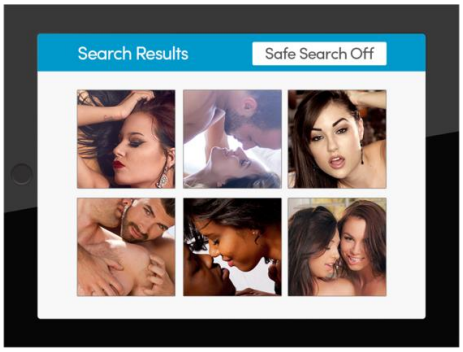
Lead Scotland

Linking education and disability

Lead Scotland



How to protect yourself from sextortion emails

Easy Read

Easy Read made by Disability Equality Scotland

made with photosymbols®

How to protect yourself from sextortion emails

A **scam** is a trick to get your money or personal information like your bank details.

Sextortion is when someone threatens to publish sexual information, photos or videos about someone.

They frighten people into paying money to stop them publishing the information.

They often want the money to be paid using **Bitcoin**.

Bitcoin is a type of digital money that is made and stored online.

Sextortion scams look real because they sometimes include details like your password.

The criminal hopes that enough people will answer the scam so they can make money.

They do not know

- if you have a webcam
- if you have been visiting adult websites

They are guessing.

What to do if you get a sextortion email

- do not communicate with the scammer

Forward the email to report@phishing.gov.uk and then delete it.

- if you are tempted to pay money to the scammer this will probably encourage more scams

Criminals think that if you have replied to one scam you will do it again.

- if the email includes a password you still use then change it straight away

Cyber Aware has advice about secure passwords
https://www.cyberaware.gov.uk/passwords

If you put your email address on the website https://haveibeenpwned.com you can

- check if your account has been hacked
- and get messages to tell you if it happens in the future

- if you have been a victim of a sextortion scam and have paid money to the scammer, report it to your local police force by calling 101

- emotional support is available from Victim Support

Phone 0808 168 9111

or look at their website
https://www.victimsupport.org.uk/