Internet Society

KIDS, THE INTERNET & COVID-19:
HOW TO KEEP OUR CHILDREN SAFE ONLINE

APRIL 9, 2020
(https://livestream.com/internetsociety/onlinesafety)

>>NOELLE FRANCESCA DE GUZMAN:: Good morning, good afternoon, good evening to everyone joining us from different parts of the world. We have a few people joining us, we'll give them a few minutes to let them get settled before we start. I'm seeing more people joining. I hope you don't mind hanging around for another minute or two before you hear from me again..

All right. I think we're ready to go. Good morning, good afternoon, good evening again for everyone tuning in.

Thank you for joining today's webinar, Kids, the Internet & COVID-19: How to keep our children safe online. Me and my colleagues, we're excited to be here with you todays a global organization, we at the Internet Society has worked for Internet Society for 30 years now, we hope that we find good tips in this webinar useful.

Before introducing our presenter, some housekeeping, this webinar, it is being recorded and we're also being live streamed on YouTube -- sorry, Facebook Live right now. The recording will be made available on our website after the webinar and you are welcome to watch it, share it with other parents, with other people who you think may be interested. You can also download the presentation slides now at the event page and we'll close that very shortly -- post that in the chat box, post your questions on the chat or in zoom, there is a Q&A button you can press. We will start to answer them after the presentation. Our presenter today is Aftab Siddiqui, he's our senior manager for internet technology. He's also a dad to two boys, one of whom is now very active online. This top, it is something close to his heart. Aftab Siddiqui, take it away u.

>> AFTAB SIDDIQUI: Hello, everyone. Thank you for the introduction.

Interesting times! So let me start. As explained, I'm Aftab Siddiqui, some of you in the region know me for a long time, I have been a part of this community and working with you all for more than a decade now.

Let's talk about something which is quite interesting to know for most of us, most of us means parents. We're currently living and working in an era of unprecedented time. I know you have heard this statement probably a million times in the last couple of weeks. Unfortunately, you will hear the same statement for a few more weeks, God willing everything will be fine soon. The challenges we're facing right now, it would have been unimaginable not too long ago. To be honest, nobody expected to go through in their lifetime. The way we're working and living in self-isolation and keeping social distancing, the term which we never heard before, we have to follow it now. You didn't plan for it until you had to just a few weeks ago. Some people were in even disbelief that it is not going to happen in their city, in their country, but to be honest, look, most of us, if not all are working from home, or staying most of the time at home. We have our families, they're at home, we have our children at home 24/7. It is good, it is amazing, you are able to spend more time with them, but there are challenges. During this time period, when our way of working has to be different, as well as we have to be resilient in order to deal with stresses we're feeling and issues we're facing and going through at the moment. Some of them, they're pretty new. We never faced it in the past. We need to understand, we need to adapt accordingly. Our home life, work life has merged together, it is a very thin line between both now because we're working from home. So as for our kids, their play time, school time, their -- their whole time has merged together as well. Why, the schools either have been closed in many places or they're suggesting to take online classes even if they're open. Sometimes you just have to watch your kids schoolteacher watching videos on Facebook to teach pupils. So it is very different. It is from traditional books, reading, filling up worksheets, things have moved to online instructor base or self-paced training or self-paced learning. It all means one thing, there are more and more screen time for the kids. This is why we're talking about it today. It is not like it happened preplanned, it happened all of a sudden. Not only there are many more additional kids joining the online world for the very first time, but the kids who were familiar with the online world are spending more time with their with devices and on the internet. We know it will be a different world altogether moving forward. It is better for us to understand and adapt. Just like we have helped kids with introduction in the physical world it is important to show them how to be safe on the internet as well. I have heard one statement quite recently that when you first teach your kids to cross the road, first thing you teach them is hold my hand. Internet superhighway is actually more than crossing the road, make sure that you're holding the hand when you're introducing them to the online world.

