Parents fear for kids' online safety, but aren't putting time in to talk about it

Kaspersky's Family Campaign Report
September 2019

kaspersky

Parents fear for kids' online safety, but aren't putting time in to talk about it

Being a parent is hard, especially when you have to navigate the rapidly developing technological landscape that could affect your children's wellbeing. Nowadays, kids are among [the most active Internet users](#), and have almost unlimited access to consumer technology.

The Internet can be a dicey place for kids who may be prone to believing in something – even if a total stranger or a faceless programmed ad promises this 'something'. Thus, parents today should be aware that, in addition to the positive side of the Internet like e-learning or keeping in touch with friends or relatives, children may also face various risks online. These, if not guarded against and guided through, can affect a child's emotional state or subsequent development.

Kaspersky's latest survey – conducted by Savanta and polling 8793 parents of children between 7 and 12 years old in 20 countries across the globe – explains their fears, experiences, and tactics when it comes to internet safety for their children. The survey also provides insights into what they consider the most effective ways to avoid and mitigate dangers to children online.
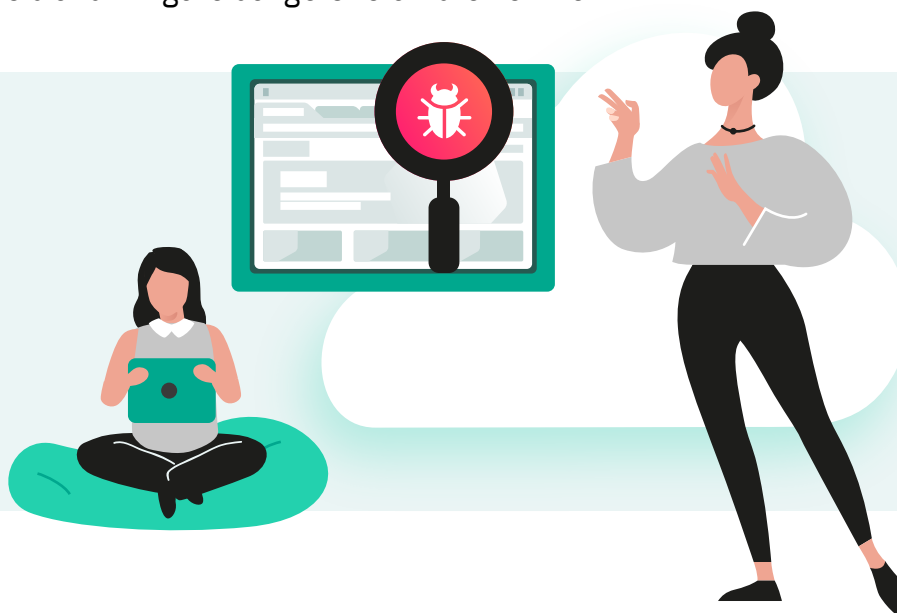
Key findings

- The time spent online in the home (excluding time on school related tasks) is on average only 1:20hrs shorter than the time spent on designated family time – 6:40hrs on average – according to parents.

- 6 out of 10 (60%) families have directly experienced or seen an online safety threat incident, with children seeing harmful content and internet addiction being the most common threats.

- 50% of parents manually check children devices, such as looking through browsing history, after use.

- 81% of parents agree they have at least partial responsibility for teaching children about internet safety.

- However, the majority (58%) of parents have spent less than 30 minutes talking to their children about internet dangers throughout their kids' childhood.

The real danger

The very real dangers facing children online are a considerable concern to 85% of parents worldwide, according to Kaspersky's latest research into the matter, in turn provoking a combination of responses, with a mix of manual checks and rules, together with one-on-one conversations playing a part in addressing these concerns.

