POLICE SCOTLAND
POILEAS ALBA

Cyber Byte

September 2025.

Sextortion;

…. a type of online blackmail.

Potential victims of Sextortion are any age, why? well cyber criminals do not discriminate, they will attack anyone. However, the age range of victims most often includes young males in their early teens up to the age of 30.

Globally there has been an increase of these incidents, usually carried out by organised crime gangs who are motivated by financial reward.

Sextortion is almost a media friendly term that doesn't really reflect the risk and harm caused to its victims.

We must understand there is a great degree of complexity in this type of attack, which is particularly difficult for victims to report by its very nature and due mainly to personal embarrassment, confidentiality, and perhaps explicit detail.

Awareness of crime, especially how it is committed, is important so we are prepared to recognise it, reject it, report it and prevent victimisation.

Remember, cybercriminals do not care about you, they also have no consideration of how their attack will affect you.

How cyber-criminals use sextortion to attack their victim;

You may be:

- contacted through an account you don't recognise, or it could be through the hacked account of someone you do know but where the communication feels unfamiliar.
- quickly engaged in sexually explicit communications, which may include the cybercriminal sharing an image first, which will of course be fake!
- asked to move from a chat on social media, or gaming platform to a private platform such as an end-to-end encrypted messaging app.
- told they have gathered more personal information about you from other online accounts, relating to platforms you visit, as they move about online.
- manipulated or pressured into taking nude or semi-nude photos or videos of yourself.

- told you have been hacked, and the cybercriminal suggests they have access to your 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 the cybercriminal sharing hacked or digitally manipulated/AI-generated images of you and threatening to share them with your contacts.
- coerced into sending further images, as the cybercriminal puts you under pressure, which could make you do things you do not want to do!

Ways to protect yourself

- Review your online settings and make sure you have the highest level of privacy on all your accounts so that people you don't know cannot see your friends/followers and personal data you share online.
- Be careful what you post and share, especially personal images. Remember, once you post anything online, you lose control of it, and it could be used against you.
- Be aware of the warning signs of an online blackmail attempt. If you are contacted by someone you don't know or from an account you do not recognise, don't engage, end the communication and block them. Take a look at NCSC's advice on spotting and reporting fake accounts. Phishing: Spot and report scam emails, texts, websites and... - NCSC.GOV.UK
- If you are a parent / carer, have frequent open and non-judgemental conversations with your child / young person about relationships, sex and being online, to build trust and understanding with them. Make them aware of the reporting routes available so that if something happens to them online they are able to react to this, in particular, the CEOP Safety Centre is a great resource for this support.

Fearless is a dedicated youth service of the independent charity Crimestoppers and they have excellent resources to support our young people. We strongly encourage you to visit their site at Sextortion - Professionals | Crimestoppers

Our partners at the NSPCC have additional resources titled Why language matters: why we should rethink our use of the term 'sextortion' | NSPCC Learning and we encourage making the use of the guidance for awareness and of course support.

Police Scotland have also produced guidance which available via this link Sextortion - Police Scotland

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101.

Police Scotland Cybercrime Harm Prevention Team

All information correct at time of distribution.