ENJOY SAFER TECHNOLOGY™

saferkidsonline

Social networks parental guide

saferkidsonline

Remember the times 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 like Instagram, Snapchat, TikTok, WhatsApp, Houseparty and Telegram.

Many of us at ESET are parents, so we understand why you might have concerned about the online world. We produced this guide to share info about potential threats lurking on social networks and solutions which will help you keep your family protected.

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 won't solve the issue—they'll find a way to do what they like. Instead, use the following tips will help make using social networks safer for your kids and family.

Keep communication channels open

Dialog 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 cyberbullying is completely unacceptable—whether they themselves are being targeted, or if they're tempted to participate in attacking others. When they encounter such behavior, even if it doesn't concern them directly, they should immediately let someone know—you, a teacher or other responsible adults.

Use parental control software

Depending on your children's ages, you can use parental control software to set a list of blocked websites or topics, and restrict the times at which your child can be online. You can also offer your child full access to everything online, with built-in monitoring that enables you to see what they're seeing.

Your child should be part of the decision making process. If you choose to limit their access or time online, ESET Parental Control (included in products such as ESET Internet Security), enables children to ask you in real time for permission to visit specific websites or have additional social network time. Remember: You want to encourage ongoing discussions about the importance of balancing time spent socializing online with other priorities like homework.

Using a reliable security solution

Installing a security solution with proactive detection capabilities onto your child's devices is essential for avoiding malware, ransomware, phishing attempts, etc., when using social networks. Make sure the solution you choose includes antispam and firewall protection.

Use strong passwords and two-factor verification

Do your children know what a safe password looks like? Hard to believe, but even some adults still use easy-to-guess options like "password" or "12345"!

Your child's passwords should be at least 10 characters long, contain upper and lower case characters, a number and a special symbol like # or @.

Adapting a phrase can be helpful in creating a hard-to-guess password. For example: Chicago Red Sox 2 - San Francisco Giants 9 turns into Crs2#SFg9.

Remind them not to share their passwords with anyone, not even their best friends, family members, teachers, etc.

When connecting on social networks, make sure your kids use the two-factor verification option offered in the security settings. Also known as two-factor authentication or 2FA, this method adds another security layer that is hard for attackers to crack—by sending the child a one-time password to enter each time they log in or use an untrusted device.

You can set this up together and discuss why it's important that only the authorized user should be able to access an account. If someone else gets in, they could delete information, add inappropriate photos or messages, cyberbully you, or even attempt to steal the real user's identity.

To set up 2FA on Instagram using a mobile phone: Log on to your child's profile by tapping the **person** icon. Swipe to the left and tap the **Settings** icon that appears. Go to **Privacy & Security**. Select **Two-Factor Authentication** > **Get Started** and then toggle on **Text Message**. Or, if you'd rather use a tool such as Google Authenticator, select **Authentication App** instead. Google Authenticator is more secure as it removes the issue and risk from SIM swapping.