Nowadays six out of ten (60%) of parents say they have directly witnessed an online safety threat incident related to their child. That is not surprising considering that over 98% of children will have received their first internet-enabled device before the age of 13, with smartphones and tablet devices being the most popular choices.
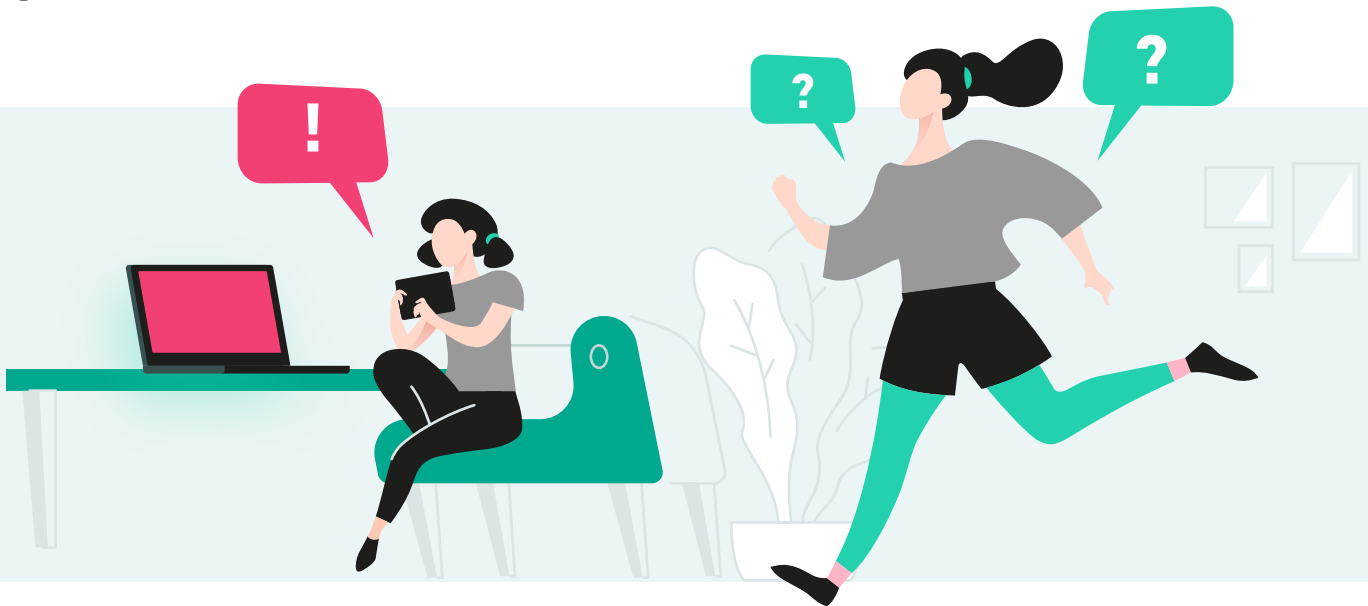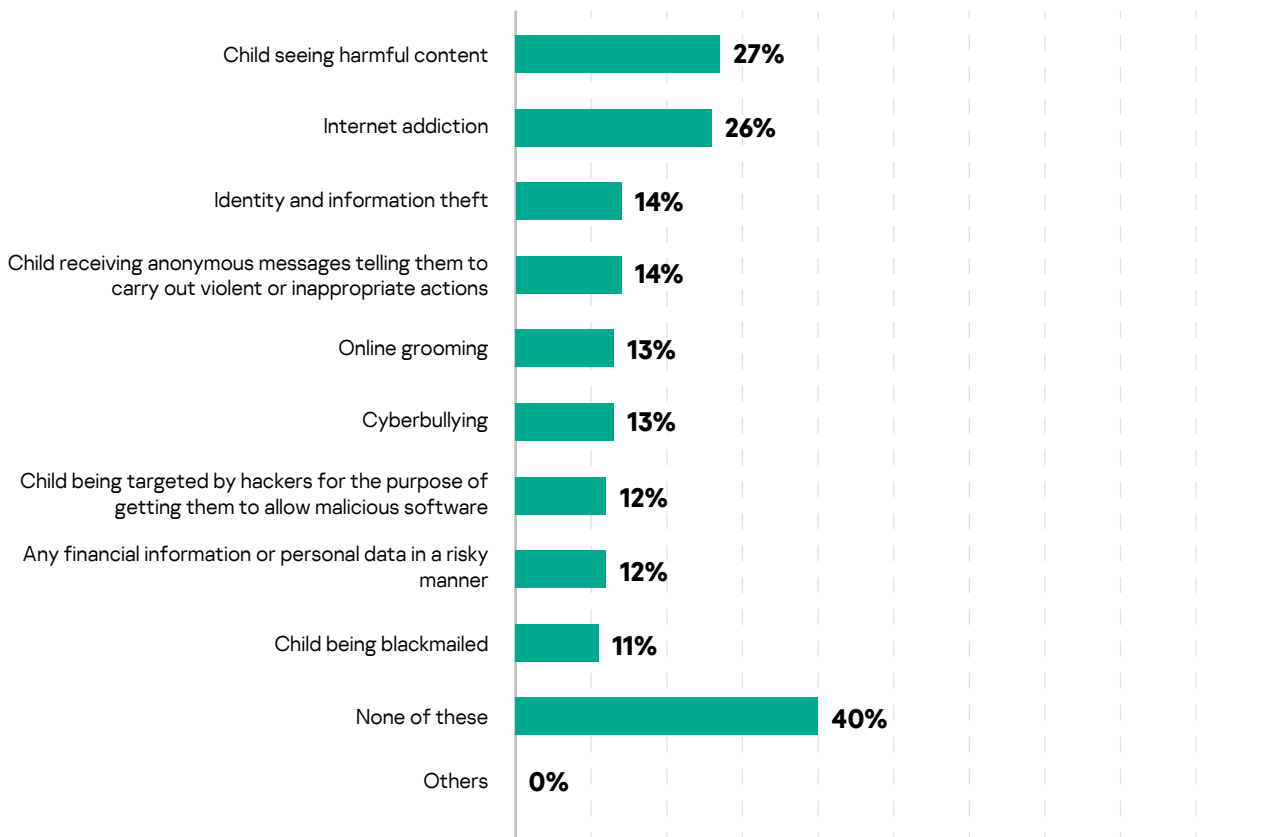

