# Keeping Yourself and Your Family Safe Online

Everyone talks about protecting children online. The media loves cases of Internet sexual predators and high profile risks. But what about protecting yourself and the rest of your family? The rules and tips that keep your children safer online keep the whole family safer online too. It's easier than you think.

Before we start talking about the risks, let's talk about the benefits. The Internet holds more books than the largest libraries in the world. It's open 24/7 and speaks all languages. Most of the sites and online content is free. And the rest is pretty affordable. You used to have to research questions for weeks. Now you can search multiple sites in minutes. You can keep any eye out for new sales, something related to your favorite hobby, and sports scores. You can support a cause or keep in touch with your high school classmates. The list goes on and on.

Try exploring with your children. Have them show you their favorite sites, try playing a game or two online with them or explore new sites that you will all enjoy. Find a cooking site and experiment with some recipes they would enjoy. Or plan a trip and research the place you would like to visit.

Start with something you enjoy and follow the cyber-breadcrumbs to explore a bit. (Just make sure you use a good antivirus, spyware blocker and firewall.) Research your family tree or plan an adventure. You can begin with Google and use the filtered settings to block most of the junk. Or look for a site you like or an article you trust and click away from there.

If you find a site you like, bookmark it so you can revisit it and recommend it to your friends and family.

### Mobile and Handhelds

Adults use their mobile phones to make calls, sometimes send text messages or pictures or send emails. Most of the other features go unused by most of us. Frankly, we have no idea what those features are half the time. Why not check out some of those features? Visit the mobile manufacturer's website and see what you can learn, or hand it over to one of your children to show you.

Everyone has an iPod or other digital music player. Some just play music, while others can store or stream your favorite TV show or videos. And you can visit iTunes.com and download podcasts and videocasts that interest you, find your favorite music from high school, or convert your CDs (or vinyls) to digital versions and enjoy them on the go.

Your children use these handhelds all the time, almost as often as their teen counterparts use their cell phones. They store pictures, videos, games and music on them. They also often store contact information and their schedules. Unfortunately, these photo-capable devices are sometimes used to take embarrassing pictures of others, or sexual or nude ones of themselves as they get a little older.

Teens have identified 87 different ways a cell phone can be used to cyberbully others. From placing prank calls, to sending thousands of tormenting text messages, to reprogramming it to call 911/999 whenever they speed-dial Mom, to posing as them to torment their friends, accessing private information and intimate images, the list goes on and on.

Intimate images taken when they are bored, infatuated or under the influence are becoming more common. These are typically called “sexting” and is when a preteen or teen takes a nude or sexual picture or video of themselves and share it with their boyfriend, girlfriend or anyone who is interested. (Talking sex isn’t sexting, only pictures and video are.)

Far too many teens and a surprising number of preteens are engaged in taking these pictures, sharing them with others or storing them on handheld devices, cell phones, gaming devices or their computer.

When teens and preteens are hanging out in groups, they frequently get into trouble with their cell phones. They take photos they shouldn’t be taking. They place prank calls. And often send text messages that shouldn’t be sent. They use the cell phones to bypass traditional computer filters.

Some parents have come up with a simple solution to these risks. Have your children’s friends (and your child) park their cell phones with you while at a party in your home. Give them back when they leave and let them use your house line to call anyone they need.

Cell phones are now providing them with more power in their backpacks, pockets and purses than most big corporate computers could provide a few years ago. It’s an area where we are seeing abusive and risky behavior very often. Ask your children to show you their own cell phones and mobile devices. Make it a surprise spot check. Then scroll through the pictures and videos they store. (Check their cloud storage accounts too!)

Tried and trusted safety tips about keeping their computers in a public place are long out of date. Now, they have to rely on the filter between their ears and exercise good judgment and care wherever they are connecting or using technology. It’s our job as parents to upload our values and common sense to those filters on a regular basis.

