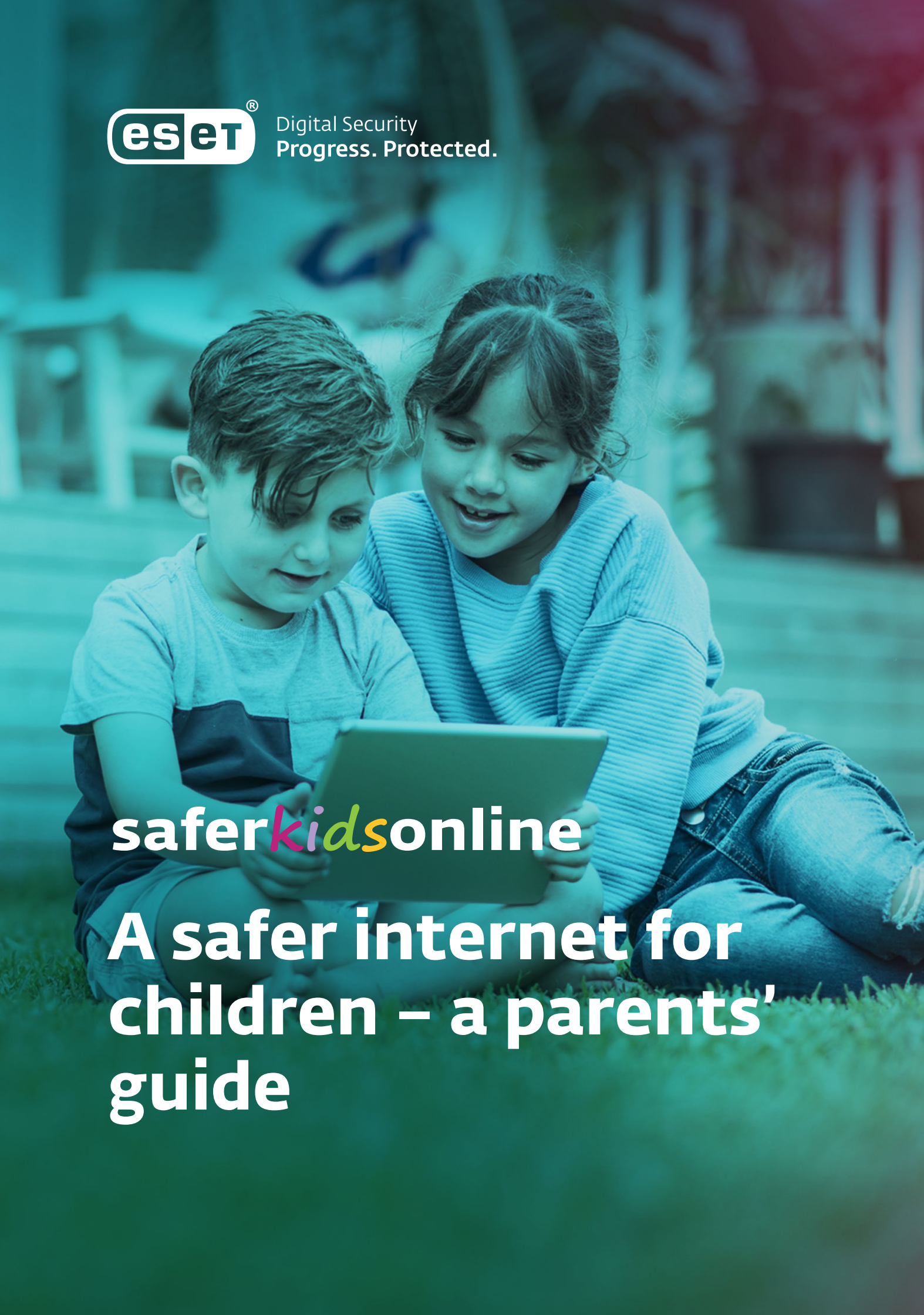


Digital Security
Progress. Protected.

