorder, or have already been involved with an adult posing as a child online. They may have a gambling problem, or involved in bullying others. If your child has a special problem already existing, online or offline, expect that they will get into trouble online. You may want to consider using a monitoring product and set it to send you alerts when you child tries to access certain sites or types in certain words, such as "sex," drugs or money.

Also, if you have a family member, housekeeper, assistant or babysitter working from your home, you should be taking extra steps to keep your personal information private and make sure that they aren't accessing inappropriate websites or otherwise putting you or your children at risk. Here too a monitoring software can be a big help. Also, consider using passwords to block their use of your computer and the Internet without your permission. Note that any illegal activities on their part may end up at your front door, and proving who was using the computer to access illegal content or engage in illegal activities may be difficult. The time to think about this is BEFORE they start using the computer.

Making Your Choices: It's your family's choice – making choices you can live with

Before we begin this section, I want you to review the title "...Making Your Choices" Heck, if I wanted everyone to implement *my* choices for their children, my books would be much shorter, just my tips and rules. But this isn't about how I raise my children - it's how you raise yours. I wrote this to empower you, remember? You don't have to answer to others about other parenting choices, do you? No one says anything about how you dress your children or what you feed them (at least not to your face). Homemade chocolate-chip cookies warm from the oven, or stale Chips Ahoy from the cabinet—that's your choice. You should be making the choices that make you comfortable. (But if I'm coming over, the warm cookie thing is a nice idea!)

So, review what I share with you, talk to your child's school and your neighbors. Then think about your values, your life and your child. Finding the right fit isn't easy, but it's worth the time.

Choosing Your Comfort Level

Throughout this section, I've given you lots of information about your options, from straightforward parenting to technological fixes, and everything in between. In increasing levels of control, I've done a quick review of the types of protection parents can offer their children—from relying on trusting them and educating them to never letting them use a computer. As you gain more control, you need to realize that you also limit more information your children can access, both good and bad, and rely less on trust. In addition, the more you limit access to certain sites or services, the more choice you give up to third parties. (Filtering companies choose which sites you can see and which ones you can't. So it's important to make sure you agree with their choices.) That's the balance you'll need to strike. And it's your choice. But know that it's not engraved in stone, and you can and should make changes as your children get older, earn your trust, and have greater needs to access broader content for school.

What Are the Choices?

When I first wrote *A Parents' Guide to the Internet* eight years ago, parents didn't have much in the way of options or choices. Since then, parental-controls and filtering and blocking products have become much better, AOL and MSN have developed very sophisticated and multi-featured levels of parental controls, and a few new powerful monitoring products have been developed. And many new websites that respect our children's safety and provide valuable entertainment and education have been created for our kids, preteens or teens. These are sites we as parents like, but more important, our children love! You can read about some of these at WiredSafety.org and WiredKids.org.

While some parents want their children to be shielded from anything they find objectionable (which may be different from what you find objectionable), others want their children exposed to everything to be able to learn from it. Some couldn't care less about overblocking information, and others think that's the only issue. Others want to use a filtered or kids-friendly search engine, but no other filtering. That's your right as a parent—to set the rules for your family. You can raise your children on sprouts and tofu, or McDonald's every night. In the same way, you can decide what your children should be allowed to do online and where they can go.

But to make a choice, you need to know what's out there. There are now lots of terrific, safe, and entertaining resources online for younger kids, preteens, and teens. Most of them are free, and a few have low monthly subscription fees. There are filtered search engines, kid-friendly Web browsers, and safe-site lists galore. Yet, whether you elect to use a filtering and blocking product, join a kids-safe subscription service, rely on free safe-harbor sites, or a combination of the above, remember that educating your children about online safety has to be the primary defense. Don't rely on any product or sites to do your job, which is to make sure your children are safe and able to exercise responsible judgment.

Adding technology is like using a seat belt and an airbag. Your first defense is being a good and careful driver. The airbag and seat belt add protection if the unexpected occurs, or other drivers aren't as careful as you are. So start with educating them. (We have many fun projects and activities at WiredKids.org, just for this purpose.)

Our children need to be taught to handle different content and difficult situations, to judge credibility and decide what is worth their attention and what isn't. Only education can do that. They need to understand their own family's values in exercising that judgment. And only you can teach your family's values to your children. Filtering may be a big help in many cases, especially when the children are young. But remember, you can't filter life. (Repeat after me...)