**The 3Cs – Content, Contact and Cost**

Unless you have a safety guide on every single device and feature in your household, it’s hard to keep up. Parry Aftab created the 3Cs to help. They stand for “contact,” “content” and “cost.” By using them, you can spot the risks and solutions for each risk, technology by technology, application by application and device by device without a degree from MIT.

Contact risks relate to direct communication features. How can people contact you using the technology and how can you (or your children) contact others? These include text messaging, instant messaging, phone calls, emails, direct messages, Twitter, Facetime, Skype and chat. It also includes voice chat on video game devices, such as Xbox.

Content risks include all information and media. It includes personal information posted online, as well as music, movies, video and text content. It covers pornography, misinformation, hate, and hype, as well as all other content issues.

Cost has two parts. One relates to commercial risks, like targeted advertising, ID theft, hidden charges or fraud risks. The other relates to all financial risks, such as lawsuits for pirating music, viruses that destroy your data or your devices and someone calling China too often from their cell phones. (In Europe this 3C approach is content, contact and commercialism, reflecting a sensitivity to marketing to children online.)

Once you can identify which risk or combination of risks apply to that feature, application or device, finding a solution is easier. Some involve education or warnings – "Don't call China too often!" Some can be remedied with technology tools, such as device settings, anti-virus programs and spyware blockers. And some can only be managed by avoiding them entirely – such as not giving a child who is too young to handle it correctly a multi-feature Internet-ready cell phone or gaming device. It comes down to being a smart consumer and making the right choices child by child for your family.

### Technology: The Risks to Your Children by Age

If your children are 8 or under:

Here are some basic guidelines to get started on setting rules for children under 8 years of age to follow when online. Think of these as a "cheat sheet." Most of the children under 6 are not yet interactive (with the exception of virtual worlds, videos, educational games, YouTube and DS).

They are not yet using messaging, e-mail, text or chat technologies (to their parents' knowledge), without parental supervision or their heavy use of parental controls. This is changing, though, with many younger kids using interactive sites for preteens.

We advise that parents carefully supervise their kids' use of these sites until they are old enough to understand risks online unless the sites have a safe site or other trusted seal of approval. If your kids are more interactive, use the tips for the next older group below.

8 to 10 Years:

Most are beginning to use interactive technologies, such as messaging, texts and cell phones, and the more precocious may also be trying to use social networking/profile sites, such as Instagram or Facebook, by lying about their age.

Cyberbullying starts to expand at this age. Cell phones are becoming more common in this age group, as are all gaming devices, handheld and laptops. Spyware is typically a real problem at this age too, as they begin to download things and use game cheat and code sites, usually rampant with spyware.

Kiddie hackers start their tricks often during these early years. (And they may include your child or one of his friends.) Keep intruders out with a firewall. And passwords, as with all ages, are the root of all cyber-evil. Choose one that is easy to remember, but hard to guess and is different for each site.

Older Preteens (11 – 12 year olds)

Most in this age range are now using interactive technologies and many have cell phones at this age. All are playing interactive games, some on handheld gaming devices or desktop devices, some on their cell phones or iPods, some on their PCs and some online. Parental controls become trickier with they reach 11 or 12, because they tend to over-block the sites they want and need. The settings become complicated and the fit is rarely right.

They are also entering the prime of their cyberbullying life. Social networks/profile sites are a growing problem at this age. This is the age range is when the trouble usually begins. They want to be "older" and do what they think teens do. That means they are taking risks by the truckload. Sexting (when they send sexually provocative or nude pictures of themselves to others) starts at 12 with some girls. They often lie about their ages on social networks too to get past the age rules.

Early Teens (13 - 15 Years)

Social networks such as Facebook, Instagram, YouTube, Tumblr and to a lesser degree, Twitter, along with texting and gaming consume their time and lives. (YouTube is vastly the most popular of these, with more than 78% of teens polled having an account on YouTube.) Parental controls are not effective at this age. Gaming devices and handhelds are being used by most of the younger male teens and they can access the Internet from their palm-tops and gaming devices, often without parents knowing. Risky behaviors and the attraction of 15 megabytes of fame cause many of the younger teens to act out, either because they don't have the tech safety skills or the judgment to act otherwise.

