LESS RISK MORE REWARD

MAINTAINING YOUR FINANCIAL WELLBEING AT UNIVERSITY

Sextortion awareness toolkit

METROPOLITAN POLICE

NASMA
National Association of Student Money Advisers

Contents

Thank you for supporting the NASMA 2024 ‘Less Risk More Reward’ campaign. This campaign aims to raise awareness amongst students of fraud types affecting young people.

This toolkit contains a range of information and resources to help your institution raise awareness and includes:

01 Key information about the ‘Less Risk More Reward’ campaign

02 Key messages about Sextortion

03 Template copies

04 Assets

05 Signposting support

06 Ideas for how to support the campaign

If you have any questions about these resources, please contact CryptoProtect@met.police.uk

1. About the campaign

Who are NASMA?

NASMA is the National Association of Student Money Advisers, a professional membership association for those across the UK working within the student money advice sector.

NASMA helps members to provide the best support to students by promoting the development and sharing of sector best practice and free exchange of ideas, developing members' skills through professional development events and conferences, and representing the views of our members by working closely with national decision makers and their influencers.

Working closely with partners, including the Metropolitan Police, to highlight areas of concern, raise awareness and provide resources to help our members effectively support students financial wellbeing, is a key priority for NASMA.

1. About the campaign

Fraud affecting younger people

In the UK, **fraud makes up 41% of all crime** and around **80% of fraud offences are enabled through computer technology**.

Fraud is largely underreported and it is estimated that **only 13% of cases are reported** to Action Fraud or the police by victims.

More than one in ten 18-24 year olds have been the victim of a phishing attack, double that of those aged 55+.

Fraud spans across all levels of crime and the impacts on victims are undervalued; from robberies where phones are stolen and bank accounts are drained to serious, organised criminals laundering assets to fund criminality such as terrorism and child sexual exploitation.

Fraud involves the psychological manipulation of individuals and in addition to massive financial losses, can also cause significant emotional harm.

1. About the campaign

Reporting fraud

- Report cybercrime and fraud in the UK to Action Fraud
  - Online - www.actionfraud.police.uk
  - By telephone - 0300 123 2040.
  - If you are deaf or hard of hearing you can use textphone 0300 123 2050
- If a crime is in progress or about the be committed, the suspect is known or can be easily identified or the crime involves a vulnerable victim, contact the Police directly by calling 999 in an emergency, 101 for non-emergencies or visiting your local police station.
- If you have any information about a crime and would prefer to stay anonymous, you can call Crimestoppers on 0800 555 111 or visit www.crimestoppers-uk.org. Crimestoppers is an independent charity.

2. Sextortion

What is sextortion?

Sextortion is a form of blackmail which involves threatening to publish sexual information, photographs or videos to extort money or to get you to do something against your will.

Criminals create profiles using images stolen from others or taken from the internet. The criminals will befriend you and start conversations with this often becoming sexual. They will suggest exchanging pictures or videos of an explicit or sexual nature or carrying out sexual acts on a video call.

Photos or recordings are often made without you realising or consenting. Criminals will sometimes demand a payment for these videos to not be released.

These types of crimes are also sometimes committed by individuals who do not hold any such videos of you. They can be committed as part of a phishing attack to numerous people or directed towards specific individuals. The communications from the criminal may also include a password or username from one of your online accounts which has been taken from a data-breach to attempt to appear more credible.

2. Sextortion

Golden rules for preventing sextortion

- Always be careful about the information and pictures you share and post online. Consider who you are sending intimate content to, if they are who they say they are and if you can trust them
- Keep your devices protected with antivirus software.
- Review your privacy settings including who has access to your friends/connections lists.
- Be aware of overly sexualised dating sites as a large number of criminals operate within this space attempting to target individuals for sextortion.

2. Sextortion

What to do if targeted

- **Do not panic** - non-judgemental help is available.
- **Don't pay the money** which is being requested. Many victims who pay continue to get demands for higher amounts of money. In some cases, even when demands are met, the criminals will still post the videos online.
- **Save the evidence** - take screenshots, save messages and images. Collect URL links and report it to social media companies.
- **Report** the matter to Police using our online reporting tools or by calling 101.
- **Delete and block** individuals who attempt to blackmail you.