saferkidsonline

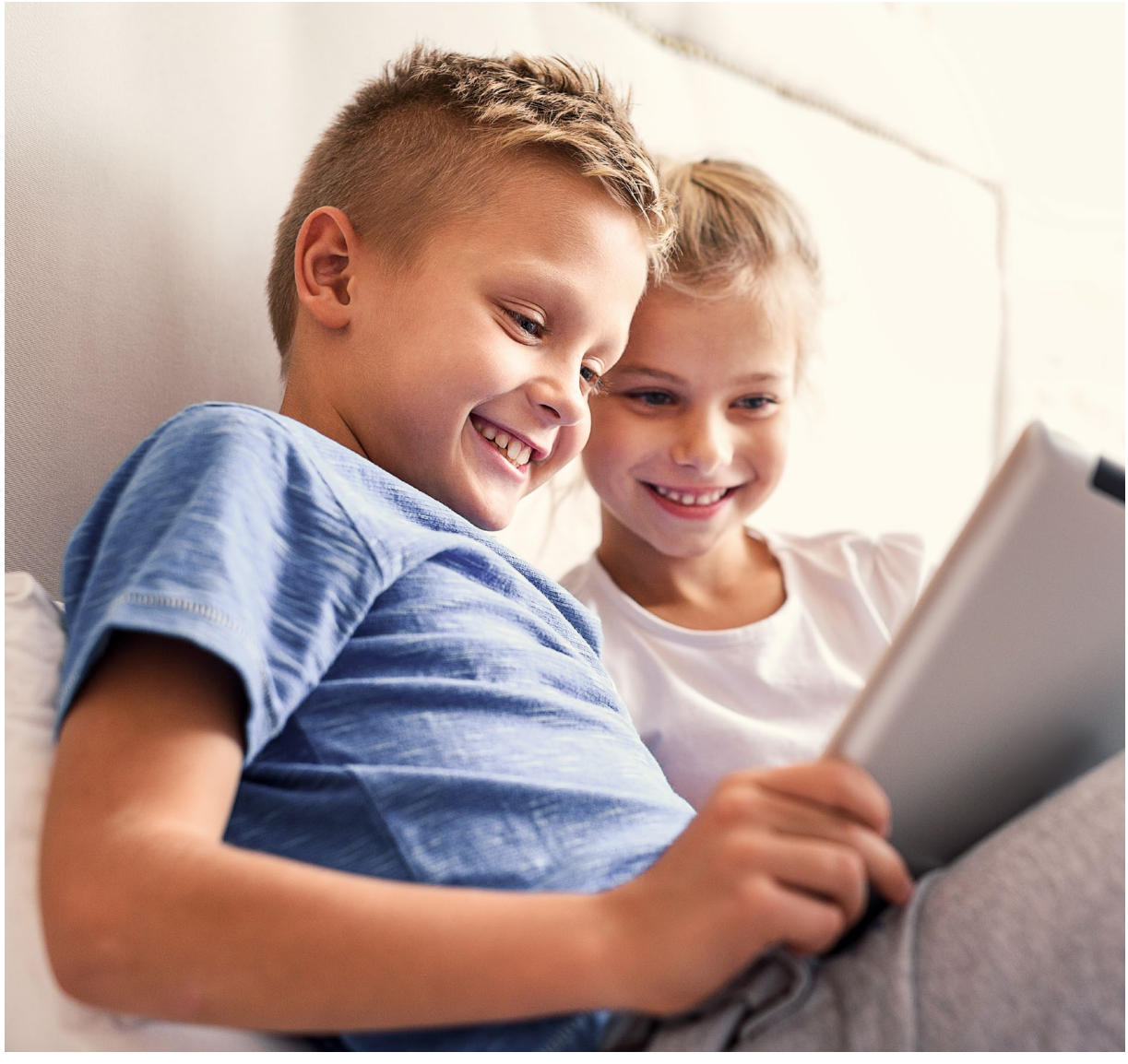
A safer internet for children – a parents' guide

Introduction

Children are our biggest asset, they are our future. Here at ESET we know that, as we are parents just as you. We also feel the need to guide them through life and protect them from harm, but today the responsibility represents a tremendous challenge.

With increasingly modern and complex mobile devices and a quickly evolving language, pressure is high on parents when it comes to educating themselves to be able to educate their children.

This guideline is offering you a helping hand and explains which aspects should be taken into account in order to make sure your children have a healthy and safe experience on the internet, and in fact in everything, the cyberspace has to offer.



Who should talk to them?

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

Throughout his or her childhood, your daughter or son will meet people who will play very important roles in his or her life, such as relatives, friends, and teachers.
Yet, none of them can take on your role as the 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. Or as soon as possible.

As your child grows older, new problems arise. A kind and loving advice in any of these new situations might be the decisive step, which will push your kid in the right direction in the future. This being true especially, when speaking of cyber space.
From the very moment, a kid shows some interest in your tablet, smartphone or computer and the internet itself, you should start explaining, that all it learned about safety in general applies for the web as well. In other words, the means change, but the threats remain the same.