The first thing, do you know what your kids are doing online? How they're spending their time online? We all have seen the biggest downloads in South Asian region, it is tech talk, Call of Duty, Fortnight, all of these games, everything they have millions and millions of downloads in just Southeast Asia and around the world. It is just massive. People are spending more time on social media, kids are spending more time on games and whatnot..

Studies show most parents don't know what their kids do online. Probably you know it well, but you don't know completely, some parents don't know at all. It is a mix. 70% of online youth in India spend more than 5 hours on the internet. Probably they're studying four hours but one hour they're doing something else. Are you aware of that? Probably not or probably you do know that. 70% have posted their contact details like email, phone, home address. Are you aware of that? If you are, then good. 5% have met someone in person that they met online. 63% of you do not turn on the low -- turn off the location of the GPS which is interesting these days, 60% of parents don't know what their kids view online.

Well, these are all numbers and statistics. Behind those statistics, they're real people, real parents, real kids.

If you are joining this session, it means that you are one of the concerned parents or concerned party in this scenario. That's why you want to learn more. Our job is to share more details with you so that you have -- so that you have a better understanding of how to handle the problems.

What are some of the risks children face online? There are many of them. Let's try to summarize all of them in three different categories. What do they see actually? Are they seeing cat videos? That's fine, cartoons? Watching something related to studies? That's all good. Are they watching some hate content? Are they watching something which is triggering violence in them? Are they watching something which to be honest they're not supposed to? Anything which is age restricted, something they shouldn't be watching, right. So this is one thing. What they do afterwards? Are they posting something hateful? Are they posting something which is dangerous for them? Are they posting something which can be seen as bullying? Are they posting something which is totally irrelevant for them but can cause problem for other people? The last, most important thing, who they talk to. I mean, online world gives you an opportunity to connect with everyone. Everyone means there are bad people outside as well. You need to know who they are talking to and what information they're sharing with them. These are major categories of online problems that your children can face.

Knowledge is power. The best way to find the details is talk to your children, talk to your kids. Tell them, I gave you an example of crossing the road, talk to your children about the online safety, what they can do, what they cannot do. You have to set some boundaries, okay, fine, you can make sure you don't download anything without my permission, make sure you don't do this without my permission or telling me that you're going to play this game. Set some boundaries.

Choose age appropriate apps and websites. These days it is very clear at least on the apps, most of the apps, that what age group it belongs to, set boundaries that you can use apps which are for you only. I mean, Facebook has a restriction of 13 years to create an account. If you're younger than 13 years, if -- you can create an account for your kid, you can use it, but not allow them to play with their own IDs, things like that.

Set privacy settings. It is a very broad statement. Set privacy settings together. You have to sit with them. Probably they know how to use internet better than you, probably. You can learn from them while setting next to them. Justifying out what are the options available that you can use to secure your information, what information you can you are giving to the world. Show them how to keep themselves secure, whatever they do in the real life, they should be doing online as well. Again, I was talking to someone, trying to explain something, I said you don't go out on your balcony and start yelling and screaming about your personal information because that information should remain private. Why are you not doing the same practice online? It is the same as telling everything to the stranger walking on the row. The online world is not different.

What you can do to keep your kids safe online? Set parental controls. There are many people online right now. I have one question to you. How many of you know that you can actually set parental controls? You can set safe surfing on Google search or on Bing, on any other search engine? If you know, that's good. If you don't know, you should know now. Parental controls, it is most important.

Supervise your kids. Don't just let them use internet on their own. Make sure that you -- if they're doing homework, what do you do? Of course up help them out. This is how you do it. You do the same thing while they're online. Teach them to behave responsibly. Online world shouldn't be very different than the real world. If you teach them how to behave while they eat, while they talk to elders, while they talk to their parents, siblings, teach them how they should be behaving online when talking to others. It's a big world out there. In the home you can control things, but when you're online, it is hard, you have to teach them, again and again and again, it is an ongoing process, you cannot just say, well, fine, I told you once, I think you have the message. It is ongoing. You have to make sure that you keep on sharing this information again and again. Sit down every now and then.

