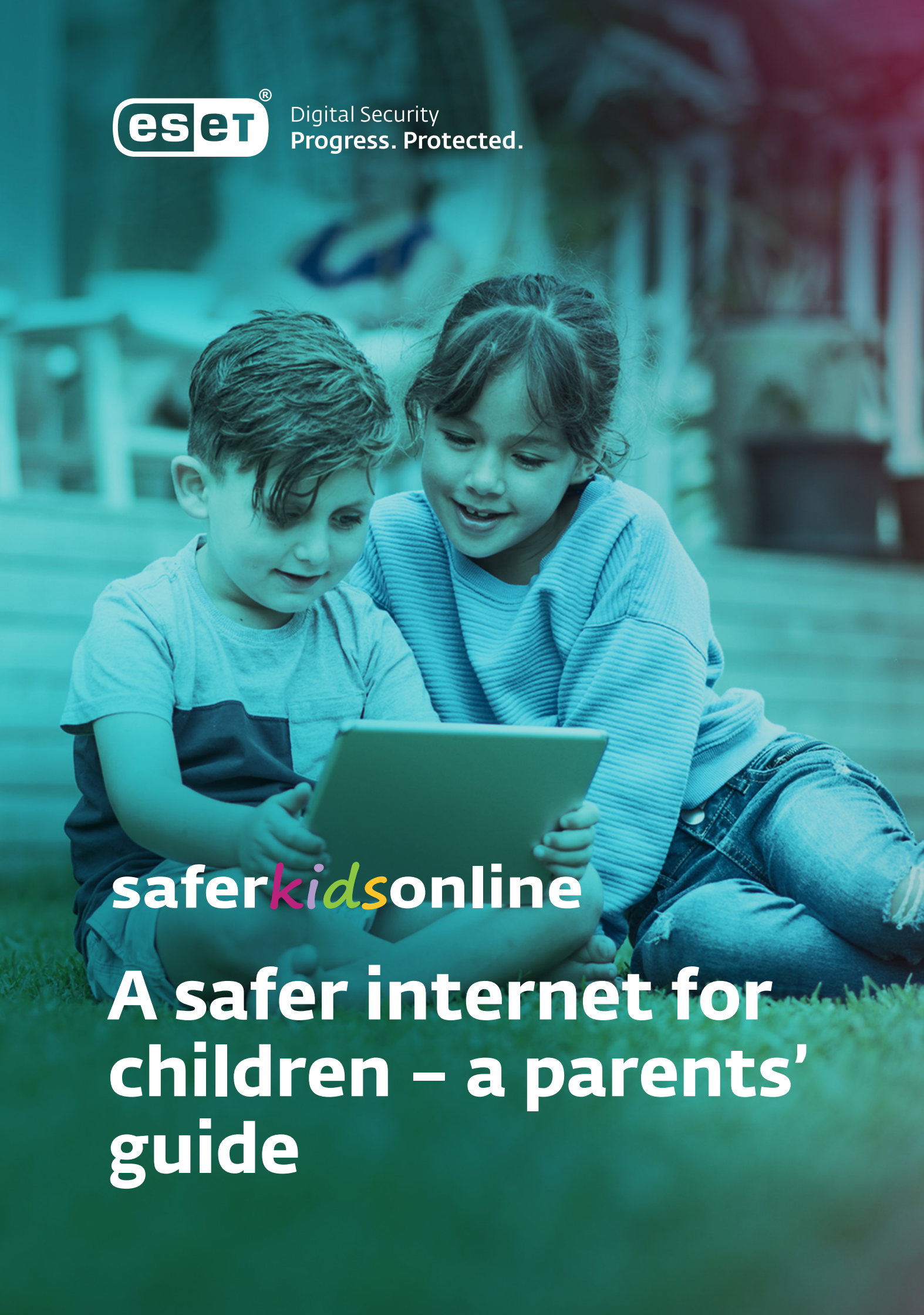

eset
Digital Security
Progress. Protected.
saferkidsonline
A safer internet for children – a parents' guide

Digital lives

Many of us at ESET are parents like you. We feel the need to guide our children through life and protect them from harm, but today the responsibility is a tremendous challenge.
With increasingly complex mobile devices, new communication platforms and a quickly evolving online language, there's a great deal for parents to learn in order to help their children.
This guide offers a helping hand and explains what needs to be done to make sure your children can use the internet safely.

Who should talk to them?

No matter how uncomfortable it makes you, it has to be you.

