CITY OF LONDON POLICE
National Policing Lead For Fraud

Official

Sextortion phishing emails

Published on 20th April 2020
Reference 2004001

Sextortion phishing emails

CITY OF LONDON POLICE
National Policing Lead For Fraud

Sextortion email scam

Published on 20/04/20
Reference 2004001

A total of **9,473** phishing emails linked to sextortion have been made to the NFIB phishing inbox between 31/03/2020 – 19/04/2020.

There has also been just over 200 reports made to Action Fraud in the last week.

Sextortion scams are a type of phishing attack whereby people are coerced to pay a BitCoin ransom because they have been threatened with sharing video of themselves visiting adult websites. These scams are made to appear all the more credible because they provide seemingly plausible technical details about how this was achieved, and the phish can sometimes also include a password used by the recipient.

The current campaign threatens that if the victim does not provide a payment within a specific timeframe (payments usually ranging from $1,000 to $4,000), which is requested into a bitcoin wallet, then a compromising video will be shared to all their contacts and social media channels.

What you need to do

- Do not reply or click on any of the links in the email. You can report the email to Action Fraud at actionfraud.police.uk/report-phishing.
- Don't be tempted to make the Bitcoin payment. Doing so may encourage more scams as the fraudster will know they have a 'willing customer'.
- If you have made the Bitcoin payment, you should report it to your local police force by calling 101.
- If the email includes a password you still use then change it immediately.
- For more information, visit: actionfraud.police.uk/sextortion

For more information about how to protect yourself online, visit
www.cyberaware.gov.uk and **takefive-stopfraud.org.uk**

Every Report Matters

If you have been a victim of fraud or cyber crime, report it to us at Actionfraud.police.uk, or by calling 0300 123 2040.