How to Keep Your Kids Safe ONLINE

nachman NETWORKS

Networks Done Right

Our children are at risk, even when at home and when you're there.

Predators are on the lookout for children via the Internet. Here are some disturbing statistics:

✓ **1% of kids admit they've seen online porn.**

✓ **29% of parents let their kids use the Internet without any restrictions or supervision.**

✓ **25% of children get away with pretending to be older to get an account online.**

Teach Your Children About Online Threats.

✓ **Viruses, Malware and Ransomware:** I'm sure you've heard these terms before. Basically, they're malicious forms of software that can infect your computers, laptops, tablets and smartphones. All of your devices are at risk. Malware can lock down your computer and files for ransom payments, and rob you of your data and confidential personal information.

✓ **Internet and Email Scams:** It's hard enough to recognize these as an adult, but your children are more likely to be taken advantage of. A criminal posing as a government official may convince your child to click a link that's intended to cause harm.

✓ **Hackers:** People always think of hackers as guys in hoodies hiding in back rooms typing away on a keyboard. Today's hackers write codes that do the dirty work. The codes go in and parse your information, such as your email address, and other personal information. It then goes back to the hacker who pieces it together and uses it against you.

✓ **Inappropriate Sites:** These may not be malicious, but damaging in other ways. Do you really want your children to watch porn videos online, or people hurting others or animals? There are some really sick individuals out there. Don't let them into your child's life.

✓ **Oversharing:** Many kids believe the Internet is a safe place. It's not. There are criminals out there who want your children to share their own personal information—where they live, go to school, and more. Some pose as kids, when, in reality they're grownups. Teach your children not to share in this way.

✓ **Bullies and Trolls:** These can be kids from school, or just mean people online. They may be strangers or not. Internet Trolls are people who unleash their cynical, sarcastic and negative remarks on others, just because they can. This may make your child feel afraid, or even guilty because they blame themselves for these attacks.

✓ **Predators:** This is the scariest of them all. The anonymous feature of the Internet allows these individuals to lure your child to dangerous places.

Protect Your Devices from Viruses and Malware.

The first line of defense is having a good, strong password. Have a conversation with your child about appropriate, secure passwords. The more complex they are, the harder they will be to hack. Hackers have tools to break easy passwords. Consider using password managers, and installing them on your child's device. All your child needs to remember is one mega-password. The software will generate complex, secure passcodes each time they login to a site.

Install a Firewall. There two types: software and hardware. A software firewall is installed on your computer to moderate what can get into it. The hardware type is installed via your modem and router to make sure anything that comes into your network is scanned for malicious content.

Tech Tip!

Did you know that a password with six-characters, in lowercase letters, can be broken in under 6 minutes?

Install Antivirus Software. Make sure you install this on all of your devices, including your computer, laptop, tablet and smartphone. Many people believe their phone is protected, but it's not. Ensure you have the same antivirus software installed across all your devices so something doesn't come get in through the "back door."

Install Anti-Spyware Software. Spyware hides and works in the background of your computer devices, and collects personal information without you knowing it. A lot of antivirus software doesn't include spyware, so it's advisable that you also install anti-spyware on your computer devices.

Set Browser Security Settings to the Maximum. Your browsers have some protection installed. Take advantage of them, and, for your children's devices, it's advised that you set the security to maximum. This will avoid cookies that identify users, and utilize back-end tracking.

Tech Tip!

Depending on your child's age and computer knowledge, they may be able to go in and reverse the settings you make. So, it's always a good idea to check their devices periodically.

Avoid Being Victim to Online Scams.

1. Educate your kids on the types of fraud that exist—And that there are people who send out random email asking for things that they shouldn't.
2. Teach kids not to open emails that are in the spam or junk mail folder. Give them specific instructions on what not to do with emails.
3. Ask your children to let you know if they receive a suspicious email.
4. Advise them to be careful about clicking on web ads or banners. These are especially popular in some online games, and may take your children to other sites altogether. Train them not to click on these ads.

Protect Your Children from Hackers

The best way to do this is a good offense. Teach your children to:

1. Keep a login passcode enabled on all your devices. As mentioned, start with a good, strong password on all your devices. And, be sure to lock your devices when not in use—You can set their devices to automatically lock after a very short time.
2. Add two-step verification wherever you can. This is where a password is sent to you to ensure you authorize entry into a particular website, email or device.
3. Use diverse passwords for different accounts. This is where using a password management program comes in handy.
4. Beware of suspicious and phishing emails. If it doesn't "seem right" don't open it.
5. Be careful about what information your children share on social media sites. Once a hacker finds your child's identity, they can go online and find out much more.

Block Inappropriate Sites.

There are a number of good applications that you can get to block inappropriate websites. They can get very specific with settings you can choose. You can specify, "no adult sites," or "no gambling sites," and more. They are very intelligent, and can let you know if your child accessed inappropriate sites. Some good ones to check out include: **Net Nanny, Norton Family Parental Control, MoBicip, Qustodio, and Kaspersky Safe Kids.**

Protecting Kids from Very Bad Stuff

These sites will also let you know what your child is doing, what websites they go to. You can check their activity for the day, and more—And all of this is posted on an easy-to-use dashboard. You can also create flags, such as: "show me anything that has to do with sex," or when they go to shopping sites, etc.

Be sure to educate your child about the firewall and anti-virus protections you implement—And, if an alert comes up saying something has been detected, to stop doing what they were, and ask you to take charge of the computer device.

Manage Your Child's Digital Footprint.

Once you put information about yourself online in a public setting, you can't remove it—It's there forever. The same goes for your child. This becomes your child's digital footprint. It's important to have a conversation about this, and how sharing information about themselves online can be very dangerous. This can also impact them in the future when they go to get jobs.

Dealing with Cyberbullying

Cyberbullying is a real issue, whether it's from kids your children know, or strangers. It can be difficult to get your child to talk to you about this. You need to make sure he or she doesn't reply to any cyber bullying.

1. Try to encourage your child to talk to you about this.
2. Save the evidence if this happens—Saving screenshots are a good way to do this.
3. Depending on the circumstance, or if your child is feeling threatened, contact the school (if appropriate), or possibly the police.
4. Get educated on cyber bullying yourself.
5. Use software to block bullies' IDs, or anyone your child doesn't know.

Empower Kids to Make Safe Choices.

Make sure they know:

1. Not to post any personal information online. For example, don't let people know that your family is going on a vacation.
2. To think carefully before posting pictures or videos.
3. Not to accept friend requests from people they don't know.
4. To always tell you about strange friend requests or emails

Other Helpful Resources

If you don't understand what's going on, it's hard to have intelligent conversations with your kids about safety online. Here are some sites to help you get up to speed and stay informed:

Connect Safely: This is a Silicon Valley-based non-profit that's a great resource to help you educate your child, as well as worksheets to download as teaching tools.

Internet Safety 101: This non-profit sprung up from issues with child pornography. It helps you keep your child safe from predators, has warning signs to look for, and more.

SafeKids.Com: The man who runs this was at the center of missing and exploited children. It contains lots of good tips and conversations to have with your kids about staying safe online.

Get Cyber Safe: This is a Canadian site that started as a national awareness campaign for families to be safe online.

For more information about helping your children stay safe online, contact Nachman Networks at (703)600-3301 or sales@nachnet.com.