Your children will meet many people who will play very important roles in their lives, such as relatives, friends, and teachers. However, none of them can take your role as parent. In the eyes of a child, it is you who holds all the answers and is able to help them if they are unsure of what to do next.

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. There are many rules we teach children to keep them safe in the real world. There are just as many for the online world. 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 problems will arise and the appropriate advice will change. Kind and loving guidance for new situations might be the decisive step, which will push your kid in the right direction.

Education – a two way street

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

Children these days are digital natives and are adept at using new technology. For many adults digital skills must be acquired.
However, knowing how to access the internet is not the same as using it safely.

There is no need for you as a parent to know more than your children about what is going on in the virtual world. But you should be in control in case your kids come across something unfamiliar and need to discuss it with someone more experienced.

The important thing is to make the child a part of the debate: create an environment where they can ask questions freely and have time to absorb new information.

What should you do when your kid is at “that age”?

Use parental control tools

Whatever the age of your children you can take advantage of existing technology. ESET Parental Control tools make it possible to block sites or even categories of pages that contain potentially offensive material. You can set time limits for internet surfing or game play. At the same time it allows your kid to ask you for permission to visit certain pages or have more play time, if their homework is done.

In addition to control tools, we have some advice for different age groups that will make children’s online activities safer.

UP TO 10 YEARS OLD

1. Accompany them during their first experiences on the web

Make sure you are there when your little ones take their first steps in 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.

2. Set conditions for the use of the internet

Set basic rules for using the internet. A good practice is to supervise the number of hours spent online and set times during which web access is allowed.

3. Be a good example

Children usually take their parents’ behavior as an example, this applies in real life and online. If family members behave positively, a child is likely to follow suit.

