POLICE SCOTLAND
POILEAS ALBA

Cyber Security Alert

Online Sexual Extortion

Police Scotland Cybercrime Harm Prevention Team.
15.05.2025

Online Sexual Extortion

In March 2025, the Suspicious Email Reporting Service (SERS) operated by the (NCSC) National Cyber Security Centre, received 2,924 reports relating to this type of online extortion from the public.

Reports suggest whilst the email titles and phrasing can vary, the message remains consistent with the cyber-criminals claiming to have installed malware on the recipient's computer and recorded them visiting adult websites.

The cyber-criminals then attempt to 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.

To make these phishing email 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. ***See point 3 below.***

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

Case Study:

A victim received numerous emails that contained a password for one of their online accounts. The emails demanded a ransom of £500. Having correctly identified the emails as an extortion scam, the victim deleted them.

Shortly afterwards the victim was unable to login into their social media accounts and after some checking, realised their bank accounts and multiple social media accounts had been hacked and were locked out of them.

What to do if you receive an email like this:

1. As with other phishing emails, do not to engage with the Cyber-criminal, forward the email to **report@phishing.gov.uk,** which is the NCSC's Suspicious Email Reporting Service (SERS), and then delete it.
2. 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 Cyber-criminal will know they have a 'willing' customer.
3. 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
4. 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/
5. How to recover a hacked account: Recovering a hacked account - NCSC.GOV.UK
6. Creating a strong password, turning on 2SV and Backing up your data: Use a strong and separate password for your email - NCSC.GOV.UK

If you have been a victim of extortion (Sextortion - Police Scotland) or concerned that someone may be in possession of intimate images of you, or if you've lost money or provided financial information because of any phishing scam, notify your bank immediately and report it Police Scotland by calling 101.

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101.

This alert was sent out for your information by
Police Scotland Cybercrime Harm Prevention Team -