So, what are the most common threats parents should be considering?

According to the survey, more than a quarter of children (27%) have seen inappropriate sexual or violent content online. All this content can influence children as they begin to develop their own sense of sexual identity and understanding of cultural norms when it comes to forming sexual behaviors.

A quarter (26%) have experienced children being addicted to the Internet, which often leads to emotional and social isolation, becoming irritable or depressed when not online, or sometimes sacrificing sleep time to spend an extra hour online. The obvious sign that a kid has an Internet-addiction disorder is a noticeable difficulty disconnecting from being online.

Meanwhile, 14% of parents say their children have received anonymous messages – or been exposed to content – encouraging them to carry out violent or inappropriate actions. For instance, a YouTube account called TellBite, which has over 167,000 subscribers, hosted videos where Minecraft–inspired characters were involved in a school shooting. Such videos gain thousands or even millions of views, and can be concerning for parents that worry about what their kids are exposed to on seemingly safe services . Despite all this, it seems the levels of danger some parents are aware of may well fall short of the true figures.

Table 1. Has your family ever directly seen or experienced any of the following online threats?

Threat	Percentage
Child seeing harmful content	27%
Internet addiction	26%
Identity and information theft	14%
Child receiving anonymous messages telling them to carry out violent or inappropriate actions	14%
Online grooming	13%
Cyberbullying	13%
Child being targeted by hackers for the purpose of getting them to allow malicious software	12%
Any financial information or personal data in a risky manner	12%
Child being blackmailed	11%
None of these	40%
Others	0%

Respondents asked to select all options that apply

There's some evidence parents aren't aware of the whole truth connected with children's activity on the Internet. An international survey from Global Kids Online found that between a fifth (in South Africa) and three-quarters (in Argentina) of children report feeling upset about something that happened online. Meanwhile, the proportion of children who have seen sexual images during the past year ranges from about a third of all children in the Philippines to slightly over two-thirds in Argentina and Serbia.

Where does the danger come from?

When it comes to where and how parents anticipate children being at risk, in terms of apps and platforms, one element of the research might be quite unexpected. Email is viewed as one of the most prominent sources of risk, according to 69% of parents. In some ways, email is still the key to our online identities as it's used to create and verify our accounts and actions on other services.

