Parent Factsheet
Sextortion: Financially motivated sexual extortion

What is the problem?

The National Crime Agency issued an alert in May following a considerable increase in global cases of financially motivated sexual extortion – a type of online blackmail widely known as 'sextortion'.

Sextortion involves people being forced into paying money or meeting another financial demand, such as purchasing a pre-paid gift card, after an offender has threatened to release nude or semi-nude photos of them. This could be a real photo taken by the victim, or a fake image created of them by the offender.

All age groups and genders are being targeted, but a large proportion of cases have involved male victims aged between 14-18. Ninety one per cent of victims in UK sextortion cases dealt with by the Internet Watch Foundation in 2023 were male.

They are motivated by making money quickly, rather than by sexual gratification, and in some cases have gone from initial contact to blackmailing their victim in under an hour.

Sextortion is a form of sexual abuse.

What does it look like?

Child victims may report being:

➔ contacted by an online account that they do not know but appears to be another child or young person. They may also be contacted by a hacked account of a child or young person they do know and the communication feels unfamiliar
➔ quickly engaged in sexually explicit communications, which may include the offender sharing an indecent image first
➔ moved from a chat on social media, an online platform or game to a private messaging app that is an end-to-end encrypted chat platform[1]
➔ manipulated or pressured into taking nude or semi-nude photos or videos
➔ told they have been hacked and the offender has access to their images, personal information and contacts (whether this is true or not)
➔ blackmailed into sending money or meeting another financial demand (such as purchasing a pre-paid gift card) after sharing an image or video, or the offender sharing hacked or digitally

---

[1] End-to-end encryption (E2EE) means that messages sent from one person to another cannot be seen or read by anyone else. WhatsApp, Facebook Messenger and many more messaging apps are bringing E2EE to their services. You can read more about E2EE on the CEOP website here.

manipulated/AI-generated images[2] of the child or young person and making the threat of sharing them wider

It is important to be aware that organised crime groups may target multiple children and young people within a social or educational setting, as it is more likely that a child or young person will accept a friend request or communicate with someone they don't know if they believe they are a 'mutual friend'.

Talking to your child

It's important to have frequent, open and non-judgemental conversations with your child about relationships, sex and being online to build trust and support them if something goes wrong. Financially motivated sexual extortion should be included in those conversations. Here are some tips about how to approach this:

➔ **Chat regularly about their life online**: have ongoing conversations with them about their life and time online. Continue to take an interest as they grow, explore new apps and sites together and talk in a balanced way, considering the benefits and the potential harms.

➔ **Talk about where to find information about relationships and sex**: organisations like CEOP Education, Childline and Brook have age appropriate advice on topics such as sexual communication and image sharing. This will help your child to understand what unhealthy relationships look like, such as applying pressure and blackmail; and give them trusted sources of information to explore these topics. You can find a list of these and other resources below.

➔ **Review privacy settings**: talk to your child about the importance of using privacy settings on their accounts to restrict who can contact them. You might find it helpful to read CEOP Education's advice on how to talk your child about their privacy settings.

➔ **Make sure they know where to go for support**: let them know that they can come to you with any concerns and won't be judged. It's also important to make them aware of other trusted adults or sources of support, if they feel they can't talk to you, such as Childline.

What can I do if this has happened to my child?

If your child tells you that someone is trying to trick, threaten or blackmail them online:

➔ **Don't pay, do stop contact and block:** you may be tempted to pay, but there is no guarantee that this will stop the threats. As the offender's motive is to get money, once you have shown you can pay, they will likely ask for more and blackmail may continue. If you have paid, don't panic but don't pay anything more. Help your child to stop all communication with the offender and block them on any accounts that they have been contacted on.

➔ **Avoid deleting anything:** try not to delete anything that could be used as evidence such as messages, images and bank account details.

➔ **Report to the police or CEOP**: call 101 or 999 if there is an immediate risk of harm to your child. Or you can use the CEOP Safety Centre to report any online blackmail attempts.

---

[2] Artificial Intelligence (AI) is able to generate realistic-looking images that can be convincing enough to be indistinguishable from real ones. The Internet Watch Foundation has found that there are thousands of AI-generated images being posted to forums on the dark web each month. You can read more about their report here.

If it has already happened and your child has shared an image and sent money to someone exploiting them:

➔ **Reassure them that they've done the right thing by telling you:** make sure they know they are not to blame for what has happened and they have done the right thing to ask for your help. Children and young people's mental health may be negatively impacted by experiences of exploitation; you can find advice on looking after your child's mental health from the NHS.

➔ **Report to the police or CEOP:** call 101 or 999 if there is an immediate risk of harm to your child, or you can use the CEOP Safety Centre to report an incident. If your child is 18 and over, they should call 101 or 999 if they are at risk of immediate harm.

➔ **Report any images or videos that have been shared:** remind your child that if a nude or semi-nude of them has been shared without their consent, they can take these 3 steps to try and get them removed:
   1. Use Report Remove, a tool from Childline and the Internet Watch Foundation. Your child can use this to remove images that have been shared or might be shared.
   2. Use Take It Down, a tool from the National Center for Missing and Exploited Children. Your child can use this to remove or stop the online sharing of images or videos.
   3. Report directly to the platform or app that the incident has occurred on. For advice on how to report to major social media platforms, visit Internet Matters.

Where can I go for more information?

CEOP Education	https://www.thinkuknow.co.uk/
Internet Watch Foundation	https://www.iwf.org.uk/resources/sextortion/
Internet Matters	https://www.internetmatters.org/
UK Safer Internet Centre	https://saferinternet.org.uk/guide-and-resource/parents-and-carers
Childline	https://www.childline.org.uk/
Brook	https://www.brook.org.uk/
Purcell Safeguarding Team	safeguarding@purcell-school.org