And if you are interested in learning more about using technological tools to help you enforce your choices, there are hundreds of different software programs and methods that have been developed to restrict and monitor access to, and rate the content contained in, certain sites on the Internet. Many also restrict information being sent from or being sent to your children on the Internet and online services. While some parents may find these tools helpful, they aren't a substitute for good parenting. When they are used, they should always be coupled with education and good communication. I've included some information about how they work so you can make your own choice about what you need and what works for your family in Internet Safety 1-2-3, Step Three— Implementing and Enforcing Your Choices, below. And I will have some recommendations posted at WiredSafety.org and WiredKids.org.

In a nutshell, here are your choices overall (in increasing levels of control and protection):

- ◆ Trust and education
- ◆ Home safe-surfing agreement (see Appendix)
- ◆ Encouraging use of child-friendly sites and supervising their surfing
- ◆ Tracking use and duration using software
- ◆ Filtered search engines
- ◆ Filtering and blocking at your desktop
- ◆ Using monitoring software
- ◆ Server-level blocking, parental controls on online services, or a filtered ISP
- ◆ Limiting all contact to pre-approved senders
- ◆ Pre-screening all contact
- ◆ Restricting all contact
- ◆ Limiting your children to child-friendly safe playgrounds online
- ◆ Limiting your children to child-friendly subscription services
- ◆ Locking the computer (or using a product that prevents online access) when you're not home
- ◆ Living in a computerless home and community (not an option!)

Note that there is no way to make sure your children are 100% protected—unless you choose to live computerless and make sure that your child's school, friends, and library don't have computers either. Since that is highly unlikely, and even more highly undesirable, recognize that everyone should be accepting some level of responsibility for safe surfing and sometimes things will get through that you wish hadn't. It's a risk we have to learn to live with—to minimize, but learn to live with nonetheless.

Get to Know Your Kids, and Create a Workable "Safe-Surfing Contract" for Them

Unless you are really extraordinary, there are many things about your children that you don't know. Once they leave the house and start school, most of their waking hours are spent away from us. We *think* we know them, but are often wrong.

Use this opportunity to get to know your child better. Find out what your children's interests are. What do they read? What do they watch on television? If they're already on the Internet, what do they access? Even without an ulterior motive, it's a wonderful way to get to know your children. Too often we talk *at* our children, rather than listen to them. And they have wonderful things to tell us if we just listen... really listen.

Ask them to show you around the Internet. Access their bookmarks with them. Don't ambush them and make it look like you're spying on them. Take this opportunity to share some of their interests. You might be pleasantly surprised to learn some of the things that interest them. For instance, how do they find their way around the Internet? Do they rely on hyperlinks (links to other sites), or do they use a search engine? If so, which one? Ask them why they prefer one over the other, and how they formulate their searches. Do they have their own website? Profile? Blog? Instant messaging "away message?" What have they posted? What are they sharing about themselves. You can learn lots about who they are by what they post online. It's not always true, though. Remember that. They may just be showing off for their friends and others online. But how they show off and what they make up about themselves can be very telling too. It's the window into their online souls.

Once you have a better idea about how your children use the Internet, you can start developing a set of rules to govern their behavior online and to guide them into safer waters. Your rules should be designed to help them understand proper Netiquette, know what to expect from others online, how to behave when something unexpected occurs, and how to protect themselves and you from getting hurt in cyberspace. Because I am a lawyer, I needed to do something legal. (Sometimes lawyers can't help themselves. 😊) So I drafted a sample "Safe-Surfing Contract."

Setting the rules shouldn't be one-sided. Like any good contract they should be constructed with input from both sides, in this case - parent and child. They shouldn't be forced upon your children. Part of what makes the rules work is the communication between you and your children when the rules are being designed. Some kids respond well to a written policy signed by both the parents and the child; others would prefer a list to be posted near the computer, as a reminder. You should do what makes you both comfortable. After all, you know your children best.

Points to Consider in Setting Your Own Rules and Drafting Your Own Safe-Surfing Contract

I have given you some basic rules to help you come up with your own family safe-surfing contract, and you should feel free to change them to suit both your and your child's needs. In the list below, I've tried to sum up the most important tips to remember. Consider it your cheat sheet in advising your child. (It also fits neatly on your inner wrist: That way you can keep the parental cheat sheet on one wrist and this on the other—a matched set!)

