ENJOY SAFER TECHNOLOGY™

saferkidsonline

A safer internet for children— a parents' guide

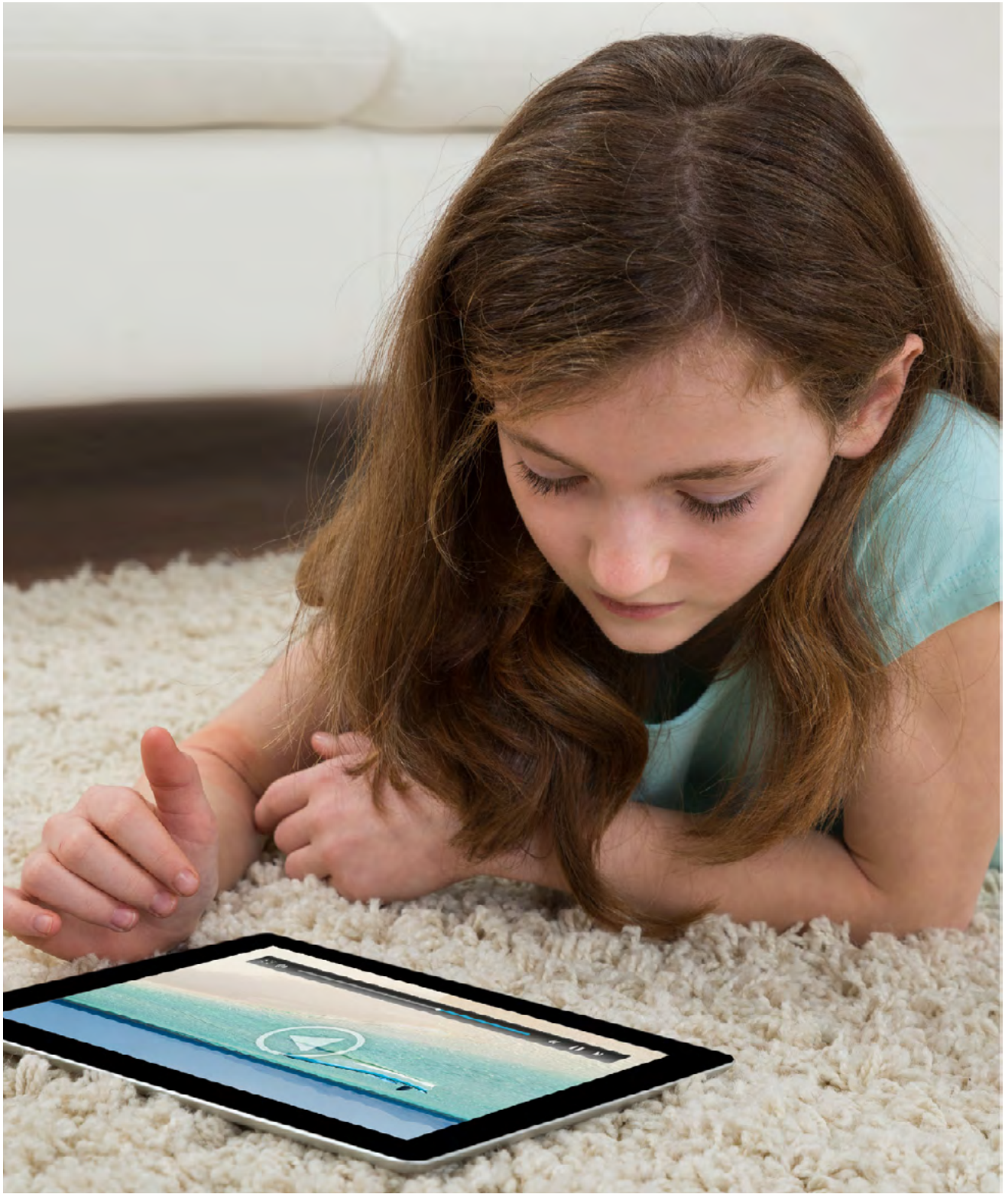
saferkidsonline

Digital lives

Many of us at ESET are parents like you.

So we understand the desire to keep our children safe online. But with increasingly complex mobile devices and new communication platforms emerging, there's a lot for adults to learn about and keep up with.

This guide provides practical advice on how, when and why to help your kids safely enjoy the internet and all it has to offer.



Who should talk to kids about security?

It needs to be you. Here's why:

Your children have lots of people who play very important roles in their lives, such as relatives, friends and teachers. However, children tend to look to their parents for answers, so make it clear that you're there to provide guidance and advice.