What you can do to keep your kids safe online, everything online is permanent. There's one statement which we are quite familiar, it is whatever you share online will remain forever. There's no way you can take it down. Even if you remove it from your own account, you have no idea how many people have copied it, you have no idea how many people have viewed it already, and you have no idea how many times it has been circulated on the internet. You have to be a role model for your kids. If you yourself are sharing information on your Facebook, on your Twitter, on Tik Tok, whatever application you are using, even in email, if you are doing these things yourself, you will not be able to set a role model for your kids. You have to be vigilant in what you are doing -- kids pick up from their parent, from their elders. You have to be able to model that.

Sometimes it is absolutely okay to just be offline. Turn off all of the devices, pick up something, and play. For me, I have a handful of puzzle games which I play with my kids. There are other things which you can do.

We can play cricket inside of the house, we all know how to do that, all South Asians, the crazy cricket fans, we know how to play one tap cricket at home, we have done it from early childhood. Do something which is not online. Take them off the screen, make sure that you are off the screen as well. Again, be a role model.

There's one thing you should learn today other than what we have already discussed, and what I have said so far, it is nothing out of -- nothing extraordinary, these are all things which most of you already know. We must learn something new as well. This is an important issue to remember, if you don't know today, learn it today here, and research more about it, and that is encryption. Encryption is one of the most powerful tools parents can use to help keep their kids saith online. How it is used, it is simple, it is used in end-to-end encryption. Again, if you go back to the balcony example, if you're talking to somebody on the road, on your balcony, you're not talking to them and sharing personal information. You don't know how many in the middle are listening. Why would you do the same thing online, you're not going to send a message, unencrypted message, unencrypted message, it is something that's in plain English, in your language of whatever is origin. It can be viewed by a third party. What encryption does, it takes a message, transforms to scrambled words and sends to the recipient, the person you want to talk to, share the information with, it will be decrypted into the actual message. The recipient, this is what you say. It goes both ways. What's happening is, both devices, phone, laptop, PC, they are sending and getting information, both understand easily and no one in the middle, they can read anything. Whatever they see, it is just scrambled words, that can be -- that person can use that information in a pad way. If you are talking to your bank, that person can see your money. You have to tell your kids as early as possible that how -- how encryption works and the significance of encryption. There are many tools which people use today to achieve this encryption. There are tools like Signal, cap telegram, all provide end-to-end encryption. Whatever message you send from your mobile phone can only be read by the intended recipient. Anyone reading the message in the middle will never be able to understand, it is encrypted. It is unreadable for anyone else other than the intended recipient. Make sure you use applications which offer encryption. It is not that hard to find out if that application offers encryption. You can go into the details of that application before you start using it and it will tell you if they're using it, any encryption or not.

Not just application, make sure whenever you log into the website or whenever you are looking at a website, a webpage, look for a lock sign. If the lock sign is there, it means that the messaging between you and the website, from where you're downloading the information, fetching the information, it is encrypted. Nobody in the middle is looking at your information. If it is a bank, don't log into it if there is no lock sign there. Whether it is a green lock, a black lock, just make sure that the lock is there. If it is a broken lock, it says not secure, there is a red sign, red is always wrong, stay away from it. Make sure that the lock is there. Another thing, set a strong password. What our kids do usually, they set the date of birth, first name, last name, thankfully all the apps and websites are moving towards more secure passwords, they ask you add numbers, add upper case, lower case, they do not allow you to set weak passwords. Tell them I didn't this is necessary. You have to do the same thing and then you'll be able to convince the kids to do the same. Make sure that the passwords are long and it is different for every application. Don't set one password for everything. If you're doing it yourself, please change your habit. Say the same thing to your kids.