- ◆ People on the Internet can pretend to be anyone or anything they want. Don't let them fool you.
- ◆ Don't use bad language.
- ◆ Don't get into arguments with or answer anyone who uses bad language.
- ◆ Don't answer if someone says something that makes you feel uncomfortable or that you feel is "bad."
- ◆ If someone is doing something that makes you uncomfortable, you should tell your parents right away. But don't turn off the computer or log out of the area where the person is doing something "bad." (The adult can then find the person and report his activities as a terms of service violation.)
- ◆ Use a fun name when you're online, not your real name (not even your real first name and not a provocative name like "teen girl").
- ◆ Don't spend all your time online.
- ◆ Never give your real name, address, ICQ number, school, parents' names, friends' names,

- where your parents work, your sports team names, your scout troop information, anyone else's e-mail address, or any telephone number to anyone.
- ◆ If anyone asks you for this information, don't answer them, and tell your parents or the adult in charge of the chatroom. (If you are using a special secret cyberspace name, you can give them that instead.)
 - ◆ Never talk to anyone you met online over the phone, send them anything, or accept anything from them or agree to meet with them unless your parents agree and/or are with you.
 - ◆ Never post your picture online or send it to someone without your parents' consent.
 - ◆ Don't put any real information on your blog, profile or website without your parents' (or if they are teenagers, without the surf buddy's) consent. Don't say things in your profile that you know will make others angry or that will provoke "bad" communications.
 - ◆ There are places on the Internet where people talk about and show pictures of things we don't agree with. If you see something like that, click the "Back" button and tell your parents.
 - ◆ Don't do anything online that costs money unless your parents say it's okay.
 - ◆ Never give out your password, even to your best friend.
 - ◆ Never give out your or your parents' credit card or banking information.
 - ◆ Don't copy other people's material and pretend that it's yours.
 - ◆ Don't steal movies, music, software or games online.
 - ◆ Use an anti-virus program and spyware blocking program, and run all attachments through them before you open them.
 - ◆ Don't rely on strangers you meet online for important advice.

Formalizing the Rules

I've included a sample safe-surfing contract at WiredSafety.org and in our Parenting Online Guide. But, I'll tell you what I tell my legal clients when they ask me if they should use a form agreement. If it fits all your needs, use it. Otherwise, you should use it as a guide in writing your own. Sometimes parents think I'm being overly legalistic in suggesting drafting a written policy. It's not a legally enforceable contract, it's a guide. If you discuss these issues with your kids, you never have to write one out. (Use this as a checklist to make sure you covered everything.) You want to make sure that you've really discussed each point, that they understand what you've discussed, and that they have agreed to follow the rules. Once you do that... there's no need for a written policy. Kids are the ones who like them, though—it makes them feel part of the decision-making. But remember that the issue here is communication, not your ability to sue your children for breach of contract. ☺

Enforcing the Rules

It's one thing to set rules and another one to enforce them. Saying "no!" when our toddler decides that a fork is exactly the right size for the electrical outlet isn't enough. We have to put down the laundry or whatever we are doing and move as quickly as possible to take the fork out of their hands and give them something else to play with -- something safer. The Internet is no different.

We have to check on them, correct them, remind them and do it all over again the next day until they finally "get it." The good thing is that as hard as it looks, there are some technology tools designed to help you. I've described the different kinds of filtering, monitoring and blocking

technologies, as well as "walled gardens" of safer sites for kids, and online communities designed with your teen in mind.

And we aren't off the hook when we finally get them to follow our rules in our home, on the family computer in a central location. (You knew there was a catch here, didn't you? :-)) You also have to figure out which of the handheld devices you bought them allow them to disobey you when you aren't looking (assuming they are so inclined) and how to monitor their use of those devices.

Here too, several trusted companies have provided parents with some technological help. Disney Mobile is a new cell phone handset and service that gives parents an online dashboard that allows them to control what their kids can do on their Disney Mobile phone. It can turn off the phone entirely (except to receive and make calls to the parent) if the parent needs to enforce their rules, or just limit what hours and for how long their kids can use the phone. And several other services have limited calling and content filters for cell phones and various mobile devices as well. At WiredSafety's new WiredMom's section, we'll be reviewing these tools and software from a moms' perspective and share what we have learned with everyone here at Yahoo!

Just remember, when it gets hard and your teen is pounding their fists on the floor screaming that we are ruining their social life for limiting their instant messaging or use of profiles, that this too shall pass. And, no matter how much they know about technology, you know more about life. You are still the parent. Repeat after me -- "Because I said so!" "I don't care what Jennifer's mother let's her do..." "If Mike jumped off the George Washington Bridge...[feel free insert any bridge closer to your home in this example]. "As long as you're living under my roof...." Sometimes, our parents really did know best. You ARE the parent. Remember that!