Social Networks Parental Guide
Introduction

It is not that long ago, when kids were playing mostly outdoors and came home only when they were hungry. But the internet boom has changed everything. Nowadays, young people instead of going outside spend several hours a day in the virtual reality of social networks.

Here at ESET we are parents too, and we understand the worries you have seeing your child absorbed by the cyber world. That is the reason why we bring you this guide. In it you will find information on the threats lurking in the social networks as well as solutions which will help you keep your family and kids protected.
1. What to watch out for?

**Malware**

It is an English abbreviation of the terms malicious and software – or in other words harmful code. Viruses, worms and trojans are some of the known examples, their attacks on users without age restrictions richly documented in theory and “in the wild”.

One of them – Koobface worm – was spreading on Facebook in 2009. Using attractive messages it was making computers of its victim’s a part of botnet – a zombie army of computers that can be remotely controlled by the attacker. Its newer version that appeared on the radar about two years later was even more advanced, infecting the social network users regardless if their devices were running on Windows, Mac or Linux operating system.

**Phishing**

Many attackers use this method to steal sensitive information – such as login credentials for social network profile of your child. It is usually done via e-mail linked to a replica of social media website. It may be pretty hard to identify the fake page as the differences are often minor and duped kids may insert their info without even noticing that something is amiss.

**Identity Theft**

Be sure your kids are not posting sensitive information like home address, cell phone number, school or class they are attending, birthday or other data, which could be used to identify them. The reason is identity theft, one of the widespread forms of cybercrime, where cyber criminals obtain your personal information and use it to impersonate you or even your child for malicious purposes.

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

Using social engineering, pretending to be a friend of your child or in his or her age, trying to extract personal information by the way.

Due to wrong network settings, too much information may be publicly accessible directly at the social network profile of your child. Important to note, this isn’t just a problem of young people but also of many adult users, unaware of the risks.
Online Stalking and Abuse

Not all threats for your daughter or son in the social networks has to involve cybercriminals. His or her peers can be a problem as well. We are saying this, as bullying is not a thing of schools and classrooms anymore. Nowadays it moved to cyber space, being as harmful as ever.

Another risk is grooming, especially targeting younger children. It describes an adult pretending to be a kid making it easier to gain their trust and persuade them to perform sexual activities. This is in many forms connected also with sexting, which includes messages with inappropriate content that might be sent to or by your child.
2. What countermeasures can I take?

In these threat scenarios, the use of social networks seems as a really dangerous activity. Yet, forbidding your child to use it is most probably not going to solve the issue, leading only to circumventing of the rules you set. But don’t worry. Below, you can find tips that will make social networks use 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. Keeping the channels and your mind open to questions and discussion is crucial if you want your kids to trust your judgment and follow your advice.

A good example is cyberbullying and its prevention. Make it clear to your daughter or son, that if they ever encounter such behavior, even if it doesn’t concern them directly, they should immediately let know you, their teacher or trainer (depending on where it happened). Important to notice, never delete the bullying message as it is the only evidence.

**Use parental control software**

Depending on the age of your children, use parental control software and its features. ESET Smart Security 9, allows you to set a list of blocked websites and also restrict the time and number of hours your child can spend online.

On the other hand, kids should also have their say. Therefore, application ESET Parental Control for Android allows them to ask you for permission to visit a specific website or have additional social network time, if they finished all the chores and homework earlier than expected.

**Using reliable security solution**

As malware is one of the most widespread threats in cyber space, installing an antivirus software with proactive detection capabilities and an updated signature database into your child’s devices is essential for avoiding infection when using the 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.

**Set up https use**

Be sure your kid is surfing via https protocol (you can see this in the location bar, where you type the name of the website) when using social networks. Doing so helps you to avoid eavesdropping attacks on legible text information. While using https protocol, all data - not just user and password of your little one - will be encrypted and illegible to any malicious actor.

Advise your youngsters to use these useful settings also when they access social network from public Wi-Fi.

**Use strong passwords and two-factor verification**

Do your children know, how a safe password looks like? Make sure they will not use easy-to-guess options like “password” or “12345”. Moreover, it should be at least 10 characters long, contain upper and lower case characters, number and a special symbol like # or @. Also, remind them not to give their password to nobody, not even their best friends.

If connecting to Facebook, Twitter or other widely popular social networks, be 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 to crack for the attackers.

**Set up social networks privacy right**

Default social network privacy settings will not guarantee safety for your kid. Thus, it is advisable to devote enough time when setting them right and also to check which information can possibly leak. To show you what we mean, we used Facebook as an example:

**Facebook**

Make sure that no profile setting of your child’s profile is publicly available, with no exceptions. Preferably, make information available only to his friends, and if possible, only to a small group of them (such as family or close friends) if they are too many.

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

Teach them only to accept friendship only from people they personally know. Make it also clear that talking to strangers or contacting them in the cyber space may be as dangerous online as it is in the offline world.

Show your kids how to manage their profile using Activity log, reviewing their actions and actions of others that are connected to them. For more detailed information read our blog: [http://blog.eset.com/2011/05/25/facebook-privacy](http://blog.eset.com/2011/05/25/facebook-privacy)
Twitter

Twitter has its own specifics, such as 140 characters tweet 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 things such as following only people they know or avoiding suspicious links, they should also check the legitimacy of any suspicious message they may. If it is malicious and they search for parts of it, it is most likely that someone has already discovered the deceit and exposed it in the network itself.

Also, install a browser plug-in on their computer or device that solves the short URL addresses and allows your kids to see the original link without having to click it.

Other social media

Are your kids favoring other social media like Snapchat, Instagram or YouTube? See also our other video guides, dedicated specifically to these networks. You can also pick one of the more appropriate social networks for children, we have in our list.
3. Conclusion

No doubt social networks are a valuable resource for Internet users. Yet, as this guide proves, there are many threats to which kids may be exposed when using them. So don’t underestimate cybercriminals or other malicious actors and make a good use of IT tools to protect the most valuable people in your lives.

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.
If you want to remember most advices given in this guide, you can apply this shorter and simpler version called Cyberspace Safety Decalogue:

1. Avoid suspicious links
2. Never access doubtful reputation web sites
3. Update operative system and applications
4. Download applications only from official web sites
5. Use Security Technology
6. Avoid entering personal information in doubtful forms
7. Be careful with the results of web browsers
8. Accept only known contacts
9. Avoid running suspicious files
10. Use strong passwords