Kids Internet Safety Guide

What to do to keep your kiddos safe online.

It's nearly impossible to keep kids off the internet these days. From homework assignments to FaceTIme with Grandma, the internet is a fact of life.

Unfortunately, it's not all academia and family connections—the internet can be a risky place, especially for children. But you don't have to go it alone. SafeWise has identified the top online threats to kids and tips for keeping kids safe.

The Top Online Threats for Kids

There are a number of potential dangers in cyberspace, but these are the top three threats that all kids face.

1. Cyberbullying: Almost 34% of kids aged 12–17 have been cyberbullied at some point in their life, and 11.5% have bullied someone else online. Cyberbullying is any aggressive, threatening, or mean-spirited activity conducted via electronic communication (email, social media posts, text messages, etc.). Girls are more likely to be the victims of cyberbullying and more boys admit to bullying others online.[1]

2. Online predators: Adults who use the internet to entice children for sexual or other types of abusive exploitation are considered online predators. Child victims can be as young as one or as old as 17. When it comes to online enticement, girls make up the majority (78%) of child victims—while the majority (82%) of online predators are male. And 98% of online predators have never met their child targets in real life.[2]

3. Exposure to inappropriate content: Inappropriate content is one of the most common online threats that kids encounter. Everything from vulgar language and hate speech to graphically violent or sexual images can have a harmful effect on an impressionable child. Over 55% of tweens (kids aged 10–12) have been exposed to violent content on the internet, and nearly 60% have come across sexually explicit words or images.[3]

NOTE: For the purposes of this guide, we're focusing on the earliest prevention possible. While these online safety tips and best practices can be applicable to anyone, we've selected steps to help protect kids from ages five through 12.

> Parents need to have transparent discussions around the vectors of cyber security, privacy, and safety issues with their children.
>
> **Dennis Chow**
> *CISO, SCIS Security*

How to **Protect your Kids From Cyberbullying**

1. Know the risks - Understand what cyberbullying is, where and how it happens, and how to spot it. Explain that online bullies can act friendly at first, but also encourage your child to be on the lookout for any interactions that make them feel bad, scared, or sad.

2. Talk about it - Have ongoing discussions with your child. Talk about what cyberbullying is and what types of communication are acceptable and unacceptable. Make sure your child knows that it's safe for them to talk to you if something makes them uncomfortable.

3. Keep a watchful eye - Place the computer in a common room and monitor all screen time. Use a shared email account, and if you let kids interact on social media, make sure you have full access to manage their accounts. Parental control software is another great way to stay in the know.

4. Set boundaries - Put time limits on screen time. Include all online activities—from homework to playing games and surfing the web. Restrict social media access and email accounts, and set rules for any IM, texting, etc. Let your kids know you'll be checking in regularly.

5. Build a network (IRL) - They don't say it takes a village for nothing. The more people you have looking out for your kid online, the more likely you are to keep them safe. Know your kids' friends and their parents. Enlist support from school, sports, and church leaders.

6. Be prepared to respond - Don't wait until the heat of the moment to come up with your gameplan. In case your kid does get bullied online, learn what the proper responses are so you can keep your emotions in check and help your child deal with what they're going through.

Steps to Take if Your Child **Has Been Bullied**

Pay attention. Look for signs of cyberbullying, like spending more time online or texting, hiding the screen from others, emotional responses to online interactions, and sadness or seclusion.

Ask questions. Gently ask your child what's going on and how they feel about it. Find out if they've responded to the bully, and what that response was.

Acknowledge their feelings. Your child may feel frightened, angry, sad, or even betrayed if the bully is someone they trusted. Let them know it's okay to feel whatever they are feeling.

Block the bully. Immediately block (or "unfriend") the abuser. Use tools like site blockers and privacy settings as extra layers of protection.

Report it. Alert website and email administrators to the bully. Most social media platforms offer options to report a user or flag dangerous posts. If appropriate, report the abusive activity to school or law enforcement officials.

Assess the damage. If your child's emotional response is extreme and protective measures don't seem to help, seek the help of a professional.

Enlist reinforcements. Talk to other adults who can help protect your child (other parents, teachers, school administrators, coaches, etc.) and bolster your child's positive friendships.

What to Do if Your Child **Is the Bully**

Look. If your child sets up new email or social media accounts without your knowledge, makes snarky remarks while online, or starts to hide their online activity, they could be picking on someone.

Listen. If you're concerned, gently broach the topic with your child, and then allow them the room to answer. Be open-minded and don't blame. Bullies are usually in some kind of pain as well.