And if the child loses control of their e-mails, it can have wide-ranging consequences like stolen passwords or other sensitive data. The second and third most concerning platforms for parents were social media networks and in-app advertising, both causing considerable concern to nearly 60% of parents.
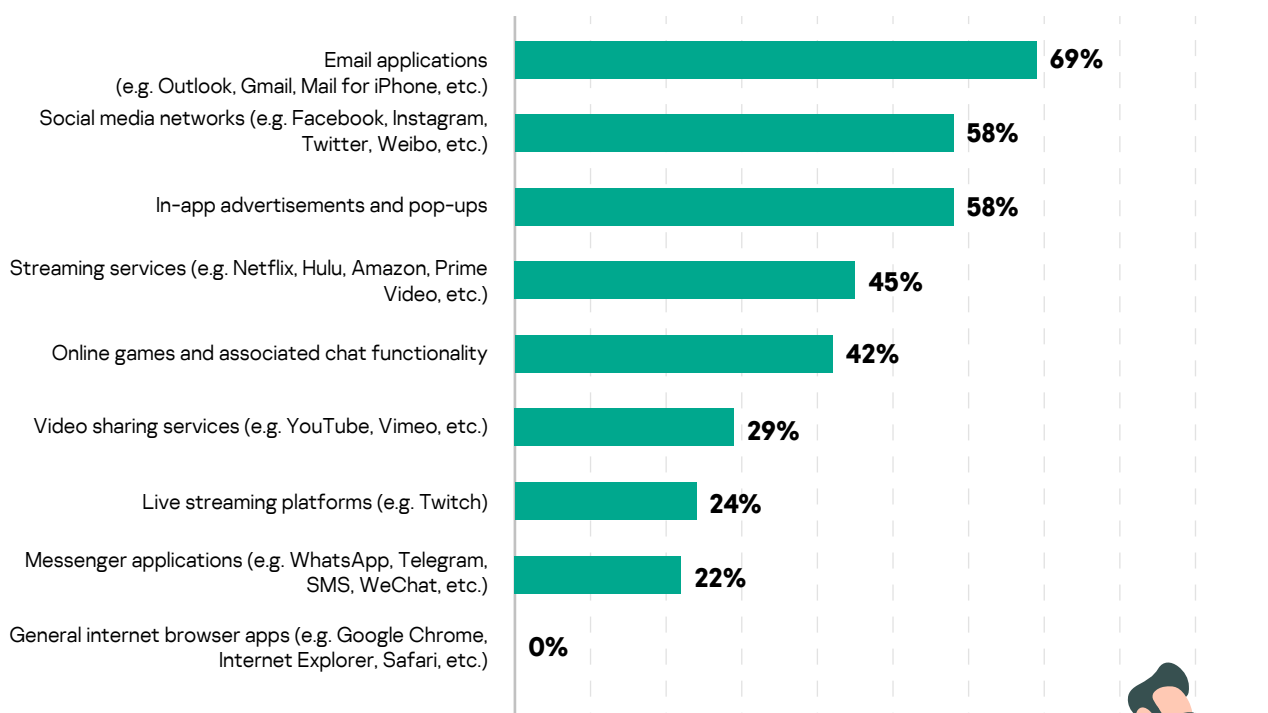
The dangers of social media, where kids live documented online, seems to be endless. When it comes to the social networks and kids the most dangerous things that come to mind are sexting and cyberbullying.

