The Ultimate Parent Guide for Protecting Your Child on the Internet by Ariel Hochstadt

Introduction

We see news stories about the impact of technology on our everyday lives all the time these days. Many of us started to think about how technology affects us personally. But how many of us have stopped to think about how it affects our children?

85% of mothers said they use technology to keep their children busy.

Kids are receiving their first internet-capable device earlier and earlier. That same study showed that **83% of American households have tablets, and 77% have smartphones**.

Even in school, technology is abundant. Teachers set homework that requires online research and tools and use apps to manage that homework.

Technology is always adapting and it's here to stay, but many do not think about the safety risk in terms of cybersecurity. A recent study revealed a startling figure: **68% of parents never check their children's online activity**. And that online activity increases year after year.

For a lot of children, the online world is more real than the real world. **It is crucial to our children's wellbeing that we understand what they see online, what is out there, both good and bad, and how it impacts their physical and emotional wellbeing.**

The problem, as many of us would eagerly admit, is that we feel we don't really understand the online world. Instagram, Snapchat, and Twitter are bewildering enough, without even

mentioning 4chan and TOR. Furthermore, we don't feel that we have the technical skills to navigate this complex landscape.
The good news is that **it's not that difficult to put certain technical controls in place to protect your children online.** Far more importantly, **the best thing you can do to protect your children is to talk to them;** set clear boundaries for what and when they access online, but also to be there for your children when they make a mistake, or when they have gone too far. Isn't that what parenting fundamentally comes down to?

In this comprehensive guide, we outlined eight areas that you should pay attention to as you navigate this complex online world. Depending on the ages of your children, not all of it will apply to you. Think of it not only as guidelines for what you should do now but what you should pay attention to as your children grow.

1. Mobile phones and apps

According to consumer research by Influence Central, the average age that children get their first smartphone is 10 years old. Giving your child a smartphone comes with numerous benefits. A phone is an excellent safety tool; your child can use it to let you know they safely reached their destination, call you for a ride, or call in case of an emergency. You can also use the GPS on their phone to track their location. Knowing that you can always reach your child is a tremendous peace of mind for a parent.

Smartphones, however, can also be misused, and in some situations can make children vulnerable. Because smartphones are personal devices, we don't often know what our children do on them, or how they use them.

If you're considering giving your child a smartphone, it helps to have some clearly outlined guidelines in place beforehand, so everyone is on the same page. If your child already has a smartphone, it's not too late to review the family rules. Demonstrate to them that having a smartphone is a big responsibility.

There are many precautions you can take to implement phone safety:

- Have your kid sign a smartphone contract before you give them one. Print out a list of cellphone rules and stick it in a public place in your home.
- Download parental controls. Parental control apps for younger children enable you to limit your child's usage, determine their location, and monitor their calls and messages. Apps also allow you to shut off certain functions at different times. For example, disabling text messaging while driving.
- Set limits when your child can use a smartphone and for how long each day.
- Set a personal example for your child. Don't bring your phone to the dinner table, and don't text and drive.
- Set up a charging station in a central location in your home. Phones should stay out of your child's bedroom and they won't be in use late at night.

2. Streaming content and smart TVs

We like to think back to a time when the whole family gathered around the TV to watch something wholesome together. (In reality, many of us probably had a TV in our rooms, and spent many hours watching TV without much guidance from our parents.)

That being said, streaming content has shot up in popularity, and there are more TV shows and movies available at our fingertips than ever before, much of it not particularly appropriate for kids.