Just in the last, I would say, create a checklist. Here is a starting point. you can add more things to it, you don't just have to follow this one. You can add more. Create a checklist, make sure you follow the checklist every week. If it is too frequent, every fort nightly, every month. Follow this. So that your kids do know, again, you have to follow a certain boundary. Again, if you go to the list, there is nothing extraordinary in that one. It gives you a background, it gives you an understanding of what is there how to protect yourself. The most important thing, you have to talk to your kids as often as possible. Security, you have to understand why you need security. You need to understand why it is important before you implement it. This is all I wanted it share with you, having a kid whose using online classes now, it has become more important for me to teach him as early as possible. I never knew that -- I never had planned for him to be using it in the preschool, but he is. Now all the assignment it's, they're online. Now I have to start teaching him how to set a secure password as early as 4 years old. This is all from my end. If you have any questions, please start doing it, start typing it in the Q&A.

>> NOELLE FRANCESCA DE GUZMAN: Thank you for tuning in. We have received some questions on the chat. I think along the way we have addressed some of the questions through the presentation. If you do have any more questions, please keep them coming. We'll be sticking around for another half an hour to answer questions from participants. Now we have come to the Q&A part, I will turn it over to the rest of my colleagues on the call to give us even more tips on protecting children online based on the questions that have been posed. So me and other colleagues will be asking

those questions to them and I hope -- we may not be asking verbatim the questions that you have, we're trying to consolidate them by topic to make it more efficient. One of the questions that we have had, it is a lot of the kids are now using Zoom for school lessons, et cetera. But we have also heard some news about some security risks and privacy risks around Zoom, is it still safe for our children to be using Zoom for school and for other activities.

Anyone want to take it? Do you have any advice?

>> AFTAB SIDDIQUI: Sorry. I -- can you read that question again.

>> NOELLE FRANCESCA DE GUZMAN: No problem. So a lot of the kids now are using Zoom, I believe parents as well, to do schoolwork, to have school lectures, but we also heard that there's been some security issues and privacy issues with Zoom recently. Would you still recommend that we use Zoom at this point in time and is Zoom still safe to use for our children?

>> AFTAB SIDDIQUI: We're using Zoom right now. We all have heard what was happening with Zoom Bombing, strangers dropping into classrooms and -- strangers dropping into classrooms and doing inappropriate things. We have heard that. That's real. It is not a made-up story. It was real.

Without supporting one platform, what happened recently, Zoom took that feedback nicely, they started giving -- if you are using Zoom, you must have seen so many updates came in in the last two to three weeks. They are fixing most of the things. They cannot fix all of the things. Again, they have added features, but you have to enable the features, you have to make sure that you're following the guidelines.

If somebody from my colleagues, if they can share that link with Zoom recently, they published which gives a quick guideline that these are the features to enable, disable to make sure that nobody, no strangers can jump into any conversation, make sure that -- they also say -- and we're also doing it, if it is a bigger session, create it the way we have done it hue here, so only the panelists, those with the right to share the videos, the right to speak can only speak or share the videos, not anybody else.

So use the right tool, use the right measures so that you can use it properly.

Every platform has pros and cons. If you think is Zoom has issues, you can switch to other platforms as well. Again, security features, they are there in every platform. We all need to understand how to use those security features, to make sure that it is not insecure for our kids or for the school as well.

I hope that answers your question.

>> NOELLE FRANCESCA DE GUZMAN: Thank you.

We have another parent here asking if we have any recommendations for opensource parental tools. Anything?

>> AFTAB SIDDIQUI: Let me answer a couple of things.

If you what DNS, the moment you write something on your web browser, www.com or something else, it is put into the DNS, without the details, there are some DNS services which provides parental control, parental locking. At home I use Open DNS. It is free. It is from Cisco. Look it up, use that.

There is another similar service from Cloud fare, they provide the services for families. It restricts all the websites which are questionable, whether it is phishing, whether it is adult in content, anything which is deemed not appropriate for families or kids. They block it anyway. We use that at home. I would recommend using it. In my personal experience, it works well. If you want to use it, talk to someone -- if you don't know how to set up a DNS in your router, in your laptop, your iPad, talk to somebody that understands that, talk to a friend, colleague, siblings who will be able to help you out. Try to use that. It is very important. It enables safe searching on the browser, on the search engines, it is Google or Bing, you can enable that, you cannot search something which is inappropriate, even with the open DNS families shield, Cloud FARE content restrict services, you can still search things in Google but if you use face search options, you will not be able to search. Try to use that, it will add more control to your household.

