# INTERNET SECURITY FOR KIDS

Prevent Your Kids From Getting Into Trouble and Danger On The World Wide Web

The web can be a dangerous place for children. Website owners are generally protected against censorship, in the US, at least, by their freedom of speech.

Preserving that freedom is important, but as parents, we don't want our kids visiting vulgar places on the web, or being exposed to pornography at an early age.

There are certain aspects of their personality that we would prefer remained innocent until they are old enough to know what the material is, it's purpose, and how things work in the adult world.

In general, if you wouldn't want them to see it at day-care, or at school, then they should be blocked from viewing it on the Web.

The biggest problem for most parents is that the kids know more about electronic devices than they do.

This means that even if you buy the latest router with child protections, you might need their help to set it up.

As a result, the first point of this article discusses that situation, and in general working with your kids so that they understand the rules of usage.

You may even enlist an older child to flag things for you that might be inappropriate for younger siblings.

Internet security might seem light a terrifying task to those who aren't very computer savvy, but have no fear.

In this article I'll show you what to look for, so that you will have a primer before you begin shopping security software and devices.

Some of the information doesn't involve electronics at all, but rather education about safe social media interactions, to keep from compromising the security of your household.

There are also some basic precautions that are self enforced, and everyone should know what they are and what the dangers are in not using them.

I'll go over them in this report, and leave it to you to discuss the importance with the young ones. Or you can let them read the report.

Any device, be it an Android tablet, an iPhone, a laptop, or whatever comes next, usually has software available that can protect young eyes from the content that is allowed to display on the device.

Some of this software is general, and blocks from a database of websites which you can modify over time.

Others go so far as to limit specific content from anywhere, such as social media posts and instant messages that may contain inappropriate information.

While this report doesn't cover the every program on the market, I'll give you a starting point to evaluate software features so that you can choose the right program for your family.

These days routers might be considered a dime a dozen, even though they usually cost upwards of fifty bucks.

When buying, most people focus on the range of Wi-Fi accessibility and the maximum speed that the router can stream online data.

We look how many devices it can support. But there's another feature that you should be looking for if you have youngsters in the house.

Some routers come with their own internal software which can both monitor and limit Internet usage.

I'll discuss some of these features and how they affect your family.

The process of Internet monitoring starts in the most usual of parenting places, with discussion.

Make your kids aware that there are scams everywhere, and anything they see while surfing the web isn't to be trusted.

People lie. They doctor pictures, and they put information out there that is blatantly wrong.

Help them to find sites and games that are age appropriate, and monitor the time they spend on the Internet, whether on their tablet, or phone, or whatever.

Make time slots during the day that they can use to research homework.

These times can be when you, another adult, or perhaps an older sibling is around to monitor their activity.

Make sure that they aren't looking at anything they shouldn't over their shoulder.

This obviously isn't going to work as well for older kids who want privacy, but for the younger ones, they might prefer spending time with you while surfing.

The easiest way to limit access is by removing the devices when they aren't to be used.

Make a point of knowing when they are using the Internet and what they are looking at.

One of the best ways to monitor the activity of older kids, both on the Internet and in real life, is to friend them on social media, and make sure that you are receiving any updates they post.

There's a new form of social media that seems to come out just about every month, so you may end up with a lot of accounts, but even if you aren't interested in using the site yourself, you should at least be there to see what your kids are doing in their public profile.

There are some basic rules that apply to all of us, whether it's a child who doesn't yet understand the dangers of the world around them, a teenager who is constantly trying to skirt the rules, or yourself.

A security mindset online is important now more than ever.

Daily, I see people making posts on social media telling everyone on their list where they are going to be and at what times.

You can "check in" with most devices if you are visiting a new place.

While these things can be a nice way to stay in contact, and alert your friends as to your whereabouts, they can also be dangerous.

If a thief is following you and your family on social media, you are broadcasting when you won't be home, letting them know your schedule, and your home's most vulnerable hours.

Does this mean that you shouldn't check in at all?

No. but you need to decide what is best for your family, and what kind of information should be shared.

Don't post pictures about your new safe and how you installed it.

Don't advertise when you will be leaving town for the weekend. Wait till you get back from vacation to post pictures.

When meeting anyone online, there's a potential security risk.

Social Engineers will get you talking for the sole purpose of figuring out the best way to scam or rob you.

Don't give out your address, your phone number, or the name of your kid's school.

This is probably the most important mindset topic to discuss with your children.

While meeting people online is "a thing" nowadays, there's no reason to let your guard down.

If you meet a stranger in real life, are you going to tell them where you live right away?

Sharing too much information with anonymous people over the web is dangerous.

Talk about things broadly, rather than giving specific information about your family.

With every request for information about you, ask yourself, "does this person need to know this?"

Use a nickname in chat rooms. The Internet is a place of anonymity, so keep your conversations secure by using a false name in public forums, chat rooms, or online games.

