Sextortion

This Document is for those who don't understand the term 'Sextortion'. It will outline what it is, give examples of where this cyber-attack will occur, and will give protect advice in line with the national guidance.

What is Sextortion?

Sextortion gets its name from exploiting sexualised content performed over a webcam or mobile device, holding this content ransom and threatening to release it to family members and friends, causing the victim complete embarrassment and shame. Cybercriminals use the fear and shame tactic to entice the victims to pay this ransom demand, usually through a cryptocurrency because of the anonymity.

Another form of sextortion is where you have randomly been subject to a phishing attack and within this email they have supplied a current or old password for one of your accounts, while proceeding to threaten you with embarrassment and shame, releasing content of you performing a sexual act. These criminals will suggest that they have installed malware on your computer and can see everything you're doing. However, this is not the case.

Other versions of this type of scam include:

- Visiting adult websites
- Sending nude images
- Any other adult content

Cyber criminals will send millions of emails in the hope that a few of them will respond and pay the ransom. They will try to use technical words to make the emails sound more convincing. However, the only real fact they may have is your password.

Why?

They have this password from a data breach, on a website that you have visited and due to their poor security, an attacker has been able to retrieve usernames, passwords, email accounts, etc. Therefore, this criminal trying to extort money from a victim, who has not hacked your computer and installed malware, but in fact has found personal information, which is usually sold on the dark web or they have found this information on the internet because it has been publicly released.

You can visit '**Haveibeenpwned**' to check if an email address is linked with any data breaches.

Protect Advice

The following advice is in line with the guidance from the National Cyber Security Centre (NCSC).

Do not communicate with the criminal

Do not engage with the criminal. If you have received an email that you are not sure about, forward it to the NCSC's Suspicious Email Report Service (SERS): **report@phishing.gov.uk**

Do not pay the ransom

If you pay the ransom demand, you are informing the criminals that you are vulnerable and you may be inviting them to send you more scams as a result. Also, there is no guarantee that this will be the end of the scam.

Check if your accounts have been compromised

Do not worry if your password is mentioned. As previously mentioned, it has probably been discovered from a previous data breach. You can check if an email has been linked with recent data breaches via **https://haveibeenpwned.com/**

Change any passwords that are mentioned

If a password you still use is included, change it immediately. The national guidance is to use three random words for a password, these can be more complex by adding numbers and symbols. For more information, visit **https://cyberaware.gov.uk**.

Report any financial loss to Action Fraud

If you have already paid the ransom, report it to Action Fraud: **https://actionfraud.police.uk**.

Other Attack Vectors

Additionally, there are increasing reports of dating Fraud. This is similar and can merge with sextortion attacks. However, these attacks usually look to find a victim through dating sites and pretend to be romantically involved with them, by creating fake profiles.

These criminals look to play on people's sexual desires and those who want a genuine relationship. They will try to extort money from a victim by using excuses, such as an ill sibling or parent, travel money to visit the victim but in fact they do not, and they will use any other excuse not to visit you when the victim asks.

Protect Advice

- Never give money to people you meet online, no matter what the emotional story the persona uses.
- Avoid giving away too much personal information when dating online. Revealing your full name, date of birth and home address may lead to your identity being stolen.
- Never send or receive money or give away your bank details to someone you've only met online, no matter how much you trust them or believe their story.
- Pick a reputable dating website and use the site's messaging service. Fraudsters tend to want to quickly switch to social media or texting so there's no evidence of them asking you for money.
- If a victim has been affected by this, or any other type of fraud, report it to Action Fraud by visiting **https://actionfraud.police.uk** or by calling **0300 123 2040**.