All of which are incredibly damaging, more common than people think, and should be discussed.
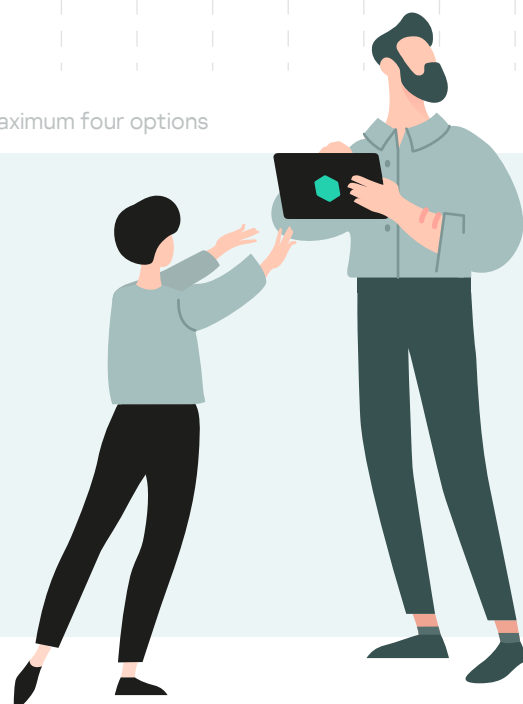
What is interesting, is how In-app advertising is producing considerable concern on two fronts. First, 'free' games targeted towards younger children often contain considerable paid content, dangled glamorously before players, and available within a few taps on an unguarded phone, or leading to unwanted nagging epidemics from children keen to experience more from their games.

Second, poor targeting frequently leads to adult content being advertised to young children. Even if the advertising is age-appropriate, campaign groups have described the techniques used by advertisers as "manipulative… and deceptive".

Table 2. Which of the following applications and services are you most concerned about your child (or children) using in the context of online security?

Application/Service	Percentage
Email applications (e.g. Outlook, Gmail, Mail for iPhone, etc.)	69%
Social media networks (e.g. Facebook, Instagram, Twitter, Weibo, etc.)	58%
In-app advertisements and pop-ups	58%
Streaming services (e.g. Netflix, Hulu, Amazon, Prime Video, etc.)	45%
Online games and associated chat functionality	42%
Video sharing services (e.g. YouTube, Vimeo, etc.)	29%
Live streaming platforms (e.g. Twitch)	24%
Messenger applications (e.g. WhatsApp, Telegram, SMS, WeChat, etc.)	22%
General internet browser apps (e.g. Google Chrome, Internet Explorer, Safari, etc.)	0%

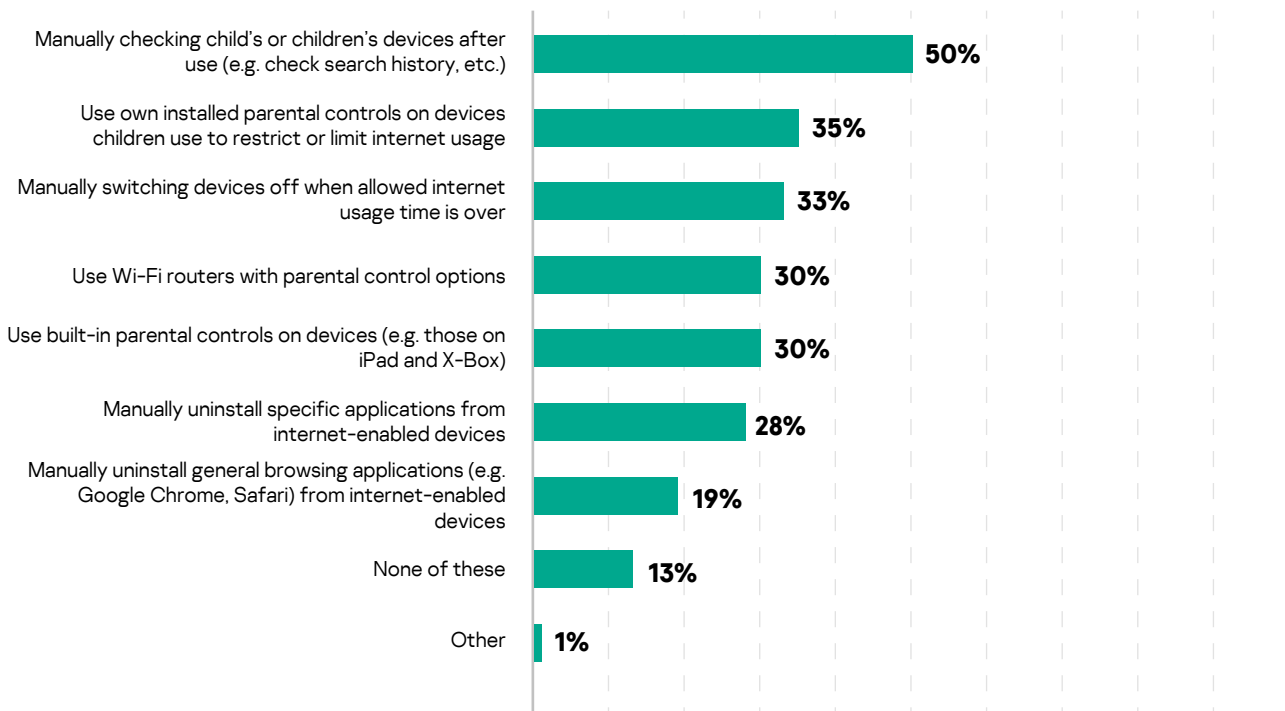Respondents asked to select maximum four options