Parents educate their children and also learn from them

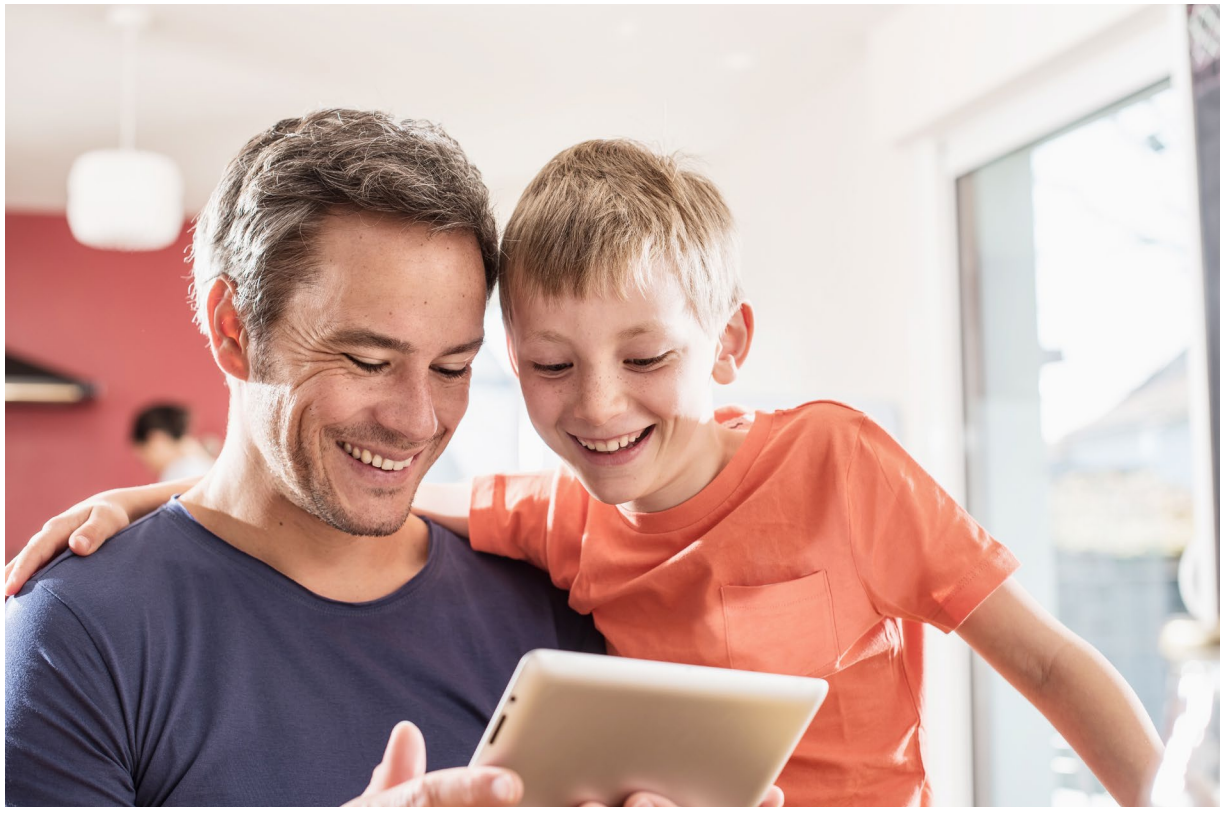
Do you feel like your children "know more about computer technology" than you do? You are not the only parent out there, suffering under this complex.

While minors nowadays seem to be digital natives who were born with smartphone in their hand, many adults have acquired these skills only later in life.

Yet, this does not mean that your child should be the one who holds the keys to all computing power in your home. Knowing how to use the internet is not the same as understanding the impact of any given action online.

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. Therefore, create an environment where they can ask freely and get their heads around all the new information.



What to do when my kid is at that age?

Below, we share a basic set of tools that make children's on-line activities safer, according to their age.

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 the first steps. The first contact a child has with the internet is a good opportunity to sit down and guide him or her in their new adventure.

2. "Set the 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 also to set times in which the use of web is allowed.

3. "Be a good example"

Children usually take their parents' behavior as an example, this rule applying equally on-line as well as in real life. If the members of the family have a positive behavior, this will immediately pass on to the child.

11 TO 14 YEARS OLD

1. "Use parental control tools"

Take advantage of the existing technology and use it in your favor. ESET Parental Control tools make it possible to block sites or even categories of pages that contain potentially offensive material, allow you to 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.