>> NOELLE DE GUZMAN: Thank you. We have another question here on if there are any apps that would restrict inappropriate content. I think we have talked about random controls. There was also a question on software. I think we know that there are surveillance apps marketed out there for parents to monitor what the child or the children are doing online. Is this something that we can recommend to parents?

>> AFTAB SIDDIQUI: Okay. Being a parent myself, it is a personal opinion. I would say it's a strong personal opinion. I wouldn't do that. The first thing for me, talk. Talk to your kids, make sure they understand. I hope and believe you don't have to go to that extent where you don't have to monitor the activities of your kids in that manner. You can still monitor what they're doing, the option I gave you, open DNS, the family fair option, they give you a complete list of what was happening from your household, what website they launched, what they have done. You can have a conversation with them. Rather than going into the full- on surveillance mode. That's my personal opinion. People can defer and choose whatever they want. There are several softwares that can record the screens, they can record keystrokes, everything. In my personal opinion, you don't have

to go to that extreme if you keep on engaging with your kids on daily, weekly basis.

>> NOELLE DE GUZMAN: Thank you.

We have another question here, is there a particular age group where you would start online education.

>> AFTAB SIDDIQUI: I didn't plan for the online education for my preschool kid. It just happened. Now I have to tell him, that -- how it all works, how -- so the other day I was teaching him how to login, it was a password, the password can only be put in by a parent. So he was frustrated why he can't login. And then I had to tell him, this is how it works, you can't login yourself. Different times, I would have planned it for a couple of years later. Now you have to do it today. I think it is a good time to start teaching your kids if you haven't done so, right now.

We are spending more time at home, we have time, it is a luxury, it used to be a luxury, it is not anymore, I hope so. Try to understand this with your kids, look it up I would say. No age restriction, start as early as possible.

>> NOELLE DE GUZMAN: Thank you.

We have another question here on -- I think it is a follow-up question on is it posting something possible, agreeable for parents to monitor children's behavior. We have touched on that. I would like to add in that the researchers about your child behavior online as well as institutions like UNICEF, they stress it is virtually impossible to monitor everything that your children are doing online. What you're more inclined to encourage, really it is for parents to talk to them. If your children trust you, then they're more likely to have an open conversation with you about what they're doing online. If you make them aware of the risks involved, because trust me, even teenagers, they don't know that there is such a thing as online grooming, they don't know that grown men will victimize them, having that conversation with them, having them not just having it one time, but in different contents, having it in at home, in school it would really help. It is really the foundation of -- it is the foundational mechanism that is most effective in protecting our children.

Let me also have a look at the questions, the remaining questions. There's a lot of kids that start their online exposure watching YouTube. Is there any recommended amount of time, say if you have a toddler, starting at 3, 4, 5, that starts to watch YouTube, is there a recommended amount of time of how much time they should be allowed to go online, go on YouTube and watch favorite shows?

>> AFTAB SIDDIQUI: There are other parents on the panel as well.

I was reading some of the questions. I saw a similar one.

It's usually up to you, whatever you think. For me, any single sitting, no more than 30 minutes is must have enough. For the YouTube, so YouTube also offers YouTube kids. It is a filtered version, providing videos which are good for kids. You can set up passwords in it, then you can set a limit for how long that will run. After 30 minutes, it will stop. That's it. It is not going to work unless you put a password into it. If you have set up the password, then it is up to you if you allow it or not. That means you may have to delete the YouTube from your phone, either from your phone if you're giving the phone to the kid or from the same iPad, tablet you're sharing with your kid. That is a sacrifice you have to make.

