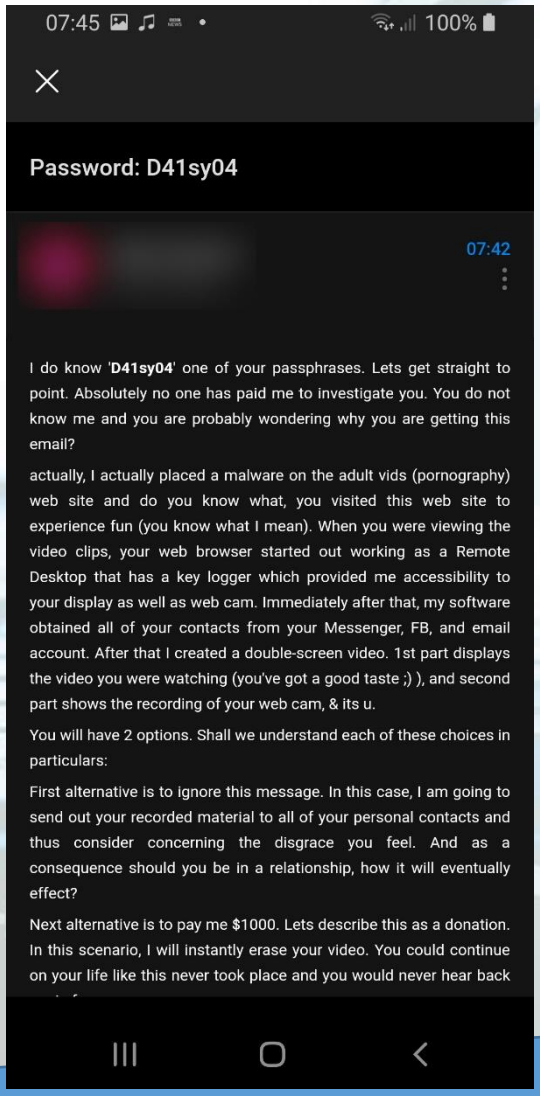
Sextortion

Surrey & Sussex CCU Newsletter – June 2020

The Cyber Crime Unit continues to receive numerous reports of people receiving e-mails threatening to disclose intimate activity unless financial demands are met. These e-mails are collectively known as 'sextortion' e-mails and, although they come in several different guises, many will include the following: -

1. It may list one of your **passwords**.
2. The author will suggest that they have **control** of your **webcam** and have **recorded** you visiting **pornography** websites.
3. A **payment** will be requested (generally in the form of **cryptocurrency**) in exchange for erasing the recording(s).
4. There will be an element of **urgency** about the demand – usually 24 hours or less.
5. The author will suggest they can **monitor the time** you received the e-mail.
6. Should the payment not be made in the requisite time, the recording(s) will be **e-mailed** to all your contacts.
7. Many will have **spelling mistakes** and **poor grammar**.



Please note that law enforcement does not encourage, endorse nor condone the payment of ransom demands.

Why me?

Your e-mail address is a bit like your home (or postal) address. Whilst you may not advertise your home address, over time, companies, organisations and individuals will become aware of it. The same can be said about your e-mail address. Anyone can send messages to it in the same way as you receive junk mail through your letterbox. Scammers have no real idea who they are targeting – it's just another address to them.

Sextortion e-mails are just one of many kinds of e-mail sent indiscriminately to large volumes of individuals in the hope that a small proportion of them may be tricked into making a payment.

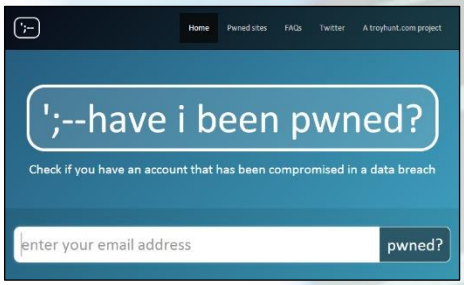
Are you interested in a free cyber awareness presentation? Our Protect & Prepare team can deliver online presentations to businesses and other groups (20+ attendees) across Surrey & Sussex. These are approximately 1 – 1½ hours in duration and cover a range of current cyber topics.

Please e-mail CyberCrimeUnit@surrey.pnn.police.uk for further information.

SEROCU: serocu.police.uk/cyber | Cyber Aware: www.ncsc.gov.uk/cyberaware | NCSC: www.ncsc.gov.uk

CYBER AWARE

Where did they get my password?



If you have read our previous newsletters, you will know that data breaches are occurring all the time. At some point, most people will have had their username / password combinations compromised. Details of these compromised accounts can sometimes be seen by visiting the website www.haveibeenpwned.com.

Passwords used in sextortion e-mails are often quite old and can usually be traced back to an historic data breach. Criminals know that putting this sort of information in an e-mail lends some credibility to the threat they are making, and some people are likely to act on the threat as a result. Sometimes, scammers will use other personal information such as your mobile phone number or date of birth.

What should I do if I receive an e-mail like this?

- Try and work out what online account the password was originally used for. It is important to ensure that if the account is still in use, the password is changed to secure it. It makes sense to review all your online passwords to ensure they all meet the requirements for strong passwords. Passwords should consist of 3 random words, be more than 12 characters in length and they can be complicated by using a mixture of symbols, numbers and capital letters. Remember, all your passwords should all be different.
- Implement 2 factor authentication (2FA) on your accounts where possible.
- Ensure you have an anti-virus and / or Internet security product on all your devices.
- Keep your computer, apps and software up to date by installing the latest updates.

What can I do with these e-mails?

Law enforcement agencies are working continually to identify individuals who are sending these e-mails. You can help by sending any suspicious e-mail to the Suspicious Email Reporting Service at report@phishing.co.uk.

Information from these e-mails is analysed and requests are made to have web servers and spamming accounts closed down.

After that – just delete them from your e-mail account.

Is there anything else I should know?

If you have any concerns, ask yourself this question: "***If the scammers really had evidence that supported the threat, wouldn't they include a clip or a screenshot in the e-mail to highlight what they had in their possession?***" We are yet to see such evidence in one of these e-mails!

Are you interested in a free cyber awareness presentation? Our Protect & Prepare team can deliver online presentations to businesses and other groups (20+ attendees) across Surrey & Sussex. These are approximately 1 – 1½ hours in duration and cover a range of current cyber topics.

Please e-mail CyberCrimeUnit@surrey.pnn.police.uk for further information.

SEROCU: serocu.police.uk/cyber | Cyber Aware: www.ncsc.gov.uk/cyberaware | NCSC: www.ncsc.gov.uk