Monitor. Double your efforts to track your child's online activity. If you're not already using parental control software, now is the time to add this tool to your efforts.

Support. Encourage your child to deal with their feelings and the reasons they are engaging in this behavior. Suggest that they apologize to the kids they've hurt, and help them do it.

Get help. It can be hard to identify why your child starting acting out in this manner. Seek professional help, and if the bullying crosses lines at school (or legally), inform the appropriate authorities and ask for resources to address the situation.

> It is a good idea to join their children's online social network so that the interactions can be monitored and actions can be taken if the children become targets or victims of cyberbullying. Parents can monitor the security settings on their children's social media accounts. On Facebook, parents can help their children choose various settings such as: 'Who can contact me?' 'Who can look me up?' 'Who can see my stuff?

Dr. Nir Kshetri
Professor & Cybersecurity Expert
at University of North Carolina-Greensboro

How to **Protect your Kids From Online Predators**

1. Understand the danger - Learn what online predators are, where and how predators attack, and how to spot it. Explain that contact from strangers is never okay.

2. Guide online behaviors - Talk about what types of online interactions are okay and what aren't. Discuss how to recognize signs of trouble and how to ask for help.

3. Rein in digital cameras - Control access to digital cameras and photo apps on every device. Make sure your kids can't upload or download photos without your permission.

4. Monitor online activity - Keep the computer in a common room, set limits on screen time, use a shared email account, and put parental controls (like filters and apps) in place.

5. Keep kids out of dangerous places - Talk about the risks of chat rooms and social networks, and set up rules and time limits if you allow your kids to use them. Always follow age restrictions for websites and apps.

6. Don't let your guard down - Know that "safe" places still require vigilance. There are kid-focused chat rooms and games where predators may pose as children.

Steps to Take if Your Child **Has Been Targeted Online**

- Let your child know that it's not their fault.
- Cut off communication with the predator.
- Change online credentials, including screen names, usernames, and passwords.
- Save screenshots or copies of messages and images from the predator.
- Report the activity to website administrators and law enforcement.
- Seek professional help for your child, as appropriate.

Safety Tips for Kids

- Never share personal information online.
- Don't respond to emails, texts, or messages from strangers.
- Don't post or share photos online.
- Don't click links, open attachments, or accept gifts from someone you don't know.
- Don't open links or attachments from strangers.
- Never agree to meet someone you met online.
- Let your parents or other trusted adult know if you need help.

> This is nothing more than a sophisticated form of “stranger danger.” Talk about these subjects (sexting, sextortion, online sexual predators, cyberbullying) and become comfortable talking to your kids about them. If you are not getting into your child’s business, then you are doing them a disservice.
>
> **Scott Pietrzak**
> *Owner, Online Safety Specialists*

How to **Protect your Kids From Inappropriate Online Content**

1. Teach kids how to navigate the internet - Talk about proper online etiquette, how to enter safe search terms, how to identify a secure website (https), and when to ask an adult for help.

2. Let kids know what to watch for - Teach them that bad stuff can come from many sources, including email and direct messages. Talk about pop-up ads and when and where it’s okay to click on something.

3. Explain email safety - Make sure kids know not to click on things or open attachments in emails, and not to respond to messages from people they don’t know. Have them contact an adult before they download anything.

4. Set up firewalls and content blockers - Use the built-in safety applications that come on your devices and add more to be extra-safe. Block all websites that aren’t rated safe for children. Use a content filter or firewall that is designed to protect children from harmful content.

5. Be Prepared - Have a plan in place in case your is exposed to graphic content online. Know what the proper responses are so you can focus on helping your child deal with their feelings.

Steps to Take if Your Child **Has Been Exposed to Inappropriate Content**

Don’t	Do
• Freak out.	• Stay calm.
• React emotionally.	• Be patient.
• Shame your child.	• Find the source of the content.
• Scare your child.	• Block access to dangerous or confusing sites.
• Blame your child.	• Help your child sort out their feelings.
	• Restore a sense of safety.
	• Keep the conversation going.

> It's not going to be easy. Protecting a child from such threats means understanding those threats. As parents, we're fighting on unfamiliar turf. Forget the difficulties in embracing new tech, try finding the time to use and explore a new service after a busy day/week/month of work and parenting.
>
> **Allan Buxton**
> *Director of Forensics, SecureForensics*

How Much Is Your State Doing to **Keep Kids Safe Online?**

To grade each state, SafeWise looked at laws for both sexting and cyberbullying. Points were assigned to states based on the types of laws currently on the books and the consequences for violating those laws. If a state has a law proposed, partial points were granted. School policies and consequences were also factors. Letter grades were determined based on the total points, with higher points earning higher grades.

