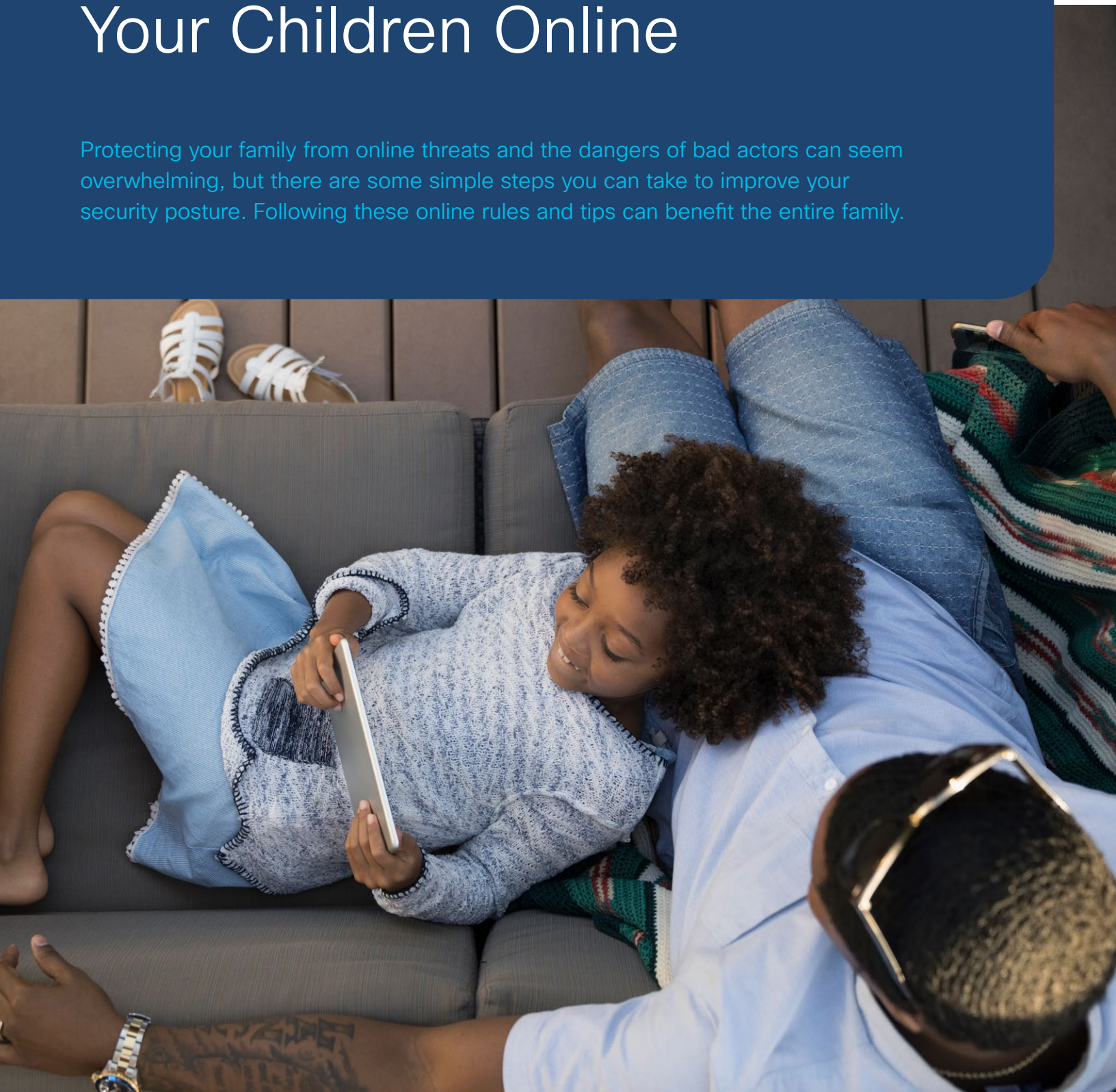
Simple Steps to Protect Your Children Online

Protecting your family from online threats and the dangers of bad actors can seem overwhelming, but there are some simple steps you can take to improve your security posture. Following these online rules and tips can benefit the entire family.