2. Sextortion

Primary messages

- 'Sextortion' is a form of blackmail. It involves threatening to publish sexual information, photos or videos about someone. This may be to extort money or to force you to do something against your will.
- Photos or recordings are often made without you realising or consenting.
- Criminals will say they will share the images with your friends or family if you do not pay them money.
- Even if you pay what’s been requested, the criminal may still distribute the images or ask for more money not to do so. This can create an ongoing cycle of payments.
- Sextortion can have significant long lasting effects on the victims including long term emotional, financial and mental repercussions. In some tragic incidents, this has led to the victims taking their own lives.
- Do not panic - non-judgemental help is available.

2. Sextortion

Secondary messages

- Criminals will often use platforms where pictures and videos are automatically deleted to build confidence that the videos will not be retained. Criminals then record the videos on a separate device or application
- They capture your friends lists from social media to use in blackmailing you.
- Victims sometimes end up paying thousands to criminals in order for the material not to be published online or sent to friends and family.
- Don't pay the money which is being requested. Many victims who pay continue to get demands for higher amounts of money. In some cases, even when demands are met, the criminals will still post the videos online.

3. Templates

Template copy

Below is a summary of the key messaging that you may wish to use on your website or in other communities such as newsletters or magazines.

We have provided two versions suitable for different word accounts.

3. Templates

Long copy

Sextortion is a form of blackmail which involves threatening to publish sexual information, photographs or videos to extort money or to get you to do something against your will.

Criminals use social networking sites to identify victims and will pose as someone who is looking to find love or a sexual partner. They will encourage the sharing of intimate content or communications. Photos or recordings are often made without you realising or consenting. Once this has been captured by them, the criminal will then say that they will release the content to your friends, family or online if you do not pay them.

Sometimes the criminal will suggest that they have material which they don’t in order to blackmail you, for example, evidence that you have visited pornographic or illegal sites. The communications from the criminal may also include a password or username from one of your online accounts to attempt to appear more credible. Sometimes this information is taken from a data-breach.

It is becoming increasingly more common for the criminal to ask for ransoms to be paid in crypto which makes it more difficult to trace.

Always be careful about the information and pictures you share and post online. Consider who you are sending intimate content to, if they are who they say they are and if you can trust them.

If targeted:

- Do not panic — non-judgemental help is available.
- Don't pay the money which is being requested. Many victims who pay continue to get demands for higher amounts of money. In some cases, even when demands are met, the criminals will still post the videos online.
- Save the evidence — take screenshots, save messages and images. Collect URL links and report it to social media companies.
- Report the matter to Police using our online reporting tools or by calling 101.

Anyone can be the victim of fraud.

Stop, challenge and protect yourself from crime online.

3. Templates

Short copy

Sextortion is a form of blackmail which involves threatening to publish sexual information, photographs or videos to extort money or to get you to do something against your will.

Criminals encourage the sharing of intimate content or communications and, once sent, will say that they will release this to your friends, family or online if you do not pay them. Sometimes recordings are made without you realising or consenting.

Always be careful about the information and pictures you share online. Consider who you are sending intimate content to, if they are who they say they are and if you can trust them.

If targeted:

- Do not panic — non-judgemental help is available.
- Don't pay the money which is being requested. Many victims who pay continue to get demands for higher amounts of money. In some cases, even when demands are met, the criminals will still post the videos online.
- Save the evidence — take screenshots, save messages and images. Collect URL links and report it to social media companies.
- Report the matter to Police using our online reporting tools or by calling 101.

4. Assets

Fraud, Crypto and Cyber Awareness

The following assets can be provided:

- The Metropolitan Police ‘Little Media Series’ is a collection of 6 books and 22 videos, created to explain some of the most common types of fraud and to give advice on how to avoid becoming a victim of them.
- The videos were created in three series;
  - The Little Mini Animated Guides
  - Little Animated Guides
  - Bitesized Guides
- All of the videos are produced including subtitles and a British Sign Language Interpreter. The books are accessibility tested.
- The above assets can be downloaded from our website - https://www.met.police.uk/littlemedia/

4. Assets

Social media – Generic Posts

This campaign seeks to utilise the hashtags #CryptoProtect, #CryptoPrevent and #LessRiskMoreReward for social media use.