When should you talk to them?

Now!

From the first moment a kid shows an interest in your tablet, smartphone or computer, you should start explaining things. Keep in mind that just as kids need rules to stay safe in the real world, they also need guidance for the online universe. While the immediate threats to personal safety might come in a different form, the potential for harm is just as real.

As your child grows up, new online challenges will come their way. Your guidance will help your offspring make smart decisions.

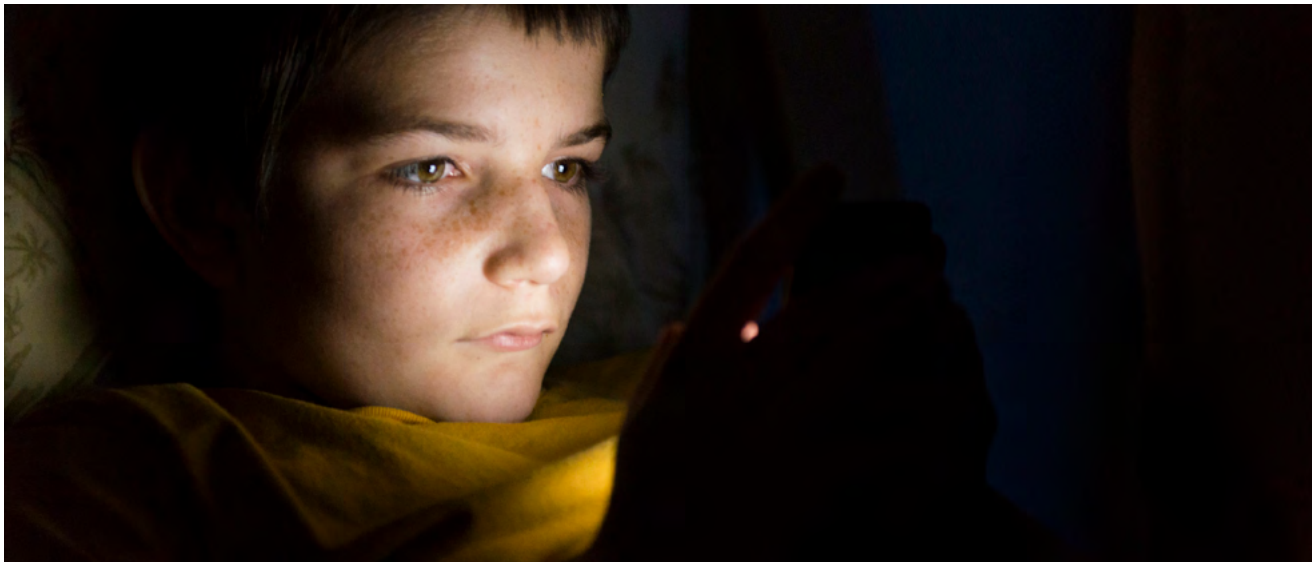
Education—a two-way street

Does it feel like your children know more about computer technology than you do? You're not alone.

Kids these days are digital natives who are adept at using new technology. However, knowing how to access the internet is not the same as using it safely.

As a parent, you don't have to be aware of everything happening in the virtual world. But you do need to be ready when your kids encounter something unfamiliar or aren't sure how to handle an email or social media situation. Listening to them is just as important as providing advice.

The most important thing is to make your child part of the conversation. Strive to create an environment where they can ask you questions freely.



What should you do when your child starts going online?

For starters, use parental control tools

Take advantage of technology with ESET Parental Control tools, which make it possible to block sites or categories of pages that contain potentially offensive material. You can filter content by your child's age, as well. Parental controls can be used to set time limits for internet surfing or game play—something you should discuss with your child so they understand the reasoning behind those limits.

ESET's parental control solution also has a feature allowing children to request access to certain sites or pages, or to ask for extra time online. Again, this is a great time to discuss why you might maintain or relax certain limits.

In addition to this technology, here's some practical advice for different age groups that will make children's online activities safer:

Up to 10 years old

1. Accompany them during their first digital journeys

Make it a priority to be present when your little ones take their first steps into the digital world. The first contact a child has with the internet is a good opportunity to sit down and guide them in their new adventure. It's also a chance to point out things like game add-ons that might require a purchase and should be authorized by you in advance.

2. Set conditions for internet usage

Set basic rules for using the internet, including parameters for games, socializing or movies. A good practice is to supervise the number of hours spent online and set times during which web access is allowed.

3. Set a good example

Children tend to follow their parents' behaviors. If you demonstrate how to safely browse and interact with others online, the kids are likely to follow suit.