You play a critical role in protecting your children online

It's not enough to rely on technological controls to do this for you: kids need cyber-training and support as they develop. For example, you wouldn't dream of letting a six-year-old child go shopping alone in the local mall in the evening, so apply the same reasoning to online access. Use real-life physical comparisons like this one as a way of sanity-checking possible online risks.

Here's another example. When your child comes home from school you might ask about his or her day. What did they do? If this same child has been using a tablet to access the internet for two hours, would you ask similar questions? Show the same interest.

Continuing with this hypothetical scenario, if your child came home from school and was very quiet, or not their usual self, would you try to find out why? Be observant of unusual behavior.

What you should know about social media

Risks

- Cyberbullying
- No privacy protection
- Sharing of information with bad actors
- Loss of ownership of your photos, videos etc.
- Identity theft
- Seeing offensive images or messages
- Meeting bad actors in real life whom they've met online

One in three young people in 30 countries said they have been a victim of online bullying, with one in five reporting having skipped school due to cyberbullying and violence[1].

[1] *'UNICEF poll: More than a third of young people report... online bullying' September 3, 2019*
'Behind the Numbers: Ending School Violence and Bullying.' Accessed September 1, 2021.

Best practices

- Only talk to people you know in real life
- Guard your passwords and don't share them with anyone
- Do not download files from strangers or unknown sources. A bad download could lead to viruses and/or malware.
- Be aware that people are not always who they claim to be on the internet
- Memorize this "rule of three":
    1) Never post any personal information online such as phone numbers, addresses, school names, etc.
    2) Never post inappropriate photos online, even if you think the communication is private
    3) Never arrange in-person meetings with someone you meet online, unless your parents have confirmed the person's identity in advance
- Remember, once you put something on the internet, it is there forever. If you wouldn't put the information on a sign outside your house, then don't share it on the internet. And if you wouldn't show your grandparents, then you probably shouldn't be sharing with everyone on the internet.
- Do not build relationships with strangers online
- Do not click on suspicious links from unknown people or websites
- Understand that influencers are marketers
    - Many pay for their likes, and are paid by corporations to market to your children and teens

Resources

Healthy Screen Time and Children

Family Screen Time Contract

Cyberbullying: What is it and how to stop it

Social Media, Apps, and Sites Commonly Used by Children and Teens

Cyberbullying

It's happening more than you know

Signs your child might be a victim of cyberbullying

Noticeable increase or decrease in device use, including texting.

A child exhibits emotional responses (laughter, anger, upset) to what is happening on their device.

A child starts to avoid social situations, even those that were enjoyed in the past.

A child becomes withdrawn, depressed, or loses interest in people and activities.

A child hides their screen or device when others are near, and/or avoids discussion about what they are doing on their device.

A child shuts down social media accounts or opens new ones.

Tactics a child might use to cyberbully others

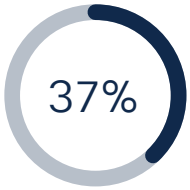
Posting comments or rumors online about someone online that are mean, hurtful, or embarrassing.

Threatening to hurt someone or telling them to kill themselves.

Pretending to be someone else online in order to solicit or post personal or false information about someone else.

Creating a mean or hurtful webpage about someone.

"Doxing," an abbreviated form of the word "documents", is a form of online harassment used to exact revenge and to threaten and destroy the privacy of individuals by making their personal information/documents public, including addresses, Social Security, credit card and phone numbers, links to social media accounts, and other private data.



37% of young people between the ages of 12 and 17 have been bullied online. [2]

60% of young people have witnessed online bullying. Most do not intervene. [3]

3% of young people admit to bullying others in the last 12 months.[4]

Parents might not see the signs of cyberbullying, but many of the warning signs occur around their kids' devices.