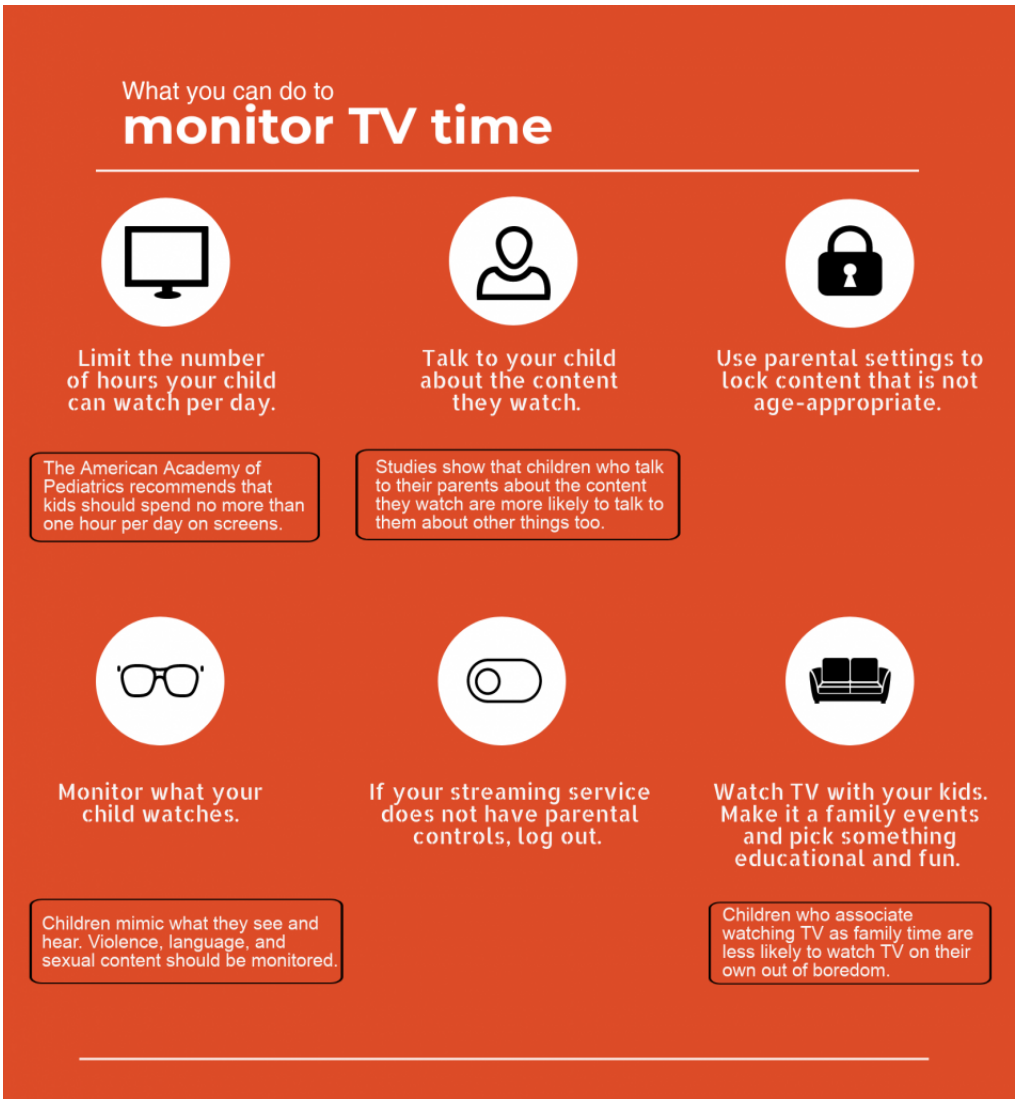
There are, however, some **great benefits of streaming services**. Many feature great, educational children's programming and documentaries. Most don't show any ads, meaning that your kids won't be bombarded with commercial messaging from all sides like they are when they watch regular TV. You can open up an entire world for your children with streaming content – the key is how you use it.

Most of the big streaming content providers have parental controls, some more robust than others. Netflix allows you to set up separate profiles for you and for your children.

Using these tools, you can **ensure that your kids only have access to age-appropriate content**. Because Netflix's children's menu features a different color scheme than the regular menu, you can easily see whether your kids access the content permitted to them or not. However, this doesn't stop kids from moving over to your profile, so you still have to be vigilant.

iTunes and Apple TV allows parents to set rating levels for the content their children watch. By contrast, Amazon Prime features no parental controls, so the only thing to do is to logout of your account and not share the password.

All of these tools, however, do not replace having frequent conversations with your children about what they watch.



3. Gaming consoles and online games

According to the NPD group, 91% of American children aged two to 17 play video games. **Gaming consoles have long been a focus of fear and concern for many parents**. With so many games featuring violent or sexual content, **it is important to be careful about the kinds of games your children play.**

In addition, console games that have a multiplayer component, or games that are entirely based online, are **open to abuse from other players**. Many games allow players from all over the world to chat with one another, potentially **exposing kids to harassment and cyberbullying**. Kids may also form relationships with other players and may give away their personal information.

Games are also a great way for kids to develop a variety of skills. They help children develop problem-solving skills, learn how to commit to long-term goals, and how to work as part of a

team. They can also be a great opportunity for family bonding. Luckily, most gaming consoles provide robust parental controls, so **parents can monitor their children's gameplay**.

Encourage your children to discuss the games they play. Make sure your child profile is set to private. Consider keeping the gaming console in a shared, social space. Study the age rating of the games. Use parental controls to set up profiles. Limit the type of people your child can speak to online.

4. Social media

While the format has changed, parents have worried about their kids' TV shows and video games for years. Social media, on the other hand, is a new worry to add to your plate.