Don't use your full name in any forum where potentially anyone could see it, and just like social media, limit your personal information.

Your name rarely has anything to do with the discussion.

Some sites are going to request your personal information, but almost all of them give you the option of how much you would like to share publicly.

Check all the settings and filters before using the site, and if you can't figure it out, then contact customer support.

As your kids grow, Internet usage becomes more and more inescapable, and security online becomes more important than ever, restricting access by looking-over-the-shoulder becomes less of an option.

You need a better solution in this ever-evolving world of technological advances.

The simplest answer typically comes from new software.

The government is going to have a hard time regulating Internet content, to preserve our freedom of speech and expression, but companies understand that parents don't want their kids seeing everything out there, and they know that parents are willing to pay for extra protection, so there's a bunch of products on the market that do exactly that.

A website can only do so much. Many websites with adult material will have a pop-up when the user visits them, prompting you to enter your age.

While this provides a warning that the material therein is meant for adults, in the real world it does very little to actually restrict access.

Let's face it, without threatening your privacy by making you prove your age via credit card or social security number, there really isn't any way for a website to truly restrict access to their site.

The Internet is a very public place, and strikes a balance between privacy for you, and a website's ability to say and show what they want.

While the blocks are ineffective, the warnings are of use to certain tracking software that can recognize the phrase "adult content" and update their filters to restrict access.

The next step is software that you can install on your PC, your tablet, or the kid's phone that will limit their access to content.

These programs come in a number of different flavors. Some of them are simple database driven programs that stop your browser from pulling data from sites that are blacklisted.

Not only are these ineffective at staying up to date with new websites, they do very little to filter content from sites that are approved, and some of them are easy to bypass for a resourceful teenager.

Better software programs like "Net Nanny" cost money. These costs can be in the form of a license for each device, or a monthly charge.

While you might not like the idea of opening your wallet, it's important for the best software to keep up with new trends, develop better features, and give you full support and easy access.

Programmers aren't cheap to hire, so if you want the best you have to pay for it.

When looking for a piece of software, don't lazily purchase the first one that you see.

All of these programs have different features, different ease of use, and different update features.

If you aren't tech-savvy, then you should also read reviews about how good their customer service is, in case you have problems setting up the filters.

One feature you should look for is if you can setup Internet access and restrictions based on what time of day it is.

If you work from home, and the kids are at school all day, you might want a system that allows access to information during the day, which can be restricted at 2 or 3 o'clock.

As soon as the kids get home, the security features are back in place, without needing to change any settings.

Most applications that do this will also include a feature to turn off all access, so you can limit how late they stay up surfing.

Blacklists are a common feature on all monitoring software.
If you come across a site that your kid shouldn't be viewing, you can update the software to block the site.

Instead of depending on a blacklist, many programs now contain content filters.

The program will scan every site as it is accessed, looking for vulgar material and restricting the individual page.

Some software even comes with features that limit explicit social media posts from being seen.

If your kid has a favorite short story website, the software can block individual pieces of erotica without limiting more innocent stories.

There are even some that will scan any post your kid makes to social media, and alert you if they are swearing or putting up their own offensive content. They can even allow you to block the post.

Monitoring comes standard with most of the better software, giving you access to how much your kids are using the Internet, what kind of stuff they are looking at, and what they're up to.

Obviously you'll want to decide how much should be private for them, and how much you want to see.

There is a bazillion options out there when it comes to security software.

Discuss the options with other parents, do research on sites like PCMag.com, and discuss the features that will be applied with your kids.

Remember, if you are going to apply filters, then they need to be applied on everything with access.

That means phones, tablets, the family computer, laptops, etc.

If there are a lot of devices in your home, you will want to look for a plan that let's you get a bundle of licenses for a reduced rate.

Each license is typically only good for one device.

Routers these days offer the same kind of Internet protection as the software used on the devices themselves, but they block access for the entire network.

Network routers with these capabilities cost a little more, but if you want to keep the entire household safe from streaming unwanted content in a more overreaching way, they can be the best solution, especially after you add up the price of individual software for every phone and iPad.

They also guarantee that play dates won't be accessing vulgarity through your network.

Phones can connect to the Internet through the phone service, of course, so you won't be able to block all of the bad stuff by upgrading your network router, but at the very least, you can severely limit what your child is seeing, even when their friends are over.

Routers aren't going to have the same advanced features as device software, because the router is a different type of machine, but at the very least you should be able to keep age-inappropriate material off your home network.

The settings on a router can be a bit more tricky to access.

Some features to look for are the ability to allow content to certain devices through the MAC address (which is printed on the bar code label on the rear of your laptop), so you will be free to access all of the Internet, even if your kids can't.

The usage is redundant, however, as you can piggyback the new Wi-Fi on your old router.

Change the password so the kids can't get on the unrestricted Wi-Fi while having a monitored device just for them.