---

[2] *DoSomething.org. Patchin, Ph.D, Justin. "2019 Cyberbullying Data." Accessed September 1, 2021*

[3] *Safety Net: Cyberbullying's impact on young people's mental health Inquiry report childrenssociety.org.uk / youngminds.org.uk Accessed September 1, 2021*

[4] *Ditch the Label.'The Annual Bullying Survey 2020.' Accessed September 1, 2021.*

Cyberbullying and online gaming

Risks

Not everyone will be nice
Some gamers might say nasty things or try to bully and upset other players. This can be done by people you know or strangers.

Not everyone will admit their real age, gender or intentions
Individuals with malicious intent often, deliberately pose as being a different age/ gender (fake identity) to build relationships with the person they are pursuing This happens for many reasons i.e. to gain the other person trust; or possibly to take advantage of their target.

Some people might use games to try and groom children
Grooming is when someone tries to build a relationship or friendship with a young person to trick or pressure them into doing something sexual or otherwise inappropriate.

Some games might have upsetting content
This might include violence, horror, or sex and can be more life-like if you play virtual reality games.

Best practices

Get involved
Play the game with your child or observe when the gaming happens to understand how it works and what your child is exposed to in the game.

Be a nosy parent
Check in periodically with your child about whom they are playing online games with.

Explain cyber-stranger danger
Teach your children about safe online behavior, including not clicking on links from strangers, not sharing personal information, not participating in bullying behavior of other players, and what to do if they observe or experience bullying.

Set boundaries
Establish rules about how much time a child can spend playing video games.

Check game ratings
These inform you whether a game is suitable for younger age groups.

Resources

unicef.org - 10 things teens want to know about cyberbullying.

staysafeonline.org - What to do if my child is being cyberbullied

stopbullying.gov - How to report cyberbullying

The dangers of sexting

Sexting is the sending of sexually explicit digital images, videos, text messages, or emails, usually by cell phone. Research finds at least 1 in 7 teens are sexting[5]. Although most of teenagers don't report sexting, 15 percent of teens say they send sexts and 27 percent receive them[6]. When discussing this subject, you should remember that children can "normalize" some of this behavior, and responsible adults must be on guard to explain that this behavior is not normal and can never be removed from the internet. For instance, an 11-year-old girl tells her friend that a boy has sent her an unsolicited nude selfie, but her friend replies "don't worry he does that to all new girls, its fine". They have normalized the behavior, but it is **NOT** okay, and we need to ensure they know this. For more in-depth information on sexting, visit a newly release report Look At Me, Teens, sexting and risks from the United Kingdom[7].

Risks

Sexting between an adult and a minor constitutes child pornography and is a felony.

Sexting can lead to sexual bullying.

Sexting can open the door to sexual predators.

Sexting puts teens at risk for blackmail.

Sexts never go away.

Exposure to sexting can ruin a person's reputation.

Not everyone in real-life is who they portray themselves online.

Sexting can lead to emotional stress - If images fall into the wrong hands, the victim's mental health can be compromised which can lead to depression, isolation, eating disorders and possible worse consequences such as suicide.

---

[5] *cbsnews.com '1 in 7 Teens Are Sexting, New Research Finds.' Accessed September, 2021.*
[6] *Time.com 'Teen Sexting Has Become Even More Common, Research Says.' Accessed September 1, 2021.*
[7] *internetmatters.org 'Look at Me - Teens, Sexting and Risks Report.' Accessed August 30, 2021.*
Patchin, Justin W. 'Current Efforts to Curtail Teen Sexting Not Working.' Cyberbullying Research Center (blog), July 14, 2020.

Best practices

Give your children or teen an out
Children are often peer pressured into sending explicit images online. Help them come up with a strong explanation to tell their friends why they don't want to send explicit images. Example: Many employers research potential candidates online and finding unwanted information or content could jeopardize the candidate's chances of obtaining the position.

