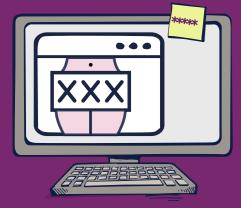


# **Sextortion phishing scams How to protect yourself**

This advice is for people who have received sextortion emails. If someone you don't know is blackmailing you by claming to have login details or a video of you visiting an adult site, **don't pay the ransom**, but follow the steps below instead. The criminals behind these attacks don't know if you have a webcam, or if you've visited adult websites.

# 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're being blackmailed

#### **Don't** communicate with the criminal

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.

## **Don't** pay the ransom

If you pay the ransom, you might be targeted with more scams, as the criminal will know their previous scam worked.

## **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



in 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.

#### **Report** any losses to Action Fraud

If you have already paid the ransom, then report it to Action Fraud (www.actionfraud.police.uk).