I have learned myself, it's worth it. It works very well. It doesn't give you a chat option. It doesn't give you unnecessary ads, and it is much cleaner version and you can have a history of what your kid was watching. They cannot remove the history unless you put in a password as well. These are things that you can do. Again, it is more about trust. If you give a iPad, a tablet, a phone to a kid, make sure that they are looking at a time clock as well so that they don't use it for endless hours.

>> NOELLE DE GUZMAN: Let's give Aftab a break. I have another question and I'll pose it to another colleague.

It is rather a trend these days for parents to be giving their kids their own devices at a young age. Is it something that we think could be appropriate? If we don't give the kid the device, then they see their friends having devices and then they go back to the parents saying how come my friend has a device, I don't. What would we recommend? Is there an appropriate age for starting to give our kids devices of their own? I think I'll pose this question to another colleague whose a parent in the group, and that would be Raj.

Do you have any advice for that?

>> RAJNESH SINGH: Hello. Can you hear me? Sorry about that? I was a bit excited with the question!

What we can see, I think, it is that with the current pandemic, a number of schools and a number of countries have started to move classes online. So there's a couple of things we have to look at in trying to answer the question. That's one.

Number two, as was rightly put, there is a lot of peer pressure of kids, others around your kids, they may have devices of various sorts. Then the third thing, of course, a lot of schools are looking at implementing online learning digital learning or digital classrooms. Not giving them a device, not letting them have access to a device, it is not really practical anymore as we move to a very digitally-based society. I think in India, you probably give access to the kids, it is probably better, however you need to set very clear boundaries and set very clear ground rules as to what and how they should be doing on the internet and what sort of things he had should be using. There are a number of questions coming up in the Q&A which in various ways, we're asking the same thing in terms of how quickly, at what age do you give kids access, how do you ensure they go to safe sites, how do you ensure that they're not looking at things that are violent, abusive, so on, so forth. An important tool, of course, to use is parental locks, some operating systems have it built in, phones, tablet devices as well, some of them have a kid safe mode which you can enable, and then, of course, you hand it over to the child so that you know at least these sort of places they go to, using the device, it will be filtered out to some extent. After using safe DNS, which prefilter content based on the age appropriate content, that's another way to do it.

The fact of the matter is that where we are today, we really need to find the right balance as parents of kids who are probably in some ways more tech savvy than we are. You know, not trying to stop them building things which they want to do, ensuring that what they do is within set boundaries.

There is a few other questions, so I'm answering a number of questions, many were interrelated. There was another question that we sort of touched on as well, you know, say how do you have the trust between the child and you as a parent when the child may want to go and access something and you say no, you can't access that. So what I have done in my family circle, you know, have a conversation with the child, say, look, I will give you the access, but then you also have to be responsible. Trust and responsibility, that's two key things that we need to discuss with the child and say, look, I'm happy to give you access, but are you going to be responsible in the way you use it and what you do with it? That's not 100% fixed, you may get in a situation where some kids will still go and look at other things, so on, so forth. Having the conversations on a regular basis and building that same trust levels that you have in the offline, physical world with the child, it will go a long way to try to ensure that whatever they do, wherever they go, online, it will let you have some semblance of risk control from that perspective. If you think you can stop them from doing anything online so, on, I think that's getting harder and harder every day. So being able to have the trust-based discussion with the child and ensuring they understand the responsibilities that they're given in having access to the internet, that will go a long way to help solve some of this issue. Thank you.

>> NOELLE DE GUZMAN: Thank you.

We have a question here for asking for recommendations on safe websites to visit. We don't have -- I don't have a complete list at the top of my head. You can look at websites like a security firm with a dedicated section for kids and websites like that, they would have a list of websites that are age appropriate depending on the age of the child.

There's another question here aside from giving children their own devices, should parents create their children's social media accounts and upload pictures of their children? What I will say about this before passing it on to my colleagues, there are age restrictions, age limits to say Facebook, Instagram, they would require that you be 13 years old or above to open an account. Now, of course, this can be -- it is not very strictly implemented. If your child would say as a 13-year-old, yes, then they can open an account. There are parents in the group that have any recommendations on this, opening your children's accounts e-mail, social media for them? To make sure maybe to have the right settings in place.