They are vulnerable, impulsive and often in need of attention, affection and approval. This is when the risk of meeting and inappropriate communications with strangers are the biggest problem. The 13 year olds are at the greatest risk, and most serious cases of sexual exploitation by adult online occur at this age.

They want to act and be seen as older and more mature and are often flattered by the attention of adult men. (Note we are now seeing female Internet sexual predators exploiting young teen boys they meet on interactive game sites.) Luckily, the younger teens tend to fear sexual exploitation and tend to avoid offline meetings. If the young teen is at-risk, they are particularly at-risk to adult predation.

Sex tends to be a big draw at this age. Cyberbullying turns into sexual harassment at this age too. Most cyberbullying-related suicides involve 13-14 year olds, more often than other age groups. It's a tough time for them. Be understanding and remember back to when we were that age. Technology magnifies these risks, so teach them to exercise care and use good judgment.

Teens 16 Years and Older:

Their offline reputations and future can be easily impacted by what they do and post online. College recruiters, coaches, scholarship committees, employers and sources of recommendations, as well as their high school administrators, can be watching. Texting, Instagramming and social networks rule their existence, along with gaming devices (more for boys than girls in this age, as tween and young teen female gamers move on to other interests).

The risk of Internet sexual predators and everyday cyberbullying decreases, while online sexual harassment attacks, sexting and sextortion (blackmail involving the threat to expose intimate images) increase when romantic interests get involved. The teens, interestingly, spend more time with focused online activities or offline activities and spend less time texting and more calling on cell phones than they had in previous years. Chatlingo and emoticons are out too. ("OMG" and "LOL" are examples of chatlingo.) They may use shortened forms of words when texting or messaging, but they leave chatlingo and emoticons behind them. "They are sooo middle school," they claim.

Sexting becomes more common at this age, when they are often sexually active and when asked, will share a nude picture with someone they "love" and trust. And this often moves off of cell phones to webcams and other digital imaging devices to share in other ways.

Colleges, jobs, scholarships, awards, team selections and rankings are all more important than ever at this age. (And, yes, colleges are looking.) What they post online stays online forever, in one form or another. All bets are off here. If they aren't ready by 16, they will never be ready. It's time to take off the training wheels and be around with the first aid kit when they take the inevitable spill. Good luck! You'll need it.

**Passwords – The Route of Most Cyber-Evil**

Most of our children (and we do too) choose passwords based on “20 Questions.” They use the same 20 questions to come up with their passwords, like their middle name, their pet’s name, their birth date,

the town they live in, their favorite movie, their best friend’s name, the car they want to drive, the year they graduate, the college they want to attend, etc. The problem is that these are easy to guess for anyone who knows them pretty well. Just think about how many of these you could answer about your friends and others in your family members. And if you can guess theirs, they can probably guess yours too unless you are careful. And since most cyberbullying happens among classmates and acquaintances, they are vulnerable to their “frenemies” taking over and accessing their online accounts, sometimes posing as them to get them into trouble.

Security experts tell you to use a password with upper and lower case letters, numbers and symbols. That might be good for security experts, but it’s really hard to remember. So, you have to write it down or stick it on a post-it sheet on your monitor to remember. That’s not very secure, though.

Instead, use a sentence with a number in it. You start it with a capital letter and end it with punctuation (a symbol!). Upper case, lower case, numbers and a symbol. Easy to remember and hard to guess. You can use the site name in the sentence and you’ll have what security experts suggest, a different password for each site that is secure and easy to remember. “Facebook has more than 1 billion users!” Holy cow! (And it’s a pretty good password once you leave out the spaces.)

Or choose something only you would know, that is easy for you to remember and no one else can guess (even and especially your children). Choose your favorite character in a book and how old you were when you first read that book, or the best birthday present you ever got and how old you were when you got it. That gives you numbers and letters and is easy for you to remember, but hard for others to guess. Get it?