Share with your children what to do if they receive an explicit text

1) Don't forward it to anyone
2) Delete the image
3) Report the image (if online) so it can be removed
4) Tell the person not to send images anymore
5) Block their number or account
6) Make a report to your mobile phone company if the images don't stop

Discuss online risks
Be open and talk to your children about why security awareness is so important. Having discussions about what they view online each time they access the internet builds a routine to help emphasize safety measures and builds trust with your children.

Remind children that no message is truly private
Make sure your kids understand that messages or pictures they send over the internet or on their cell phones are not truly private or anonymous. Make sure they know anyone can—and often will—forward their pictures or messages to others. Ask your child what their boyfriend or girlfriend will do with those pictures if they break up.

Get to know you children's friends
Know who your children are communicating with online and on their cell phones. Do your best to learn who your kids are spending time with online and on the phone by checking their messaging buddy lists, social networking friends, and mobile device address/contact lists.

Teach your child to unplug occasionally
Consider placing limits on electronic communication. Check out the parental controls offered by your mobile provider. Many mobile carriers offer family plans that allow you to limit the amount and types of text messages your kids can send. Disable attachments on text messages.

Set expectations
Make sure you are clear with your children about what you consider appropriate online and texting behavior.

Resources

Internet Matters. 'Look at Me – Teens, Sexting and Risks Report.' United Kingdom

Tips for Dealing with Teen Sexting

[8] *Patchin, Justin W. 'Current Efforts to Curtail Teen Sexting Not Working.' Cyberbullying Research Center (blog). July 14, 2020.*

What can you do?

1) **Educate yourself**
   It can be hard to tell your child what to look out for if you're not completely sure yourself. Online threats change all the time, so it pays to follow the news and stay alert to the newest dangers.
2) **Get involved and stay involved**
   Keep your computer in an open area so you can monitor computer activity. Take an interest in where your children are going on the internet.
3) **Establish your own rules**
   Establish clear boundaries with your children about what is and isn't acceptable when they are online. Draft an age-appropriate online contract so your child knows and agrees to the rules. Install and use parental controls to help enforce these rules.
4) **Keep lines of communication open**
   Have local house rules but plan how you will react to various possible scenarios. Your child might be upset or confused by what has happened, they might feel it's their fault. Be prepared to handle questions and try not to over-react.
5) **Teach kids that the internet is forever**
   Once the information is out there, whether it is comments, photos, or video, it is there forever. And as the parent or caregiver, remember that you should not overshare information and details of your children! A lot of material has been innocently uploaded by proud parents, without thinking of the 'internet is forever' concept.
6) **Keep your child's privacy private**
   If you are sharing pictures of your children online with family and friends on Facebook or another social media platform you are sharing it with the world. Once their pictures are out there, they are out there for everyone to share.
7) **Be mindful of your circle of friends and family**
   Many times we are told about the stranger dangers in the world, but we need to be mindful that trusted individuals can unfortunately be a harmful source. Be aware of who is befriending your child and teen online.

Learn more about keeping your family safe online

- Staysafeonline.com
- Download tip sheets, lesson plans and other safety resources
- Cyberbullying, sexting, social networking, and more
- U.S. Federal Trade Commission's main resource to educate consumers on staying safe and secure online

Cybersecurity and Infrastructure Security Agency (CISA)

Concerned Parent's Internet Safety Toolbox

Identity Theft Resources

National Do Not Call List – Action: Register your phones

Local Victim Service Provider – Most communities in the United States have victim advocates ready to help following a crime. Find local victims service providers here.

Global Resources:

Children Helpline International

EMEAR NSPCC

EMEAR Secure Internet Centre (SIC)

APJC Go safe online

Homeland Security

UNICIF East Asia – Child Protection in the digital age

UNICEF - End Violence online