Social media usage is now ubiquitous amongst US teens; 71% use more than one social platform. Children nowadays also spend an enormous amount of time on social media. A survey

by the non-profit group Common Sense Media showed that **8 to 12 year-olds were online six hours per day**, much of it on social platforms, and **13 to 18 year-olds a whopping nine hours**! According to a recent Harvard study, even though most social media platforms require users to be 13 years of age to sign up, 68% of parents surveyed had helped younger children set up an account.

Social media can be particularly addictive for tweens and teens. It also opens the door to a variety of different issues, like cyberbullying, inappropriate sharing, and talking to strangers (more on those below).

Access to social media is also central to teens' developing social identity. It's the way that they connect to their friends, and it can be a healthy way to hang out. The key is to figure out some boundaries so that it remains a positive experience.

Enforce a safe environment. Do not let your kids on social media until they're old enough. Keep the computer in a public location. Limit the amount of time spent on social media. Block location access to all apps. Adjust the privacy settings. Monitor your child's online activity.

5. Cyberbullying

Our children's lives have moved online. Unfortunately, their bullies have moved online too. Cyberbullying is frequently in the news, with reports of teen suicides due to online harassment. **Cyberbullying occurs across all of the platforms we have outlined above**, and it comes in many forms: spreading rumors and sending threatening messages via social media, texting, or email, pretending to be another child and posting embarrassing material under their name, forwarding private photos without consent, and generally posting online about another child with the intent to humiliate or degrade them.

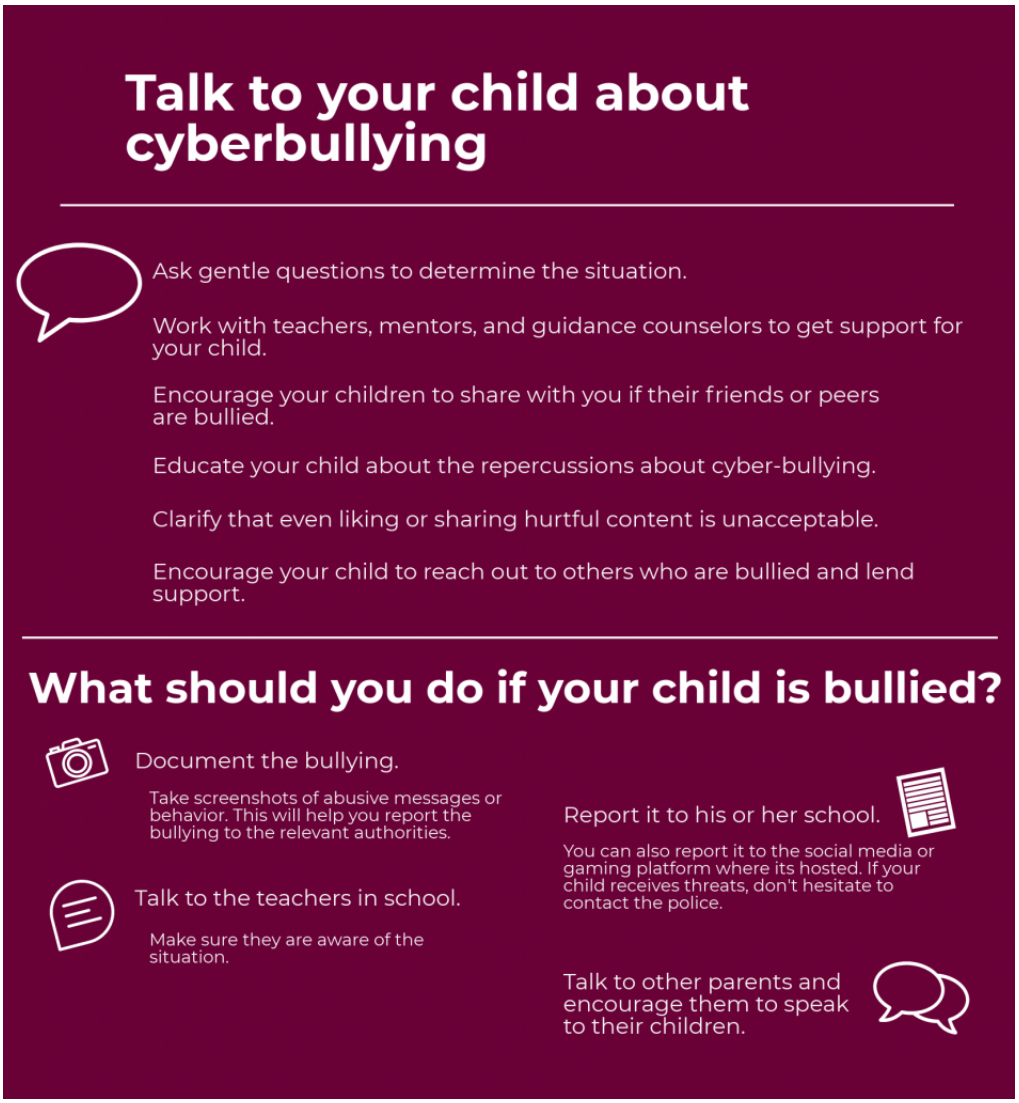
Cyberbullying is particularly harmful because it is so public. In the past, if a kid was bullied on the playground, perhaps a few of his peers saw. Now, a child's most private information can be splashed across the internet and is there permanently unless reported and taken down. Cyberbullying can negatively affect the online reputation not only of the victim, but also of the perpetrator, and have a deep impact on that child's future, including college admissions and employment.