More than 85% of elementary school students and 70% of teens polled said that they had shared their passwords with at least one friend (often their boyfriend or girlfriend). That’s one friend too many, especially when friends get into fights or couples breakup. It’s not smart since when armed with their secrets and your passwords, your children’s friends can do some serious damage.

Don’t click “save my login and password” when using a computer that anyone else can access. And logout of your accounts when leaving your work computer untended, even and especially at home.

**Cyberbullying and Harassment – Using Technology as a Weapon**

*Separating the Men from the Boys*
Cyberbullying is when one young person uses technology as a weapon to hurt another. It’s called cyberharassment when adults do the same thing. When someone takes over your accounts, passes

nasty rumors, poses as you or makes private information public to hurt you, it's cyberharassment. When they do it to your children, it's cyberbullying.

Often adult offline disputes turn into cyberharassment. You end a marriage, break up with someone or have a problem at work and it goes online. But sometimes it starts by accident, and the person who receives your message feels attacked and launches a counter-attack against you. "They started it" doesn't matter. All fifty states have cyberharassment laws and if you send a message online designed to harass or annoy someone anonymously, you can go to jail for up to two years under federal law too.

The best way to handle any harassing message you may receive is by following the tip we created for elementary school students - "stop, block and tell!" You should stop and not answer back. It only feeds the harassment campaign. You should block the person or message. Why torment yourself further or give them access to you? And you should tell someone you trust to help you deal with it and keep it in perspective. (Seventy percent of cyberharassment and cyberbullying occurs anonymously, so you never know if it's your best friend, neighbor, coworker or ex.)

And if you are tempted to answer back…do something else. Parry Aftab, WiredSafety's founder, calls this "Take 5!" Do something you love to do for five minutes to help you calm down.

Review the tips for preteens and those for teens to learn more about how cyberbullying works at that age. Your role in any cyberbullying episode involving your child as the target is to be supportive. Give them a hug and tell them that you are sorry this happened to them. Promise not to make things worse and keep that promise. Visit StopCyberbullying.org to download the checklist for parents to help you understand if the police should be contacted. And remember that it took lots of courage for your child to come to you (only 5% of teens polled said they would tell their parents). Be worthy of that trust. Help them, don't overreact and make things worse. Before you call the FBI, RCMP or Home Office, give them a hug and make them feel loved, appreciated and safe.

**Safe Shopping and Banking Online**

Shopping online is one of the best things about the Internet. You can find bargains, collectibles on Craigslist or eBay. You can download the latest CDs and locate that hard to find size. You can compare prices and conduct an online garage sale. It's open 24/7 and makes our lives easy. No traffic (at least not the vehicle kind) and no rain, snow or problems parking.

The problems come from scams, cybercriminals, and forgetting the one thing all shoppers have to remember – "Buyer Beware!" If it appears too good to be true, it's for a good reason – it's NOT true!

Start with trusted offline brand sites. The ones that have brick and mortar stores are sometimes easier to deal with when you need to return something or want a number to call for customer service. Then branch out to sites you can trust online, like Amazon. The further you stray from well-known brands, the more careful you have to be. See if anyone has certified their security practices, like VeriSign or McAfee Secure. Check and see if they have a privacy seal or the Socially Safe Best Practices Seal from WiredTrust (also founded by cyberlawyer Parry Aftab). Click on the seal to confirm that it is up to date.

Read the privacy policy (no matter how boring it is) and their terms of service. See if they offer returns and if so, who pays to ship them back. Search for the item in Google to see who else is selling it and for how much (always including the shipping price and sales tax when comparing prices).

When you are convinced it's what you want, at the right price and from someone you trust, the hard part begins. How are you going to pay for it? Keeping your bank details secure is crucial.

PayPal (owned by eBay) is now being used as a trusted payment method at many sites, not just eBay. It allows you to pay directly from your bank account, without the buyer having your banking information and gives you the option to use a credit card to fund the purchases as well. Note that if you pay from your bank account, certain consumer protection options that apply to credit cards may not be available to you if things go wrong. So, always select the credit card option when using PayPal.