11 to 14 years old

1. Teach them not to share information that might identify them

It's vital to teach kids that in the virtual world, not everyone is a friend—and not everyone is who they claim to be. Explain why it isn't safe to share information online such as your address, phone number, school details or daily schedule.

Have your child check with you before sharing potentially sensitive photos. Kids need to understand that once they've shared something online, it's going to stay there.

2. Keep dialog open

Encourage your kids to be open with you and ask freely about what they see on the internet. Try to handle questions about "fake news" or doctored photos by talking about using reliable websites to find information.

15 to 18 years old

1. No one else should know their passwords

We know that teenagers have minds of their own, but make sure they understand and exercise best practices when it comes to passwords. Emphasize that they should never share their passwords with strangers. Explain why passwords shouldn't even be shared with friends, as they can easily fall into the wrong hands and allow access to social media accounts or banking information.

2. Immediately report stalking and cyberbullying

Remember the school bully? Nowadays, many bullies have moved to modern technology and are hiding behind the anonymity of the internet. What hasn't changed is the fact that they try to psychologically (or even physically) harm others. Teens should be encouraged to inform their parents or other responsible adults and save any emails, posts or photos related to bullying or unwanted attention online.

3. Online financial transactions need to be secure

Purchasing items online can be perfectly safe—as long as security precautions are in place. Until kids understand the safety measures necessary when providing personal financial information, they should do so only under parental supervision.

What are the main threats online?

Malware

Malware (malicious software) is designed to damage or lock your device, steal your data or spread to other networks. Various types of malware can encrypt your files and hold them for ransom; attempt to access your financial information; spy on your activities via your webcam; and much more.

In addition to using a reliable internet security solution, educate children about the internet threats listed below and how to avoid them. One great resource for both kids and adults is the National Cyber Security Alliance.

Spam

You've seen spam before, in the form of all those unsolicited junk emails that appear in your inbox. They should be deleted without opening them. Remind your kids that these unwanted messages often try to lure you to websites or ads designed to spread malware by claiming that you've won a contest or offering "free" products.

Scams

Internet scams can take many forms, such as spam and the use of social engineering techniques. In the latter, the scammer may masquerade as a schoolmate or official to attempt to collect confidential information such as social security numbers, usernames and passwords. Emails or texts requesting social network usernames and passwords are other common scams.

Cyberbullying

This hostile behavior is usually aimed at children and teens, although adults can also be victims. The target is threatened and humiliated by their peers, or even strangers, in cyberspace. This can cause extreme emotional trauma or even drive victims to harm themselves.

Cyberbullying has many routes; even chat functions within console games can be used. Emphasize to children of all ages that any kind of harassment or bullying is unacceptable and should be reported to you immediately.

In addition, if your child is a victim of cyberbullying they should not retaliate. Explain that the stalker wants to provoke a reaction as it feeds their desire to harm others. If online attacks continue, notify the appropriate authorities—school officials or law enforcement. Don't erase any message received, as it could be used as evidence.

Grooming

Grooming occurs when an adult tries to persuade a kid to perform sexual activities either online or in person. A groomer attempts to create an environment of trust and build an emotional connection with the child, perhaps by "friending" them on social media. Often, an adult will pretend to be another child in order to establish a friendship, then try to arrange a meeting in person.

In addition to keeping track of who your kids spend time with online, remind them never to meet anyone they've met online unless a parent is present.

Sexting

"Sexting" (from "sex" and "texting") has been around for years.

While it originated with the SMS function for texts on mobile phones, now sexually explicit photos and videos can easily be sent as well. Remind your kids that once they've shared such material online, it can spread unchecked. Photos can be used for blackmail, cyberbullying and much more. A good rule of thumb is not to share anything you wouldn't want posted for the world to see.

Data and identity theft

Information sent via the web without the necessary precautions (such as data encryption or using a secure website) can be intercepted by third parties. In the case of account numbers, banking information, social security numbers, etc., the info may then be used for accessing bank accounts or stealing someone's identity. Be sure your children know that reputable organizations won't request their account data or banking PIN numbers via email or chat.

Stay up-to-date

Obviously, denying your child access to online technologies is not an option. Digital devices are part of their everyday lives, and are increasingly important for their development. Help your children use them safely and take part in the interaction between the child and the device.

It's also worth noting that many of the risks above can affect adults, and that internet safety rules apply to users of all ages.

For more information, visit our websites and social network pages:

www.eset.com

www.welivesecurity.com

Become a Fan www.facebook.com/eset

Follow us at https://twitter.com/ESET @ESET