Control and conversation

Naturally, parents are taking action to protect their children from these threats. Broadly speaking, their approach might be divided into either direct action (controls and checks), or indirect action (discussion, special warnings or advice).

Concerning manual or technology-enabled interventions, parents often say they trust their kids to act safely online, but they back this up with direct checks and controls. This is natural – an analogy might be to young children crossing the road safely: Parents might trust their children not to take risks and look before crossing, but that doesn't mean they will let go off their child's hand when crossing or let them cross a particularly busy road on their own. And sometimes you may trust your child but, similarly to bad drivers on the road, the ones you can't trust are the nefarious actors online.

Nearly all parents (87%) say they use some form of technology or manual solution to control or monitor their children's internet usage and claim they have set rules for their children around the acceptable use of their devices. They check on their children's online behavior after using devices – through, for example, checking their browsing history (50% agreed); they use parental control solutions, installed by themselves on children devices (35%); and they manually switch off devices when internet time is over (33%).

Table 3. Do you use any of the following technology and manual solutions to control or monitor your child's (or children's) internet usage?

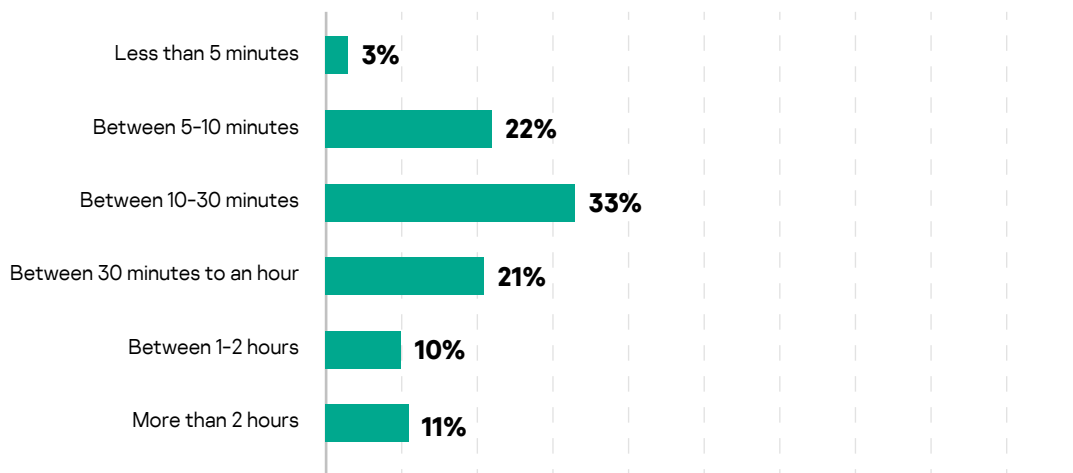| Option	Percentage
Manually checking child's or children's devices after use (e.g. check search history, etc.)	50%
Use own installed parental controls on devices children use to restrict or limit internet usage	35%
Manually switching devices off when allowed internet usage time is over	33%
Use Wi-Fi routers with parental control options	30%
Use built-in parental controls on devices (e.g. those on iPad and X-Box)	30%
Manually uninstall specific applications from internet-enabled devices	28%
Manually uninstall general browsing applications (e.g. Google Chrome, Safari) from internet-enabled devices	19%
None of these	13%
Other	1%

Respondents asked to select all options that apply

Parents also confirm that they need to adopt more personal, verbal approaches for creating safer internet experiences: talking to children about potential dangers, and what they should do if anything happens.