You can also use the monitoring software on the new router not only to see how much your kids are using the Internet, but frequent checking will let you know if the neighbors are stealing your Internet connection.

You should be able to see every device on the network at any time.

Routers don't have the same social media monitoring that software can have, but this might improve in the future.

If you are thinking about this general solution to putting a barrier between your kids and the biggest blacklisted sites, the Netgear Nighthawk is a good solution to check out.
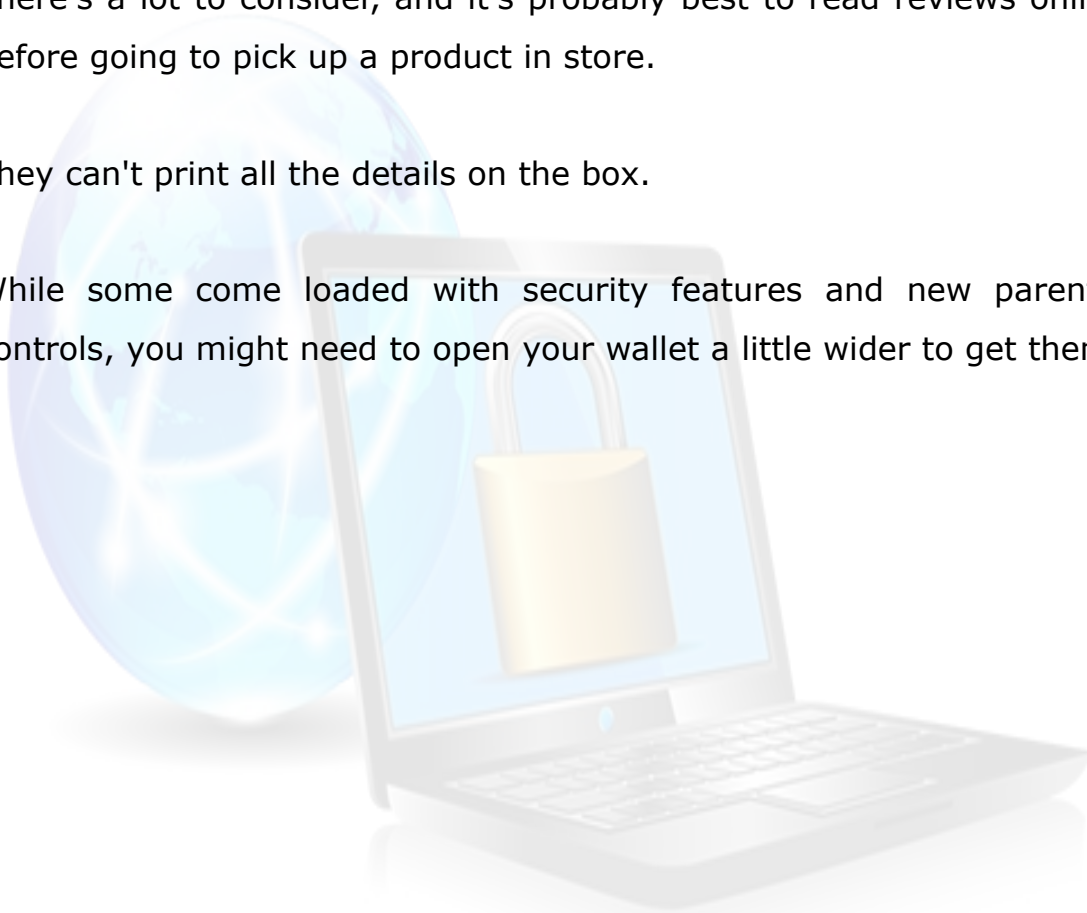
Remember, the next time you go shopping for a router, check out more than the speed and range of the Wi-Fi.

There's a lot to consider, and it's probably best to read reviews online before going to pick up a product in store.

They can't print all the details on the box.

While some come loaded with security features and new parental controls, you might need to open your wallet a little wider to get them.

There are numerous solutions to protect your kids from some of the obscenity that riddles the Internet, starting with education and discussion, and going as far as playing Big Brother to make sure that they are safe.

In general, the best solution is to apply everything in this report to some degree or another.

Weigh price against features when selecting device software.

Become educated about Internet safety, and educate your kids about the dangers of information sharing.

Play a role in their online life, whether through friending them on social media, or asking them about the kind of things they're doing on the net.

If you can't afford a fancy new router, ask your ISP about controls they might have in place to block content coming into your house.

With the speed that the technological world is moving, things are going to continue to change.

Restrictions are never going to be 100% foolproof, and being smart about what your share publicly will remain a requirement.

New technologies are going to emerge to make your monitoring and in-home protection against smut easier.

Stay current, be diligent, and protect those innocent eyes from things they shouldn't be looking at.

In the end it all comes down to you. I hope this report was helpful and informative.

The services listed are only examples, and there are hundreds of products out there to protect your family.

Do your homework.