2. "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 every person 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, telephone, schools or after school activates they attend, etc. The child should also ask you for authorization before sharing potentially sensitive pictures on the internet.

3. "Keep the dialogue open"

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

15 TO 18 YEARS OLD

1. “Nobody should know their passwords”

We know how the teenagers are and that they can get really difficult, but make sure they understand the best practices when it comes to passwords. After all, they are like their house keys. Respect the privacy of your teenagers but at the same make sure they never give a copy of their passwords to a stranger, or “borrow” them to another person, neither in person nor over the internet.

2. “Immediately report the stalking and cyberbullying”

Remember the bullies in your class? The big kid that was making the life really hard for the geeks? Nowadays, many of them have moved to modern technology and are hiding behind the internet. What hasn’t change is the fact that they try to psychologically harm others. Therefore, children should be told to immediately inform their parents if they ever come across these wrongful acts.

3. “Keep the dialogue open”

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

Cyber Safety Vocabulary

“At home or in school”

Although being a parent gives the crucial responsibility for child’s cyber security to the parent, it doesn’t mean you have to carry all that load only by yourself. Check the programs your kid’s school offers if there are any lessons focusing on internet safety. Moreover, if a popular teacher is leading the course, he can be a really strong role-model for the teenager, who refuses to listen to his or her parents. Building on the cyber security basics you gave your kid earlier, school can bring his or her awareness to the next level.

“Parental Control”

Imagine you have a program that can set specific times and hours for your kid to access the internet, limit the types of pages he or she can visit, allows or restrict games to be played or monitor the exact location of the child. Such software is called parental control and it gives you a powerful tool to check what your son or daughter is up to, when they are online.
On the other hand, it should offer them a say too. Since if it feels like they have no control and the restrictions are too harsh, it will only make them circumvent the rules.

“Social networks”

Think of all your schoolmates, friends and acquaintances you have ever met. Now put most of them in a single room and let them talk about what they are doing at the moment, show you their holiday pictures or favorite video. That is basically how the social networks work nowadays, allowing the user to organize events, communicate with other people individually or in a group and see what they like.
This small microcosm you create is only a small part of a superstructure formed by hundreds of millions of users that are there to interact with you at your wish. However, all those benefits are accompanied by some risks.

Which are the main threats?

Malware

It is the abbreviation for malicious software. The purpose of this type of applications is to damage the computer in various forms. Some of it will encrypt files on your computer, other will try to spy on you or download other dangerous application into your computer.
In most cases, the infection takes place due to "mistakes" done by the users (or their kids), 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 are filling your inbox every day. Usually this type of messages include advertising that invite 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 take many forms, such as spam as well as 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 our social network user and password over the internet are also a frequently seen example of scam.

Cyberbullying

This hostile behavior is aimed especially towards children. The victim is usually threatened and humiliated by his or her peers in the cyber space and is frequent among teenagers. It can potentially harm the child, causing him or her an emotional trauma. Cyberbullying usually takes place over the internet, but even cell phones or game consoles are not immune to this malicious behavior.