The majority of parents (81%) agree they bear at least some responsibility – alongside schools and teachers – for setting out the risks to their kids, and the best way to respond to threats. And most parents (62%) say they conduct small, informal conversations with their children regularly, as well as discussing the matter with them as and when incidents arise.

However, they are not currently dedicating a lot of time to this: 58% of parents have spent less than 30 minutes in total, through their kids' entire childhood, talking about internet safety. Only 11% say they have spent more than two hours talking to their children about the dangers.

Table 4. How much time in total have you spent discussing online safety with your child or children?

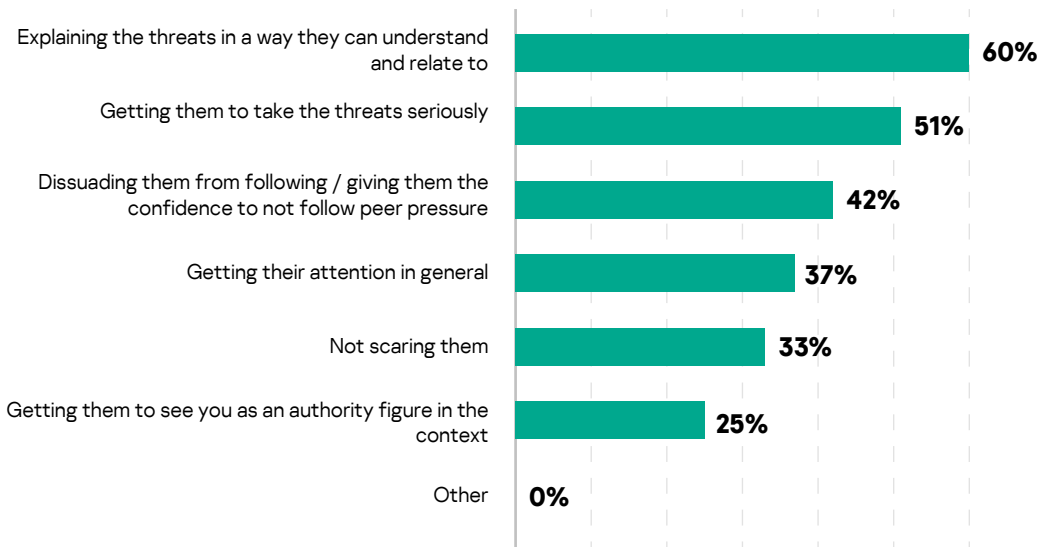| Time	Percentage
Less than 5 minutes	3%
Between 5-10 minutes	22%
Between 10-30 minutes	33%
Between 30 minutes to an hour	21%
Between 1-2 hours	10%
More than 2 hours	11%

There is at least one clear reason for this unfortunate lack of necessary communication. These are a number of difficulties connected with these conversations.

Parents often find it hard to explain threats in a way their children can understand and relate to, as 60% of them noted. Perhaps by extension, they find it hard to persuade their children to take the threats seriously (if the threat isn't explained well, then how can children be expected to be wary of it?). And, like every parent ever, the parents find it very tricky to dissuade children from giving in to peer pressure when it comes to risky behaviors.

Table 5. What do you feel is the biggest challenge to having conversations around online security with your child or children between the ages of 7-12?