It is also extremely persistent. If a child is the target of traditional bullying, his or her home is more often than not a place of refuge. Because digital platforms are constantly available, victims of cyberbullying struggle to find any relief.

It's often very difficult to tell if your child is being bullied online. It happens online, so parents and teachers are less likely to overhear or notice it. **Fewer than half of children bullied online tell their parents or another adult what they are going through**, according to internet safety organization i-SAFE. In fact, according to a US government survey, **21% of children aged 12 to 18 have experienced bullying, and an estimated 16% were bullied online.**

The best way to prevent cyberbullying or to stop it in its tracks is to be aware of your child's behavior. A number of warning signs may present themselves.

A child who is bullied may shut down their social media account and open a new one. He or she may begin to avoid social situations, even if they enjoyed being social in the past. Victims (and perpetrators) of cyberbullying often hide their screen or device when other people come into their vicinity and become cagey about what they do online. They may become emotionally distressed or withdrawn.



Talk to your child about cyberbullying.

5. Privacy and information security

As parents, we are most concerned about the effect of the online world on our children's emotional and physical wellbeing. Children are susceptible to information security threats that can cause financial harm. These are the exact same threats that adults face: **malware and viruses, phishing scams, and identity theft**.

The issue is children are far less experienced and are generally far more trusting than us cynical adults. To kids, sharing their personal details, like their full name or where they live, may not seem like such a big deal. **They may even be tricked by a malicious third party into sharing your credit card details.**

There are a number of ways that hackers and thieves can get information out of children. Free downloadable games, movies, or even ringtones that market themselves to children can place viruses onto your computer and steal your information.

Hackers posing as legitimate companies like Google send emails purporting to ask for your child's password. Or, they may pose as one of your children's friends.

What should you communicate to your child?

- **Have a discussion with your kids about the big threats online today**. Make sure they know what a phishing attack and a disreputable games website looks like, so they know not to fall for these scams.

- Make sure they keep all of their information private and that they never publish their full name, phone number, address, or school they attend in a public place.

- Talk to your kids about passwords. Having a strong password is the first and best measure to prevent hacking and identity theft. Using a secure password generator like the one we created is great for this occasion, and trying out passwords together is a fun way of ensuring your child's password is as strong as possible.

- Tell your kids to avoid using public wifi – this is an easy way for hackers to get into their devices.

What you can do to create a safe environment:

- Install a strong antivirus program on your home computer and the devices of all family members.

- Think about installing a VPN on your computer. A VPN, or virtual private network, encrypts your connection and anonymizes your web browsing. This makes it far harder for hackers to access and steal your private information.

- If you and your kids use a lot of different devices around the house, consider installing a VPN on your router. That way, all internet traffic that goes through the router will be protected, without having to install the VPN on every device.

- Install an ad blocker so your children won't have to face deceptive advertising that encourages them to download malicious programs onto your computer.

- If your kids have smartphones, make sure that their security settings are set to maximum.

6. Viewing inappropriate content online

Because the internet is so open and public, it is also a place where kids can stumble upon content intended for adults, content which they may find upsetting, confusing or distressing. "Inappropriate content" can mean many things to many different people, from swearing to violence to sexual nature.

It's not easy, but eventually, you will need to have a conversation with your children about what they might see online. **Many children don't go to their parents when they see something they perhaps shouldn't have seen**, for fear that their parents will be angry at them, and take away their devices or internet access.