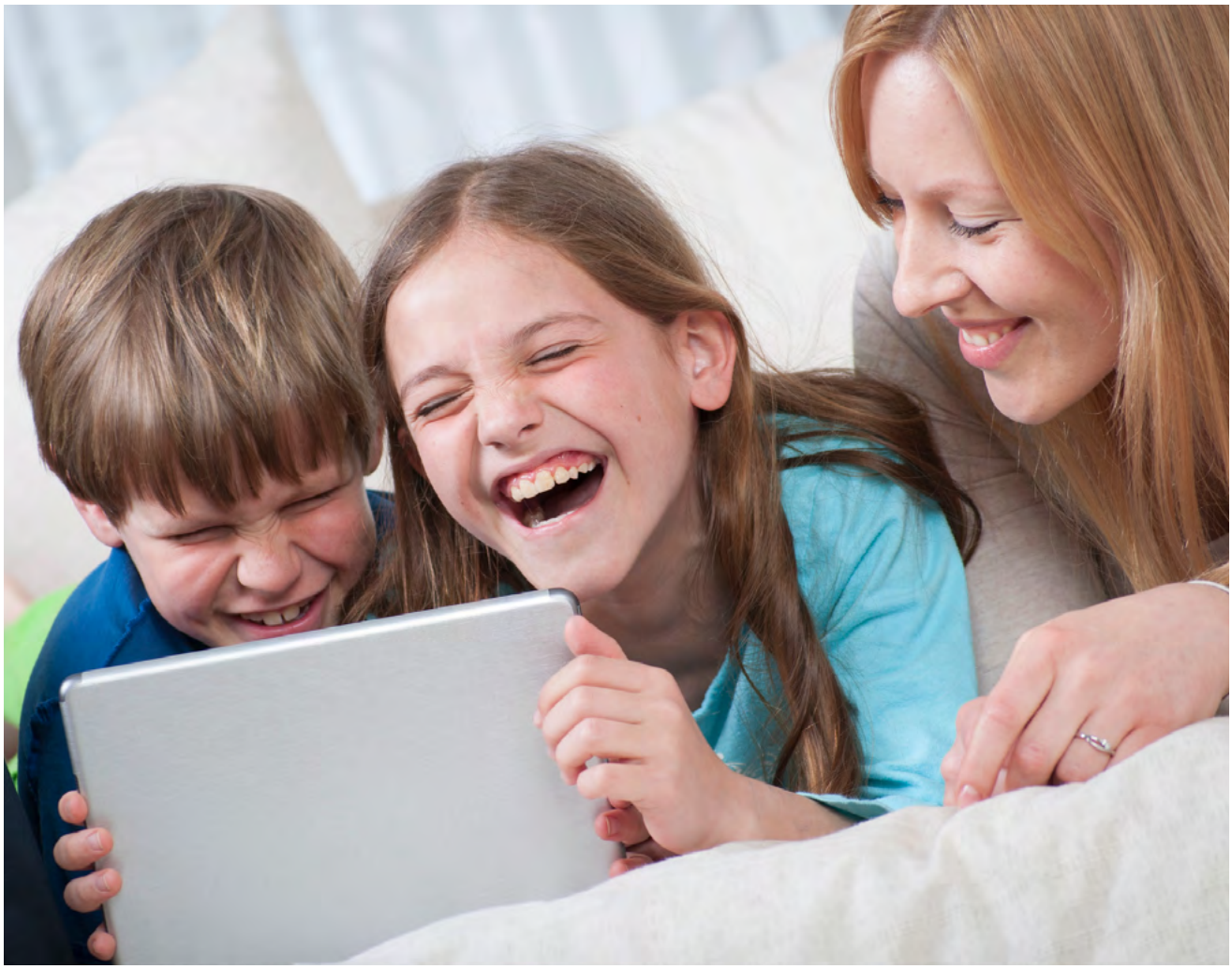
Change profile settings to “private”

The default privacy settings for social networks will not guarantee safety for your kid. For starters, profiles should be set to **private** instead of **public**. Let’s use Instagram and a mobile phone as an example:

Log on to your child’s profile by tapping the **person** icon. Swipe to the left and tap the **Settings** icon that appears. Select **Privacy and Security** then **Account Privacy**.

Toggle **Private Account** on.

This basic information only scratches the surface of available privacy settings. For details and to set stricter limits for increased safety and privacy, visit the social media site’s help page (for example, **https://www.facebook.com/help, https://help.instagram.com/**).



10 top tips

1. Teach your kids to stop and think before clicking on links and download buttons.
2. Remind them to approach online communications with a healthy sense of caution, as not everyone online is who they claim to be.
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, such as being irritable, withdrawn or upset after spending time online. Talk to them about it.
8. Use a reputable parental control app like ESET Parental Control.
9. Encourage them to use strong passwords and two-factor authentication.
10. Ask them to think carefully before sharing personal information, videos or photos.