Devon and Cornwall ALERT

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Urgency: 3 2 1

SCAM

Action Fraud Alert: rise of extortion phishing email reports

Action Fraud are urging the public to look out for phishing emails that relate to extortion as the Suspicious Email Reporting Service (SERS) received over 2,924 reports in March 2025, a staggering increase compared to only 133 reports made in February.

The reported phishing emails received by the National Cyber Security Centre's SERS relate to a type of extortion referred to as 'Financially Motivated Sexual Extortion' (FMSE).

Reports suggests the phrasing of the email and subject lines can vary, but the theme remains consistent: the phishing email claims to have installed malware on the recipient's computer and recorded them visiting adult websites. The sender will then coerce the email recipient to pay a ransom demand by threatening to release the videos. The ransom is usually demanded in a form of cryptocurrency, such as Bitcoin.

In order to make these phishing attacks convincing, emails will often include genuine pieces of personal information relating to the victim, such as a password or home address. It is likely these would have been obtained from historic breaches of personal data.

Analysis shows that many people who received these emails also later reported becoming victims of online account hacking.

In 2024, a male victim in his thirties received numerous extortion emails that contained a password he used for one of his online accounts. The emails demanded a ransom of $500. Having correctly identified the emails as a scam, he deleted them. However, shortly afterwards he noticed that he was unable to login to one of his social media accounts. After some checking, he realised that one of his bank accounts and multiple social media accounts had been hacked and he was locked out of them.

What to do if you receive an email like this:

- As with other phishing emails, do not to engage with the phisher, forward the email to **report@phishing.gov.uk,** which is the NCSC's Suspicious Email Reporting Service (SERS), and then delete it.
- If you are considering paying the Bitcoin ransom, you should be aware that doing so, you will likely become the target of more scams, as the phisher will know they have a 'willing' customer.
- The inclusion of genuine passwords or other personal information in phishing emails is a strong indication that you may have been affected by a historic data breach. You can use this service to check which of your online accounts were affected: https://haveibeenpwned.com
- If the phishing email includes a password you still use**, then change it immediately**. Advice on how to create suitable passwords and enable other factors of authentication is available here: https://stopthinkfraud.campaign.gov.uk/protect-yourself-from-fraud/protecting-against-online-fraud/improve-your-password-security/

If you have been a victim of extortion, or concerned that someone may be in possession of intimate images of you, you should report it to your local police force by calling 101.

Find out how to protect yourself from fraud: https://stopthinkfraud.campaign.gov.uk

If you've lost money or provided financial information as a result of any phishing scam, notify your bank immediately and report it to Action Fraud at https://www.actionfraud.police.uk/report-phishing or by calling 0300 123 2040. In Scotland, call Police Scotland on 101.