Grooming

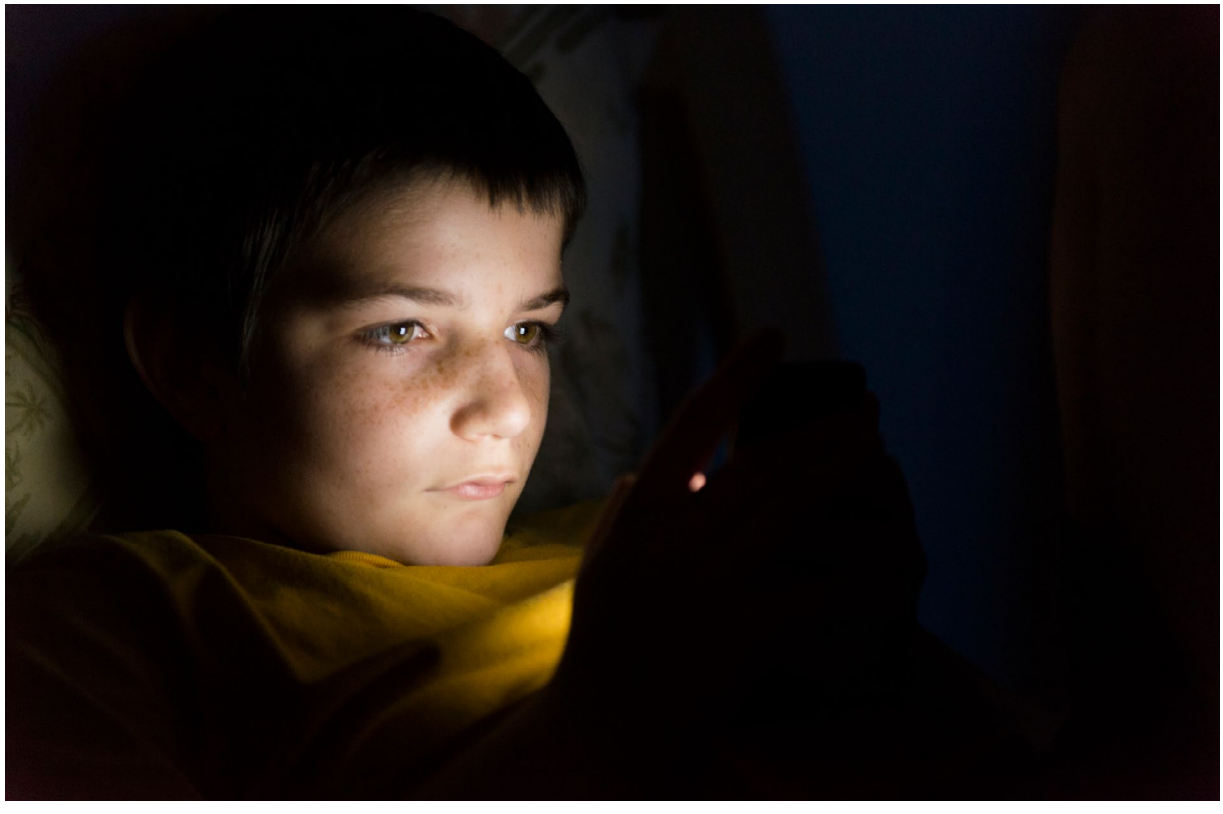
It is when an adult tries to persuade a kid to perform sexual activities creating an environment of trust and building an emotional connection with the child. Many times adults pretend to be children so as to establish a close relationship and then, try to arrange a meeting in person. For a parent it is important to have a good overview of who the people your kid is interacting with online are.

Sexting

Sexting comes from the acronym of Sex and Texting. Initially, as its name indicates, it referred to e-mails that contained erotic messages. Later on, due to technological progress, this evolved to include the exchange of images and videos, and it became common practice since most of the teenagers and kids have their mobile devices with them at all times.

Information Theft

All the information that travels through the web, without the necessary precautions, may be intercepted by third party. And many times, this is the purpose of an attack. Usually, the targeted information is personal data of you or your child. Taking a wrong step in this sort of incidents may expose the minor to the loss of family money or in the worst case to identity theft.



Final suggestions

1. Use parental control tools

This can be used both in browsers and also in antivirus software. It can be found in Version 9 of ESET Smart Security or also as a separate app ESET Parental Control for Android. This sort of tools are also available for game consoles, such as Nintendo Wii and Xbox 360.

2. 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 and much less your PIN in this way. It is also important not to give such valuable information to your children.

3.Do not answer nor eliminate stalking messages

If your child is a victim of cyberbullying he or she should not retaliate. Explain that the stalker wants to provoke exactly this sort of reaction as it feeds his or her desire to harm. If you come across this sort of situations and if they happen again, notify the corresponding authorities. However, never erase any message received, as it is evidence of the act.

4. Not everything you see on-line is true

Not all the information that can be found on the web comes from a reliable source and it is important for the child to know the difference. Create a blog where you can post your opinion to demonstrate how easy it is to acquire a space online and manipulate the content.

5. Open dialogue

The communication you have with your children plays a key role in their safety. It is much more productive to encourage them to talk about their fears and concerns than to punish them. A good environment and an open dialogue, both on the internet as well as in real life, may be the key to success when dealing with their well-being.

6. If you post something online, it stays there forever

Teach your kids, that anything posted online stays there forever. What is more, they lose control over it as it can be shared by anybody, even by strangers. A good rule of thumb is not to share any photos, statuses or other content, they would not want you or their grandma to see. This applies to all forms of online presence – social networks, instant messengers, blogs or comments.