If your child comes to you with this type of issue, **the best thing to do is to respond calmly and be open to discussion**. If the content under discussion is sexual, your child will likely be embarrassed already, particularly when talking to their parents about these kinds of issues. Let them know you are there for them and are ready to answer any questions without judgment. Young people may see sexual content online for all kinds of reasons. They may have seen it by mistake, a friend might have sent it to them, or they may have sought it out themselves out of natural curiosity.

It helps a great deal to talk to your kids honestly and frankly about sex, and a discussion about online pornography is a crucial part. A lot of research has shown that pornography can have a detrimental effect on young people, giving them distorted and unhealthy notions about sex. Pornography can also lead people to think of others as objects, rather than people with thoughts and feelings. At the same time, it's totally normal to be curious about sex and relationships. **This conversation is a great opportunity to direct your kids to positive resources about sexuality.**

There are also a number of steps you can take to try to prevent your kids from being exposed to content they're not ready for, like setting up parental controls on your internet connection. Remember, though, that technical fixes can't replace open communication with your child.

Communicate with your child:

- Let your kids know that they can always come to you if something is bothering them, or if they have questions about anything they have seen online.

- Let them know that it's totally normal to be curious about sex. Direct them to positive online resources like Brook and Thinkuknow. Thinkunow is particularly good for younger children, and it includes different, age-appropriate sites for different age groups. You may find it helpful to look through the site together and discuss some of the issues.

Steps you can take to block inappropriate content:

- **Set filters to block inappropriate content like pornography.** Your ISP (internet service provider) should provide free parental controls, as should most gaming consoles. These are usually pretty easy to set up.

- Set Google to "safe" mode so that your children won't inadvertently see inappropriate content in search results.

- Install an ad blocker to prevent viruses that might have inappropriate content.

7. Online predators

In our last section, we take a look at the darkest and scariest online threat of all: online child predators. According to the US Department of Justice, **13% of young people with internet access have been the victims of unwanted sexual advances, and one in 25 children have been solicited for offline contact.**

Predators engage in a practice called "grooming". In other words, they attempt to form a relationship with a child with the intention of latter abusing them.

The internet has made life a lot easier for child predators. **Predators target their victims through any and all online mediums: social media, email, text messages, and more.** By far the most common method, however, is via an online chatroom: **76% of online encounters with sexual predators begin in a chat room**.

Predators often create multiple online identities, posing as children to trick kids into talking to them. They discover as much as they can about the children they are targeting by researching those children through their social media profiles, and what they have posted on chatrooms. They may contact a number of children at once but tend to concentrate their efforts on the most vulnerable. These predators aren't satisfied with merely chatting with children online. **They frequently trick or coerce their victims into online sexual activity, via webcam or by sending sexual images.** They may also attempt to meet and abuse their victims in person.

It's not always easy to tell if a child is being groomed, particularly because most keep it a secret from their parents. **There are a number of warning signs**: children who are being groomed by predators may become very secretive because the predator often threatens the child not to share information with their parents or friends. Children can also become sad and withdrawn, distracted, and have sudden mood swings. It is absolutely crucial to let your child know that you are there for them and that they can talk to you about anything.

What should you communicate to your child?

- **Have a discussion with your child about the risks of online predator**s. Make sure they know to be careful about who they talk to online, and not to share any personal information with strangers.
- Tell your kids that they can come to you with any problem, no matter what it is.
- Think about working through some educational content with your children relating to this topic, like the excellent videos at Thinkuknow.
- If you think that your child is at risk, **seek support from their school, a social worker, and the police.**

Conclusion

There are lots of different technical tools available out there to help keep your kids safe online. These vary from VPNs and antivirus software to internet filters and parental controls. **But none of these are really enough to help keep your child safe**.

As we've repeated over and over in this guide, the key isn't mastering a set of complicated technical tools. (In fact, most are very easy to set up, so don't let a lack of technical ability hold you back). It also doesn't mean you have to master the latest internet fad every time one pops up – believe us, you will never keep up!

The far more important, but also far more difficult task, is to have **frequent, open and honest discussions with your children about their lives**. Remember, internet companies, social media networks, gaming providers, and everyone else in the online space may be able to help you set content limits, but they don't necessarily have your child's best interests at heart.

The very best person to keep your child safe online is you. Talking about how to stay safe on the internet is an excellent conduit to build a trusting and positive relationship with your child. Internet safety needs to be a priority for every parent and caregiver. If you have found this guide useful, consider sharing it with friends and family via Facebook and Twitter.

About the Author:

Ariel Hochstadt

Ariel Hochstadt, Formerly Gmail Marketing Manager globally for Google, and today web entrepreneur. Ariel is a successful international speaker and author of 3 published books on computers and internet. He is the co-founder of vpnMentor and an advocate of online privacy.