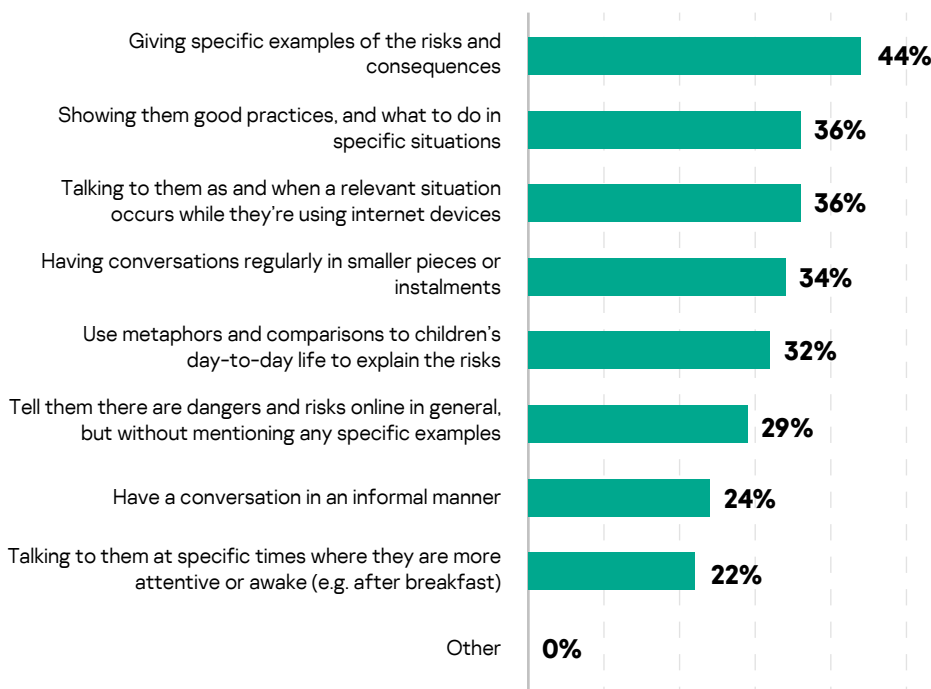| Category	Percentage
Explaining the threats in a way they can understand and relate to	60%
Getting them to take the threats seriously	51%
Dissuading them from following / giving them the confidence to not follow peer pressure	42%
Getting their attention in general	37%
Not scaring them	33%
Getting them to see you as an authority figure in the context	25%
Other	0%

Respondents asked to select maximum three options

The most effective ways

Fortunately, the survey also helps clarify three of the most effective tactics parents can use to help their children understand the potential dangers lurking on the Internet. These should allow parents to plan conversations ahead of time, allowing them to have more successful, impactful discussions.

Table 6. What do you think are the most effective ways to have a serious conversation with your child or children about online safety?

Category	Percentage
Giving specific examples of the risks and consequences	44%
Showing them good practices, and what to do in specific situations	36%
Talking to them as and when a relevant situation occurs while they're using internet devices	36%
Having conversations regularly in smaller pieces or instalments	34%
Use metaphors and comparisons to children's day-to-day life to explain the risks	32%
Tell them there are dangers and risks online in general, but without mentioning any specific examples	29%
Have a conversation in an informal manner	24%
Talking to them at specific times where they are more attentive or awake (e.g. after breakfast)	22%
Other	0%

Respondents asked to select maximum three options

Family Campaign Report

The first of these is to give very specific examples of the risks and consequences. Conversations that discuss dangers vaguely, or through euphemisms, with talk of 'bad people' and 'naughty pictures', are almost doomed to be unconvincing. The second part of the approach, which relates to the first, is to describe exactly how children should behave, in general, and when potentially dangerous or upsetting situations arise. The third part to best practice lies in relevancy. Discussions are most effective when they happen as and when situations occur when children are using their devices.

How can parents best protect their children?

To conclude, the prevalence of disturbing and dangerous incidents revealed makes child safety online an urgent, thorny, global problem. As we have shown, 60% of parents have directly witnessed a direct internet threat, and the actual proportion seen by children may be even higher.

Cybersecurity software like Kaspersky Security Cloud or Kaspersky Safe Kids can help protect against some threats, but an equally vital safety measure is communicating with your children.

Currently, parents aren't putting enough time into communication, despite their awareness of the threats. The majority have spent less than half-an-hour discussing the topic with their children, over their entire lifetime to date. But planning these conversations ahead of time can make them both easier and much more effective. By pooling their wisdom, we found parent's advice must be specific, practical and timely, and delivered in a way that is useful and memorable for children.

Thus, technological solutions, watchfulness and the ability to offer practical, timely guidance each have a part to play, making a combined approach the best route forward for concerned parents.

To learn more about how to keep your kids secure on the Internet, read renowned psychologist's, Emma Kenny's, post with her top tips on tackling online safety conversations here.

kaspersky

www.kaspersky.com