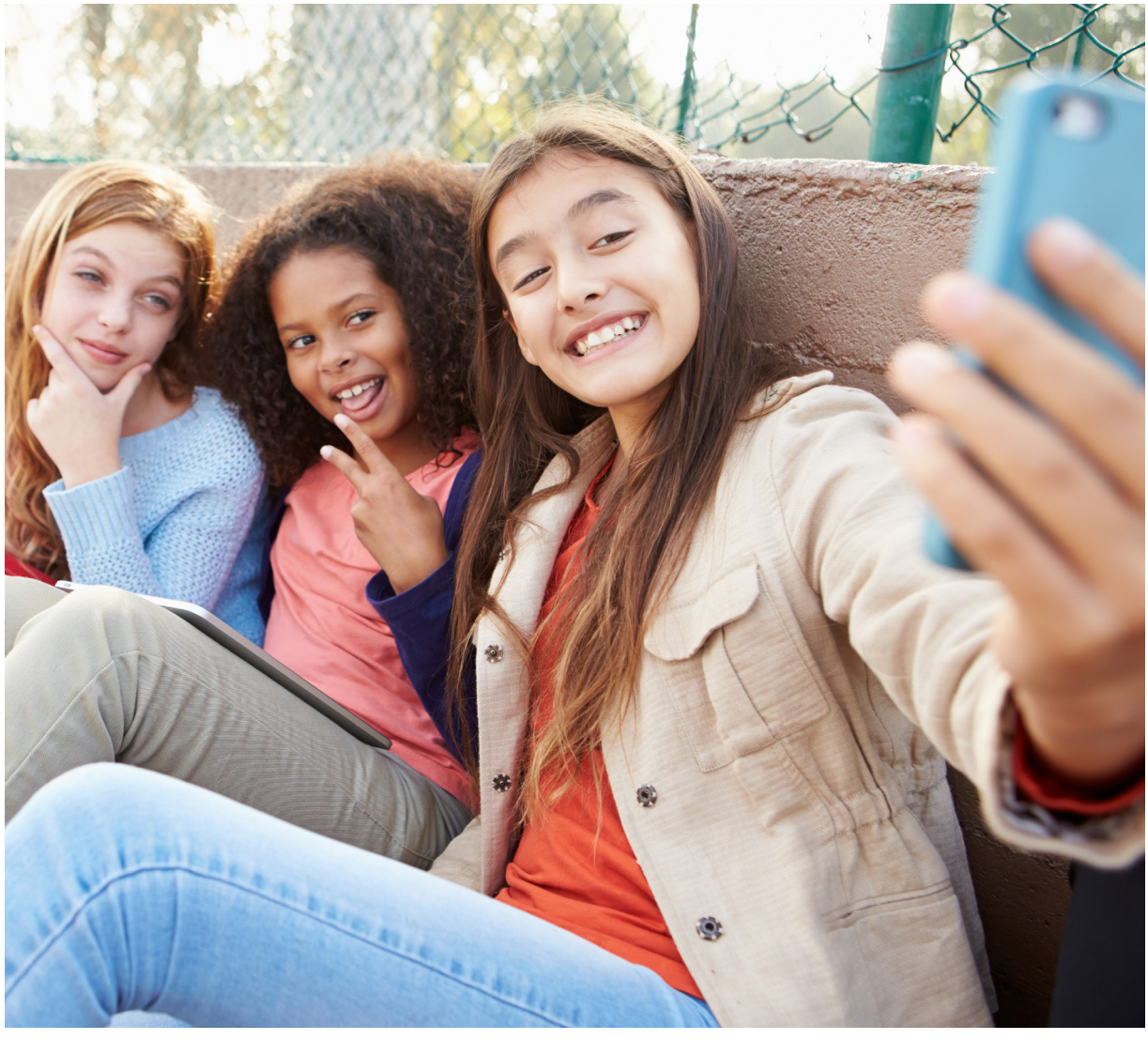
11 TO 14 YEARS OLD

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

It is important to make it very clear to kids that in the virtual world, not everyone is a friend, and that some people may even want to hurt them. Explain why it isn't safe to share information such as address, phone number, school or after school activates they attend. The child should also ask you for authorization before sharing potentially sensitive pictures on the internet.

2. Keep dialogue open

Encourage your kids to be open with you and ask freely about what they see on the internet. If using a desktop computer, try to install it in a room where the whole family spends time and where it may be under your supervision, not in their bedroom.



15 TO 18 YEARS OLD

1. No one else should know their passwords

We know that teenagers can be difficult, but make sure they understand and exercise best practice when it comes to passwords. Respect the privacy of your teenagers but at the same make sure they never give a copy of their passwords to a stranger, or lend them to another person, in person or over the internet.

2. Immediately report stalking and cyberbullying

Remember the school bully? The big kid that was making life really hard for the others? Nowadays, many bullies have moved to modern technology and are hiding behind the internet. What hasn't changed is the fact that they try to psychologically harm others. Therefore, children should be told to immediately inform their parents if they ever experience bullying.

3. Online financial transactions are only for adults

Purchasing something on the internet should not be a problem, as long as it is carefully done. Until kids understand the necessary precautionary measures to be taken when sending personal financial information, they should do so only under their parents' supervision.

What are the main threats online?

Malware

"Malware" is the abbreviation of malicious software. This type of application tries to damage a device in various ways. Some of them will encrypt files on your computer, other will try to spy on you or download other dangerous applications to your computer.
In most cases, the infection takes place due to "mistakes" made by users after being deceived by the attacker. Applying reputable security solutions and good practices reduces the risk of being infected by this kind of malicious code.

Spam

You have seen spam before. It is all those unrequested "junk e-mails" that appear in your inbox. These messages usually include advertising that invites you to visit certain pages with "miracle" offers, mostly harboring potentially harmful content.

Scam

Scams are deceitful acts carried out over the internet. They can initially take many forms, such as spam and the use of social engineering techniques. In the latter case, the attackers offer to sell something, act as your colleagues or even impersonate your bank, while all they want is to obtain confidential information. False messages requesting social network usernames and passwords are also a frequently seen example of scams.

Cyberbullying

This hostile behavior is usually aimed at children. The victim can be threatened and humiliated by their peers in cyberspace and is common among teenagers. It can potentially harm the child, causing them an emotional trauma. Cyberbullying has many routes: even chat functions within console games can be used.

