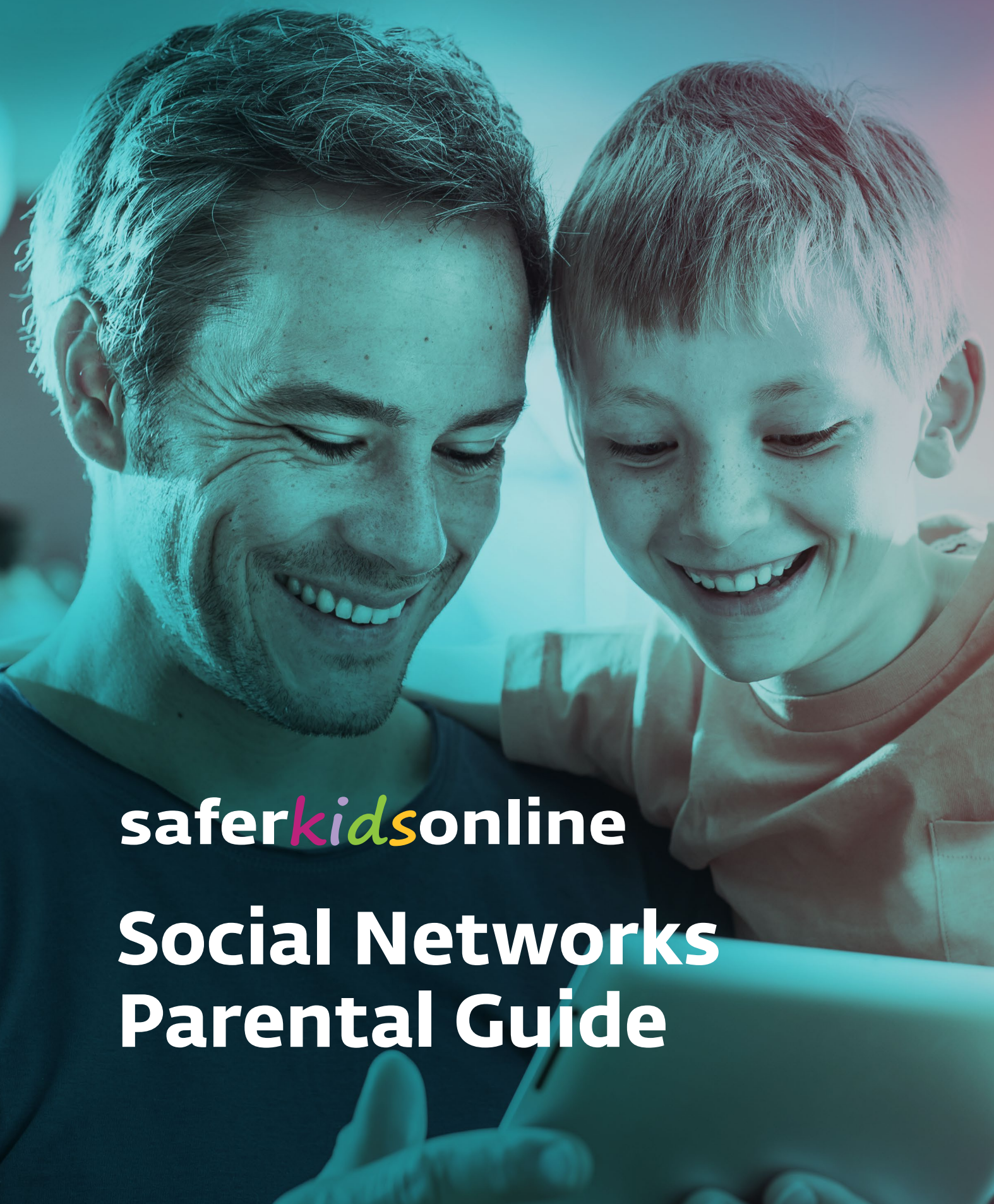
ENJOY SAFER TECHNOLOGY™



saferkidsonline

Social Networks Parental Guide

Introduction

Do you remember a time when kids played outdoors and only came home when they were hungry? The internet has changed everything. Nowadays, young people can spend hours every day on social networks.

Many of us at ESET are parents too, so we understand the worries you have seeing your child absorbed in the online world. That's why we've produced this guide. In it you will find information on the possible threats lurking on social networks and solutions which will help you keep your family protected.

1. What to watch out for

Malware

Malware is a combination of the terms malicious and software – in other words harmful code. Viruses, worms and trojans are some examples. Scammers use social networks to lure users into downloading malware, often by promising pirated software or games.

Phishing

The term "phishing" is derived from "fishing", as bait is used to catch victims. Many attackers use this method to steal sensitive information – such as login credentials for a child's social network profile. It is usually done via email linked to a replica of a social media website. It can be quite difficult to identify a fake page as the differences are often minor and kids might insert personal information without even noticing that something is amiss.

Identity Theft

Make sure your kids are not posting sensitive information like home address, school address, phone number or birthdate which could be used to identify them. Identity theft is a widespread form of cybercrime, where criminals obtain users' personal information and use it to impersonate them for malicious purposes.