State-by-State Online Safety Laws

State	Letter Grade	Laws Address Cyberbullying or Online Harassment	Legal Consequences for Online Harassment	Schools Discipline Cyberbullying	Includes Discipline for Off-Campus Offenses	Laws Address Sexting	Misdemeanor Penalties for Sexting	Felony Penalties for Sexting
Alabama	C	YES	YES	NO	NO	NO	NO	YES
Alaska	C	NO	YES	YES	NO	NO	YES	NO
Arizona	B	YES	YES	YES	NO	YES	YES	NO
Arkansas	A	YES	YES	YES	YES	YES	YES	NO
California	B	YES	YES	YES	YES	proposed	NO	NO
Colorado	B	YES	YES	YES	NO	YES	YES	NO
Connecticut	A	YES	YES	YES	YES	YES	YES	NO
Delaware	C	YES	YES	YES	NO	NO	NO	NO
Florida	A	YES	YES	YES	YES	YES	YES	YES
Georgia	A	YES	YES	YES	proposed	YES	YES	YES
Hawaii	B	YES	YES	YES	NO	YES	YES	NO
Idaho	C	YES	YES	YES	NO	NO	NO	NO
Illinois	B	YES	YES	YES	YES	YES	NO	NO
Indiana	B	YES	YES	YES	NO	YES	YES	NO

Iowa	C	YES	YES	YES	NO	NO	NO	NO
Kansas	A	YES	YES	YES	NO	YES	YES	YES
Kentucky	C	YES	YES	YES	NO	NO	NO	NO
Louisiana	B	YES	YES	YES	YES	YES	NO	NO
Maine	D	YES	NO	YES	NO	NO	NO	NO
Maryland	C	YES	YES	YES	NO	NO	NO	NO
Massachusetts	B	YES	YES	YES	YES	proposed	NO	NO
Michigan	C	YES	YES	NO	YES	NO	NO	NO
Minnesota	C	YES	NO	YES	YES	NO	NO	NO
Mississippi	C	YES	YES	YES	NO	NO	NO	NO
Missouri	C	YES	YES	YES	NO	NO	NO	NO
Montana	D	YES	YES	NO	NO	NO	NO	NO
Nebraska	B	YES	NO	YES	proposed	YES	NO	YES
Nevada	C	YES	YES	NO	NO	YES	YES	NO
New Hampshire	D	YES	NO	NO	YES	NO	NO	NO
New Jersey	B	YES	YES	YES	YES	YES	NO	NO
New Mexico	C	YES	NO	YES	NO	YES	NO	NO
New York	B	YES	YES	YES	YES	YES	NO	NO
North Carolina	C	YES	YES	YES	NO	NO	NO	NO
North Dakota	B	YES	YES	YES	NO	YES	YES	NO
Ohio	C	YES	YES	YES	NO	NO	NO	NO
Oklahoma	B	YES	YES	YES	NO	YES	YES	NO
Oregon	C	YES	YES	YES	NO	NO	NO	NO
Pennsylvania	A	YES	YES	YES	YES	YES	YES	NO
Rhode Island	C	YES	YES	YES	NO	YES	NO	NO
South Carolina	C	YES	YES	YES	NO	proposed	NO	NO
South Dakota	A	YES	YES	YES	YES	YES	YES	NO
Tennessee	C	YES	YES	YES	YES	NO	NO	NO
Texas	A	YES	YES	YES	YES	YES	YES	NO
Utah	A	YES	YES	YES	NO	YES	YES	YES
Vermont	B	YES	YES	YES	YES	YES	NO	NO
Virginia	C	YES	YES	YES	NO	NO	NO	NO
Washington	C	YES	YES	YES	NO	NO	NO	NO
West Virginia	C	YES	YES	YES	NO	YES	NO	NO
Wisconsin	D	NO	YES	YES	NO	NO	NO	NO
Wyoming	D	YES	NO	YES	NO	NO	NO	NO

Sources:

1. Cyberbullying Research Center, “2016 Cyberbullying Data”
2. National Center for Missing and Exploited Children, “The Online Enticement of Children: An In-Depth Analysis of CyberTipline Reports”
3. Bark, “2018 Children and Teen Cyber Fact Sheet”
4. Cyberbullying Research Center, “State Sexting Laws”; Cyberbullying Research Center, “State Cyberbullying Laws”