>> RAJNESH SINGH: I'll try to answer that.

There is a number of social media sites with age restrictions, of course, there is no solid way to abide by them in a manner of speaking. You know, in terms of setting up the device, if you feel the child should have access to the social media, some of it goes back to the comments I made earlier. You know, you need to be able to establish the trust relationship with the child. I think parenting in today's day and age is different than it was for example when my parents were bringing me up as a child. Things have changed. They will continue to change.

I think we have to have a bit of a reset in how we approach parenting to start off with.

Then having the discussion with the child, saying, if you want to go to this, use this particular social media app or service, discuss the risks that possibly will be there. At the same time, you need to be also very firm with them to say, you know, if they feel that they're getting bullied online for instance or getting exposed to material which they should not be -- which they should not be willing or listening to, that they should be able to discuss it. So this goes to how the mode of parenting also needs to change. It is not that hard and fast way that I know my parents brought me up which was the stick system, you know, you do something wrong, you get a good whack across your backside. Those days, they're gone to a large extent. I think you need to be able to build with the child, as a peer, of course you're not a peer, you're a parent, you need to see how you can change the dynamics. It takes a lot of conversation, a lot of discussions with the child. You can't do it for 2 minutes by yelling at them once a week. That won't work.

It literally has to be daily conversation to see what they're doing and how you can ensure that they're safe in that manner.

>> NOELLE DE GUZMAN: Thank you.

There is a couple of questions here about what is the appropriate limit in terms of the number of hours a child can spend online every day. Would parents in the group have any recommendations for that? Is 15 minutes a day enough? Is 1 hour a day enough?

>> RAJNESH SINGH: I'll try to answer. Others can jump in as well.

There are a number of studies that are talking about screen time. Some say more than 2 hours is bad, some say anything for more than an hour is bad. There are different points of view. I think anything that goes over 2 hours a day is probably getting into a bit too much. The way that I have tried to do is to say that, you know, you have to take a break. The break has to be to do something totally different, taking break doesn't mean checking email, watching TV instead, it has to be something different, taking a walk, playing a game, going out in the garden or something, going outside for a while or having some sort of physical activity.

Continuous use will obviously cause other issues, what I have seen again within my family, you know, once the screen time, for example, it may be gaming, watching videos, whatever it may be, when that starts going into the hours, the behavior of the child also starts to change. Over time you will see they'll continue to change. You have to instill discipline in that child and say, look, you need to take a break. It usually means you have to say hey, have you taken a break? What did you do? Read a book for instance. So that's some thoughts I have. Perhaps others will have some ideas.

>> NOELLE DE GUZMAN: Any other suggestions from other parents in the group? All right.

Let's move on to the next question. There's a parent wondering what is the role of social media or what role can social media play in keeping our children safe. I think we have already touched on social media platforms making tools available for parents to try and kind of coral what their children can see online. Is there anything else that we think social media is doing that we have not touched upon yet? Aftab or Raj maybe?

>> AFTAB SIDDIQUI: It is hard to give a short answer. I don't know. The responsibility, you can't just -- of course -- our expectations are -- our expectations, they are there, the platform should be doing things.

At the end of the day, you have to make sure that you -- I mean, I was responding to one of the questions on chat as well. You can do things to help understand the kids, the consequences. You can help them understand what are the real life consequences of what they're doing online. There are numerous case studies, there are numerous real life cases which you can explain to them. Okay, if you do this, you know, this is what happened actually. Sometimes the very innocent mistakes they make have real life consequences, platforms can do a lot of things. They are doing in some way or form, they should be doing more, but what is in your control, you should be doing it.

It is very hard to answer this one. It has a very multifaceted answer I would say. Anyone else want to jump in? I would be interested it hear.