5 more tips for parents

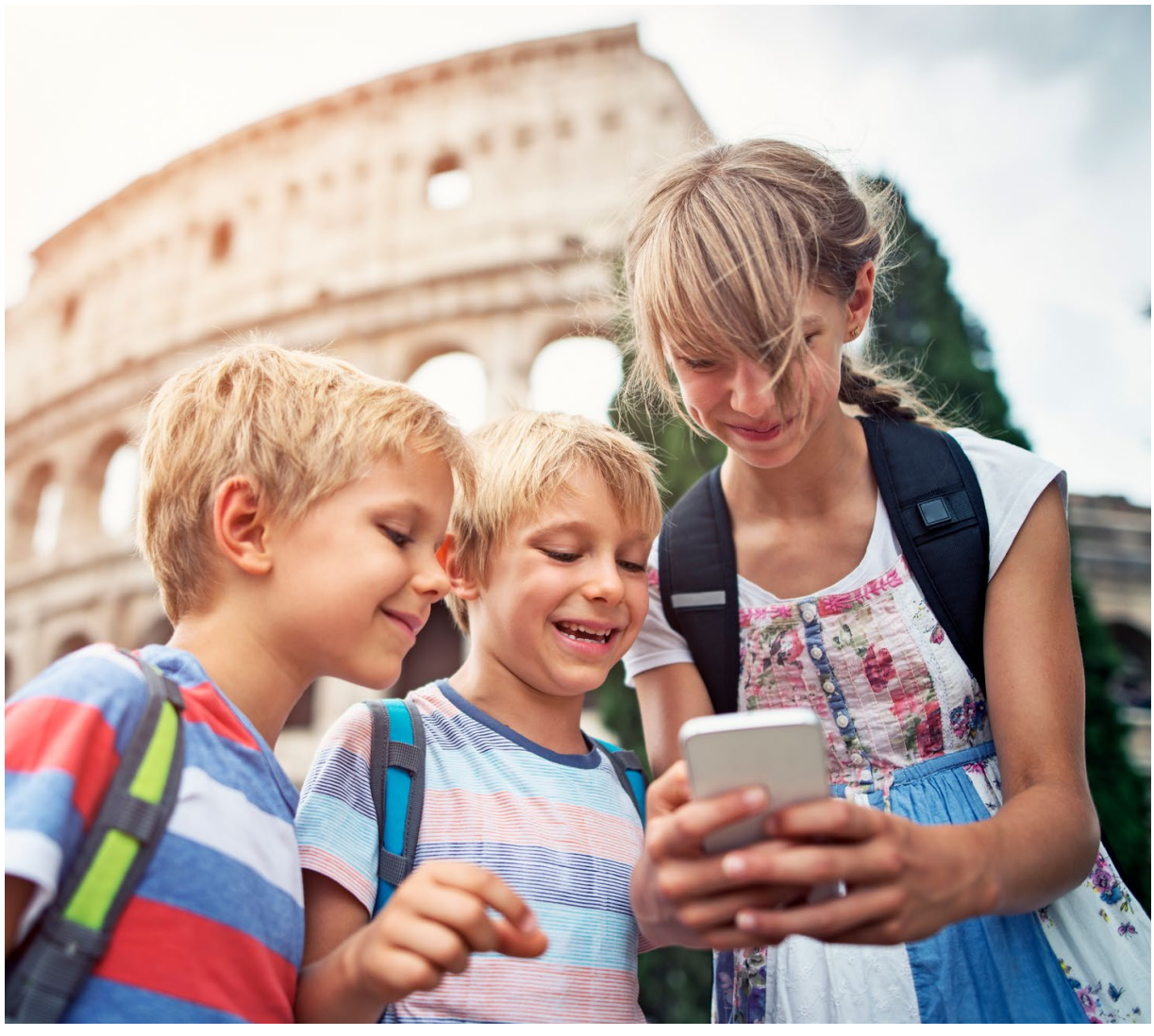
1: Assign a user account to your child. This is the first step to efficiently control his or her activities online. The role of system administrator should always be played by an adult.

2: Keep your antivirus and parental control tool updated.

3: Monitor his or her browsing history. If this is cleared, it is a good reason to have a talk.

4: Control the web camera, and make sure that it is disconnected or covered (if built-in) when not in use.

5: Check the child's social network settings. A profile that is publicly shared with no limitations may put a young person's integrity at risk.



Conclusion

Nowadays, denying your kid access to technologies is not a solution. They are part of his or her everyday life, and are increasingly more 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 under any situation and at any age.

Children's safety is everybody's responsibility, and the tips provided in this guideline will help adults protect minor's information, systems, and integrity. For more, visit our websites and social networks:

www.eset.com

www.welivesecurity.com

Become a Fan www.facebook.com/eset

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