All US credit cards are required to correct any billing related to fraud. They also have an obligation if you notify them in the manner set out on the back of your bill (and by certified mail!) to credit any charge related to a certain kind of dispute. And if you have a valid dispute that isn't resolved by the seller, that credit becomes permanent. Even if PayPal and other payment mechanisms offer you buyer protection, it may not be as good as what you get under existing credit card dispute laws. So, if in doubt, opt for a credit card payment.

But, even though using credit cards is safer when buying online, if you don't check your credit card statement you may miss fraudulent charges and early signs of ID theft. So, check them and let your credit card company know if you suspect unauthorized charges or fraud as early as possible. Some scammers only bill your card for small charges, under $10. We often overlook smaller charges and $10 times 500,000 unsuspecting victims can make you rich!

WiredSafety recommends using one card for all online purchases. It's easier to track spending and protect your financial identity at the same time.

When buying on sites such as Craigslist, where anyone can post an ad without having to prove their identity or the truth about their ad, be especially careful. Go with others to check out the item being sold, never get cornered alone in the basement or house and make sure you are certain it's what you want, at the price you are willing to pay for it and have all the pieces before you leave. Most Craiglist sellers don't accept credit cards. They are mostly people like you, selling something they don't need anymore.

If you are selling on Craigslist or Kijiji, don't let people drop by when you are alone. Move the item to the driveway, garage or other open area for them to check it out. You don't want anyone in your house you don't know. Make sure you are paid in full (preferably by cash) before they take the item or any part of the item. (You won't be able to sell a dresser without one of its drawers, or a set of china with seven place settings, very easily.) Don't hold an item. First come- and- paid- for first-served should be your motto.

Talk to your bank about security tips. Select a special password that is especially hard to guess for any financial sites and transactions. Don't save it on your computer. And don't share it with anyone, especially your children who may be tempted to buy that big screen plasma TV they wanted or share it with someone offering to split a $50 million dollar inheritance from Nigeria's president with them if they put up the first $5000. And check your bank statement every month as soon as it arrives. Some banks allow you to set an alert to let you know if there are online transactions or purchases being made using your account. Ask your bank.

We work too hard for our money to lose it to scammers, criminals and creeps.

### Security, Family Safety Tools and Resources

Security includes choosing a good password and using it the right way. It includes not sharing too much personal information online and keeping private information private. It also includes using a firewall, antivirus, spyware blocker and pop-up blocker to make sure your machine remains clean. It's a way of life online and offline.

We have locks on our windows and on our doors. In case someone breaks a window to get in, we sometimes have burglar alarms too. We teach our children to shut the door behind them and take their keys. We keep valuables in a safe place, medication out of the reach of children and cash away from our teens.

The Internet and digital technologies, such as cell phones, Xbox and handheld gaming devices like Nintendo's DSi or iPods and tablets, have to be treated as securely as other important things in our offline lives. Shut down the device when you are done. Logout before turning it over to your child, to make sure they log in as themselves using the security settings set for them. Don't share your password with others, save it on computers used by others or post it on your monitor.

Keep your adult surfing private. Certain things that are acceptable for consenting adults may not be as acceptable for their kids when they check out what Daddy was doing online last.

One in ten laptops is lost or stolen. Back up your data regularly and keep it safe. Use passwords when you can to control who can access your data on the laptop. Securely wipe old data off of your computer hard drive before selling it, giving it away or throwing it out. A simple "delete" doesn't delete anything. Buy a DoD-grade wipe technology to make sure what you deleted stays gone.

Use passwords, if available, on your cell phones too and parental controls on the Xbox. Check devices for the 3Cs risks before turning them over to your children and use up-to-date anti-virus programs. If your children are ten and under consider using a good family protection product, and make sure you secure your wireless Internet router. If you start safe, you can stay safe!

### Learning More

While WiredSafety's advice is flexible and applies to all technologies, things change fast. So stay involved and informed. Follow us on Twitter, volunteer at WiredSafety or sign your children or teens up for one of our Tweenangels or Teenangels programs.