There are two main ways in which the attacker may get this sensitive data:

Using social engineering, often by pretending to be your child's friend.

Using information that is publicly accessible on a social network profile - selecting the appropriate privacy settings is crucial.

Online Stalking and Abuse

Not all threats to your children on social networks have to involve cybercriminals. Their peers can also be a problem. Bullying doesn't just happen in schools: nowadays it's occurring on the internet and can be just as harmful as in real life.

Another serious risk is grooming, especially where younger children are concerned. Grooming involves an adult trying to gain a child's trust and build a relationship with them to persuade them to perform sexual activities. This often includes sexting, (messages with inappropriate content that might be sent to or by your child).

2. What measures can you take to protect your children?

Looking at the potential threats, the use of social networks might seem like a dangerous activity. However, forbidding your child to use them is not likely to solve the issue. They'll find ways to get what they want. Below you can find tips that will make using social networks safer and provide adequate protection for your children and family.

Talk

Dialogue is one of the most important parts of keeping your children safe online – especially when we talk about social networks. Maintaining open and honest communications with your children is crucial if you want them to trust your judgment and follow your advice.

A good example is cyberbullying and its prevention. Make it clear to your child that if they ever encounter such behavior, even if it doesn't concern them directly, they should immediately let someone know - you, their teacher or other responsible adults.

Use parental control software

Depending on your children's age, use parental control software. ESET Smart Security, allows you to set a list of blocked websites and restrict the times at which your child can be online.

However, kids should also have their say. Therefore, ESET Parental Control for Android allows them to ask you for permission to visit specific websites or have additional social network time, perhaps if they have finished the chores or homework earlier than expected.

Using a reliable security solution

As malware is one of the most widespread threats in cyber space, installing a security solution with proactive detection capabilities onto your child's devices is essential for avoiding infections when using social networks.

Antispam and firewall tools also make system safety optimization possible in the face of these risks. Also, your child should never use an administrator account when surfing social networks. Set up a special user profile for your kids to minimize the impact of security incidents.

Use strong passwords and two-factor verification

Do your children know what a safe password looks like? Make sure they don't use easy-to-guess options like "password" or "12345". It should be at least 10 characters long, contain upper and lower case characters, a number and a special symbol like # or @. Adapting a phrase or lyrics from a song can help:

Mary had a little lamb becomes Maryhadalittle1@mb

Also, remind them not to share their passwords with anyone, not even their best friends.

If connecting to Facebook, Twitter or other popular social networks, make sure your kids use two-factor verification offered in the security settings. Receiving a single-use passcode on their smartphone adds another security layer that is hard for attackers to crack.

Change profile settings to "private"

The default privacy settings for social networks will not guarantee safety for your kid. It is therefore advisable to spend some to set them up right and to check which information could be leaked. Let's use Facebook as an example:

Facebook

Use the profile settings to ensure that nothing is shared with all users. Preferably, make information available only to their friends and family, and if possible, only to small groups (such as close family or best friends).

Limit the audience which can see pictures, statuses and other content where your kid has been tagged. Prevent applications from accessing their personal information or posting on their wall.

Teach them only to accept friendship requests from people they know personally. Make it clear that talking to strangers or contacting them on the internet can be as dangerous as meeting in the real world.

For detailed information about using Facebook settings, please read our blog: http://blog.eset.com/2011/05/25/facebook-privacy

Twitter

Twitter has its own specific considerations, such as 280 character limit, or frequent use of shortened URLs. It is these differences that you should also address when explaining to your child how to stay safe.

In addition to only following people they know and avoiding suspicious links, they should also check the legitimacy of any message they may receive. Malicious messages are often identified by other users and the information shared so a quick search using part of the message can often help.

Also, install a reputable browser plug-in on their computer or device that allows your kids to see the original link from a short URL address without clicking on it.

Other social media

There are many social media sites catering for different interests and age groups. It's important to check your children are using ones appropriate for them. We have video guides covering Snapchat, Instagram and YouTube and have also compiled a list of appropriate social networks for children.

3. Conclusion

Social networks can be a valuable resource for Internet users. Yet, as this guide proves, there are many threats to which kids may be exposed when using them. Don't underestimate cybercriminals or other malicious actors. It's essential to implement best practice and use dependable security tools to protect the important people in your life.

Helping them set their social network profiles properly and offering simple but useful advice might be the decisive thing to do when it comes to keeping them safe.

10 top tips

1. Teach your kids to stop and think before clicking on links and download buttons
2. Teach them to approach online communication with a healthy sense of caution
3. Set your children's accounts to private mode
4. Teach them to decline friend requests coming from strangers
5. Keep their operating system and security software updated
6. Be a good role model and keep your own digital consumption under control
7. Look for signals that might indicate that a child is a victim of cyberbullies
8. Use a reputable parental control app like ESET Parental Control
9. Encourage them to use strong passwords
10. Ask them to think before sharing personal information, videos or photos.