National Cyber Security Centre

Sextortion phishing scams
How to protect yourself

This guidance explains what to do if you've received an email that's trying to blackmail you. The email may state that your login details have been compromised, or may threaten to reveal some compromising information (such as a video of you visiting an adult site). You can protect yourself by following the steps below.

What is a sextortion scam?

A **sextortion scam** is when a criminal attempts to **blackmail** someone, usually by email. The criminal will claim they have login details or a video of the victim visiting an **adult website**, and will threaten to disclose this unless the victim pays a **ransom** (often in Bitcoin).

The criminals behind these attacks do **not** know if you have a webcam, or know if you've visited adult websites. They are attempting to **scare their victims** into paying a ransom, and will send millions of emails in the hope that someone will pay. They'll often include technical sounding details to make the email sound convincing. It may also include a password the victim uses or has used.

Sextortion is an example of a **phishing attack**, where victims receive emails that try and **trick them** into doing the wrong thing.

What to do if you've received a threatening email

Don't communicate with the criminal

As with other phishing attacks, our advice is to **not** engage with the criminal. If you have received an email which you're not sure about, forward it to the NCSC's Suspicious Email Reporting Service (SERS): report@phishing.gov.uk, and then delete it.

Should I pay the ransom?

If you are tempted to pay the ransom, you might be targeted with future scams, as the criminal will know they have a 'willing' customer.

Check if your accounts have been compromised

Do not worry if your password is mentioned. It has probably been discovered from a previous data breach. You can check by visiting https://haveibeenpwned.com/

www.ncsc.gov.uk

@NCSC

National Cyber Security Centre

@cyberhq

Change any passwords that are mentioned

If a password you still use is included, then change it immediately. For advice on how to create good passwords, please visit www.cyberaware.gov.uk .

If you've already paid the ransom....

If you have already paid the ransom, then visit Action Fraud for further advice (www.actionfraud.police.uk).