parenting *ideas

Sextortion on Instagram

Even though Insights is for parents of children of all ages, we sometimes share content that is aimed specifically at parents of older children. This issue is one such example. However, parents of younger children will gain from reading this Insights article, simply because soon your children will be big enough to be utilising social media and online games. Once this happens, whether at your home or at a family member's or friend's home, your child is exposed to risks like those outlined below.

Our children are curious, and potential child predators recognise and prey on this. Recently we have had several disclosures of sextortion. Sextortion is a hybrid of the words 'sexual' and 'extortion.' Sextortion is a serious crime that occurs when someone threatens to distribute your private and sensitive material if you don't provide them images of a sexual nature, sexual favours, or money.

The way this often works is that your child will be approached and targeted through a direct message request from a stranger on their social media platform, such as Instagram. These approaches can also happen on games with chat functions including Roblox and Minecraft.

The most recent case that we referred to the Police was a 16 year old girl that had checked her direct message requests and accepted them (as most teens usually do even though this is very dangerous). Once the connection was made, the sextorter (that is, the new "friend" or "connection") said "If you don't send me a nude in 60 secs I will send this image to your friends and say it is you". They sent her a cropped image of a naked young woman laying on a bed.

The 16 year old responded, saying that she would report them. Again they gave her 60 seconds. The girl responded with some forceful profanities in an attempt to shut down the conversation. The blackmailer went ahead and sent the image through another DM to three boys that were on her friend's list.

The perpetrator had done their research, and they knew the boys lived in the same town as they played sport together and had commented on a recent post the girl had shared. (This is easy to figure out through a public account on Instagram and why setting an Instagram account to private is a must.)

The girl blocked the person doing the sextortion, but messages kept coming through under multiple account names. The girl took screenshots to use as evidence. They were all reported to Instagram and blocked. We notified the Police so that they were aware if the images were shared by other teens who may have believed it was her. They contacted the teens involved who had received the photo and shut the whole situation down very quickly.

As frightening as this is, this is a good news story. The boys knew it wasn't her. They didn't pass things along. The girl blocked the perpetrator. The issue was reported and police intervened.

Nevertheless, this example highlights the enormous and urgent need we have to engage with our children with conversations about the way that they are using social media or online games and other platforms where our children can interact with, and be contacted by, people not known to them. Things you need to discuss with your children include:

parenting *ideas

- That they should never accept DM requests from anyone they don't know. Accepting a DM request from an unknown contact is not safe. Never. Ever
- That they should never share personal details with people they do not know personally. Children are groomed every day by people who are not who they say they are. (E.g., a 47 year-old man pretending to be a 12-year-old boy)
- Tell them to use an alias, and to avoid sharing anything about their location, school, favourite hobbies, or anything else with people on the Internet, even if they think they know who they are talking with
- Ask them to show you the DM request section of their online profiles from time to time. (DM's are usually just from their friends, but the DM request section is almost always from strangers)
- Ask your child to show you how they report and block to be assured that they know what to do when things go wrong
- Make sure they know not to pay or respond to any demands at all. They should not engage at all
- Teach them that they should take screenshots if something happens to have evidence if the authorities need to be notified
- Let them know that they can always speak to you without judgment, that you will help them if they make a mistake online, and something goes wrong. They need to know that they should never be afraid to speak up.

In closing

- If you are in Australia, make an image-based abuse report to https://www.esafety.gov.au/report/image-based-abuse
- Report suspected grooming to https://www.accce.gov.au/
- Or report to your local Police or Crime stoppers via https://crimestoppers.com.au/
- If you are not in Australia, immediately contact your local Police for advice and to make a report.

Kirra Pendergast

Kirra Pendergast is the CEO of Safe on Social Media Pty Ltd and The eSafety Training Company Pty Ltd. Both are purpose-driven organisations, aiming to keep as many people across the world safe online through education and empowerment. For further information visit www.safeonsocial.com and www.esafetyhq.com