Cyber Security Centre of Excellence
West Bengal
Department of Information Technology & Electronics
Government of West Bengal

SEXTORTION AND YOUR ONLINE SAFETY

Sextortion is a form of blackmail where criminals use fake identities to befriend with victims online, using social media platforms such as Facebook, Skype, LinkedIn etc.

The cybercriminal, posing as an attractive person, initiate communication which is sexual in nature, with the victim (majority of victims are male). The cybercriminal simply shows the victim a pre-recorded video of a performer, then messages the victim at points in the video where the performer appears to be typing on the keyboard, to give the illusion that the performer in the video is messaging them.

The victim is then persuaded to perform sexual acts in front of a webcam. The video is recorded by the cybercriminal, who then reveals their true intent and demands money or other services, and threatening to publicly release the video to video services like YouTube and send it to family members and friends of the victim if they do not comply.

ONCE YOU'VE BEEN A VICTIM

- Don't panic.
- Preserve evidence.
- Take screen shots of all your communication.
- Make a note of all details available about the offenders, for example, social media usernames.
- Be aware that the scammers' user name might be different to their social media ID, and it's the ID details that police will need.
- Contact your local police and ISP immediately. The police will take your case seriously, will deal with it in confidence and will not judge you for being in this situation.
- Use the online reporting process to report the matter to Skype, YouTube etc. to have the video blocked and to set up an alert in case the video resurfaces.
- Deactivate the social media /Facebook accounts temporarily rather than shutting it down.
- The account can also be reactivated at any time so your online memories are not lost forever. The data will remain preserved and will help police to collect evidence.
- Keep an eye on all the accounts which you might have linked in case the criminals try to contact you via one of those.
- Don't communicate further with the criminals.
- Don't pay. Many victims who have paid have continued to get more demands for higher amounts of money.

- If you have already paid, check to see if the money has been collected. If it has, and if you are able, then make a note of where it was collected from. If it hasn't then you can cancel the payment – and the sooner you do that the better.

GENERAL SAFETY TIPS

- Never disclose any personal information on social media platform.
- Avoid making friends with someone whom you do not know from other sources.
- Be cautious that social media profiles can be fake or honey-traps.
- Be wary of pictures/videos you post online – once they are published on the internet it can be downloaded and shared by other people.
- Make sure your passwords are strong, and change it regularly – of course, never give this information out.

Ref:
https://digiinfomedia.online/online-sex-crime-what-is-sextortion-and-how-to-keep-yourself-safe-online/
https://en.wikipedia.org/wiki/Sextortion
https://www.anandabazar.com/district/nadia-murshidabad/jangipur-police-busted-a-bank-fraud-racket-3-arrested-from-rajasthan-dgtld-1.1226476