>> NOELLE DE GUZMAN: Raj, did you want to --

>> RAJNESH SINGH: No, I was --

>> NOELLE DE GUZMAN: It is the role of social media and protecting our children.

>> RAJNESH SINGH: Not everything on social media is bad. Obviously there is a lot of good content out there as well. I think you need to try to balance that out as well.

The question I think, the answer, would social media, would it give the child access to, I'm in the aware of all of the social media apps having parental controls, the operating system, they may have parental controls, some apps have parental controls, I'm not sure that all social media apps have parental controls built in, that in itself is becoming problematic. I think you have to look at it from the perspective of, okay, is the service, the app A, B, C, which one is the more kid friendly one? If you then decide none of them are kid friendly, I have to give them access to Tik Tok, Facebook, whatever else there is then it goes back to having that conversation with the child and say, you know, what are you using it for? It also can extend to hey, what did you do today on it, what did you see? What did you do today? If you ask the questions every day, the child knows that you're interested in what they're doing online as much as you are interested in what they're doing offline when they go to school, meet their friends, going to school events, whatever else it may be.

I think I have sort of repeated this a number of times now.

The key thing I think for me, or the key suggestion I have, it is that you need it keep on having this conversation with children.

If the conversation becomes very -- you start acting as a hard parent, then you will see that the child will start hiding things from you, as they do in the physical and real world. You should not treat online anything different to the offline world. Just like you teach them not to do bad things to other people physically, same thing applies online. It is just trying to, you know, bridge those dimensions between the offline and online worlds and ensure that you're having similar conversations, giving them similar advice and wisdom so that they themselves can, of course, lead better lives.

>> AFTAB SIDDIQUI: Allow me quickly two points: One, it is, again, what you do in real life, you have to do in the online life. You don't -- you don't have to tell your kids that throwing the stones at someone is bad. They know it is bad. Right? So -- because they learned it from the

childhood that if you try to hurt someone, it is bad. You don't do that. If you simply say don't use this application, it will not answer their curiosity. When you say don't use the application because of X, Y, Z reasons, and how it can harm them, harm them, how it harms the family, how it harms the whole siblings, other things, they will then understand. Don't just say simple no and move on.

Another, trying to come back to that one, you can do as much as surveillance as you want, but it is not enough for you. If you go into that direction, it won't be enough ever. That time, is it agreeable to your children, someone was asking that, the tools are there, are -- are your children happy with that? It is more about talking to them rather than trying to do surveillance.

>> NOELLE DE GUZMAN: Thank you. We're coming to the end of our time. I'll touch upon another question, a bunch of questions coming up on whether Tik Tok, other house party, they're good or bad for children. I think we know that Tik Tok is one of the most downloaded apps now in the world especially South Asia as well as the fist, seconded most downloaded app last year. It has benefits for children. It allows them to socialize, allows them to express themselves. There are valid security and privacy risks, for example there's a feed on Tik Tok, a common feed where children can be exposed to inappropriate content. I think if I'm not mistaken in Tik Tok, strangers can also contact each other. That said, a thing that we can recommend, it is that through -- try and use the apps yourselves, try Tik Tok, try using that yourself, enjoy -- well, try to explore it, try to see what people are saying, try to see what you think could be the risks for your child, try to read about it. There's been a lot of articles written about Tik Tok and use for children. Then you can decide.

Unfortunately, we have come to the end of our webinar, it is now the top of the hour. Please do stay in touch with us. We're very engaged in this topic and you can follow us on Twitter and Facebook which will now be posted on the chat. If you would like to know more about our work, you can visit us on our website, internetsociety.org and we would like to hear from you regarding this webinar. Before you go, take a minute, two, answer the feedback form, on Zoom it will pop up after you end the webinar, and I think in Facebook, the link, it is being posted on the chat, that would really, really help us in our webinars going forward. Thank you very much, unfortunately we did not have time to answer all of the questions. Thank you for joining, have a wonderful day, afternoon, evening. Good-bye.

***