Grooming

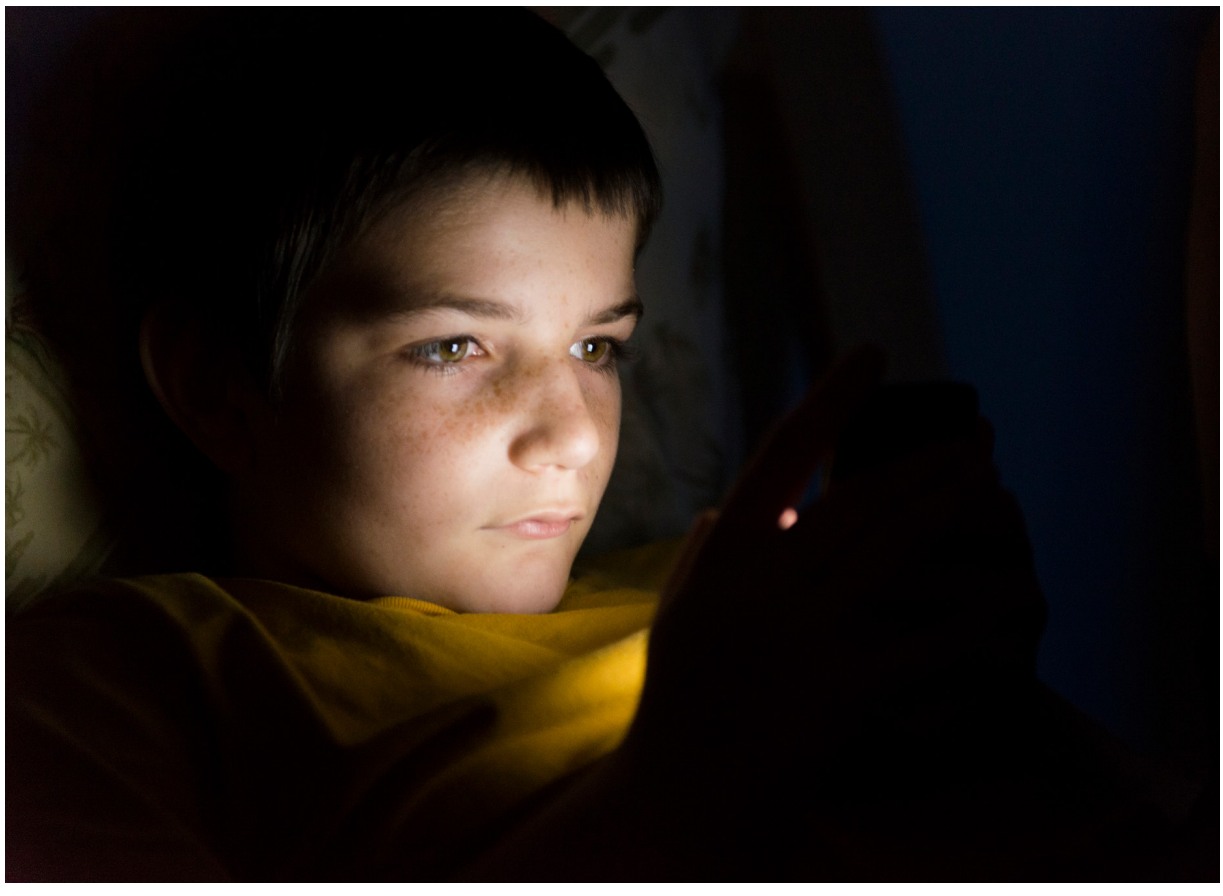
Grooming occurs when an adult tries to persuade a kid to perform sexual activities. A groomer attempts to create an environment of trust and build an emotional connection with the child. Adults often pretend to be children to establish a close relationship and then try to arrange a meeting in person. For a parent it is important to have a good overview of who your kid is interacting with online are.

Sexting

“Sexting” is derived from “sex” and “texting” and has been around for some time. While the SMS function was used on mobile phones to exchange text messages, the development of emails and other messaging services meant that photos and videos could also be sent. It’s common practice as most teenagers and kids have their mobile devices with them at all times.

Information Theft

Information sent across the web, without the necessary precautions, can be intercepted by third parties. Information intercepted in this way can be used for purposes such as identity theft or blackmail.



Final suggestions

Use parental control tools

Parental controls can be used in browsers and antivirus software. It can be found in the latest version of ESET Smart Security or also as a separate app ESET Parental Control for Android. These sort of tools are also available for game consoles.

Do not let your kid send confidential information over the internet

Sensitive information should never be requested via e-mail or chat. Banks do not request your account data or your PIN in this way. It is also important not to give such valuable information to your children.

Do not answer nor eliminate stalking messages

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 this sort of situation keeps happening notify the appropriate authorities. Don't erase any message received as it could be used as evidence.

Stay up-to-date

Nowadays, denying your kid access to technologies is not a solution. Digital devices are part of their everyday lives, and are increasingly important for their development. Instead of putting restrictions in place, help your children use them safely and take part in the interaction between the child and the device. It is also worth pointing out that many of these risks may also affect adults, and many of the precautions described here should be taken at any age.
Children's safety is everybody's responsibility and the tips provided in this guideline are just the basics. For more information, visit our websites and social network pages

www.eset.com

www.welivesecurity.com

www.saferkidsonline.eset.com

Become a Fan www.facebook.com/eset

Follow us at www.twitter.com/ESET @ESET