The below are suggested posts for social media use:

- Criminals are experts at impersonation and practice deception to manipulate us into performing actions or divulging sensitive information. Stop, challenge and protect yourself from crime online. #LessRiskMoreReward
- Criminals use social engineering to create an emotional response in us and add time pressure to make us react instead of stopping to think. Stop, challenge and protect yourself from crime online. #LessRiskMoreReward
- Criminals encourage secrecy and confidentiality as a way of targeting us. Sense check with friends or family before divulging information or transferring money on behalf of others. Stop, challenge and protect yourself from crime online. #LessRiskMoreReward
- Received a message that you’re unsure about? Phishing messages can be difficult to spot so make sure to check before clicking on links in emails or text messages. Stop, challenge and protect yourself from crime online. #LessRiskMoreReward

4. Assets

Social media – Sextortion Posts

This campaign seeks to utilise the hashtags #CryptoProtect, #CryptoPrevent and #LessRiskMoreReward for social media use.

The below are suggested posts for social media use:

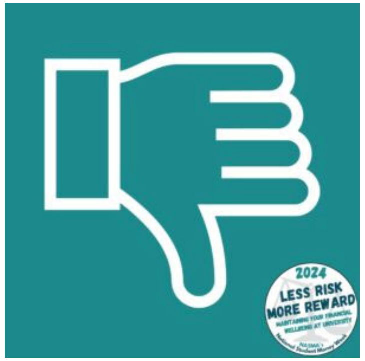
- Keep private communications private. Be careful about the information and pictures you share and post online. Consider who you are sending intimate content to, if they are who they say they are and if you can trust them. #LessRiskMoreReward
- Sextortion is where a criminal threatens to release sexual images of you unless you pay them money. If you become a victim, do not panic. Non-judgemental help is available. Visit https://www.met.police.uk/advice/advice-and-information/sexual-offences/sextortion/ #LessRiskMoreReward
- Stay Safe, Stay Private! Criminals can threaten to send your intimate photos to your friends and family. Turn on your privacy settings. Visit https://www.met.police.uk/advice/advice-and-information/sexual-offences/sextortion/ #LessRiskMoreReward

4. Assets

Social media - Imagery

The following imagery can be used alongside the aforementioned posts in support of this campaign (images can be provided separately)

2024
LESS RISK
MORE REWARD
MAINTAINING YOUR FINANCIAL WELLBEING AT UNIVERSITY
NASMA's
National Student Money Week


2024
LESS RISK
MORE REWARD
MAINTAINING YOUR FINANCIAL WELLBEING AT UNIVERSITY
NASMA's
National Student Money Week

2024
LESS RISK
MORE REWARD
MAINTAINING YOUR FINANCIAL WELLBEING AT UNIVERSITY
NASMA's
National Student Money Week

5. Signposting support

Support agencies

Revenge Porn Helpline

This is a UK service supporting adults who have experienced intimate image abuse and revenge porn including images recorded without consent and webcam blackmail. They provide non-judgemental and confidential advice, guidance and support to help remove intimate content which has been non-consensually shared online. They also provide advice with how to report violations to social media and signposting towards legal advice. They have an automated 24/7 chatbot, an anonymous reporting form as well as phone and email assistance. Their operating hours are 10am-4pm Monday – Friday.

Website - https://revengepornhelpline.org.uk/

Phone – 0345 6000 459

Email – help@revengepornhelpline.org.uk

Stop Non-Consensual Intimate Image Abuse

StopNCII.org is a free tool designed to support victims of non-consensual intimate image abuse. It works by generating a hash from your intimate image(s) or video(s) and then sharing the hash, or digital fingerprint with participating companies so they can help detect and remove the images from being shared online. It does not download the image and collects minimal data to run the service. It is operated by the Revenge Porn Helpline and cases can be created from their website.

Website - https://stopncii.org/

5. Signposting support

Support agencies

Samaritans

The Samaritans are a 24/7 support service for individuals who are struggling to cope or who need non-judgemental listening and support to prevent crisis'; in particular for individuals contemplating suicide. They can be contacted from any phone free on 116 123, via an online chat service via their website, by writing a letter or face to face. They also have a self-help application to keep track of how you're feeling and things you can do to help yourself cope.

Website - https://www.samaritans.org/

Phone – 116 123

Email – jo@samaritans.org (it may take several days for them to respond to emails)

Face to face - https://www.samaritans.org/branches/

Report Harmful Content

Report Harmful Content can help individuals to report content online by providing up to date information on community standards and the reporting facilities across multiple specific platforms. They provide advice on reporting eight types of online harm, namely; threats, impersonation, bullying or harassment, self-harm or suicidal content, online abuse, violent content, unwanted sexual advances, pornographic content and other harmful content.

Reporting is through an online form and they can accept information from individuals aged 13 or over.

Website - https://reportharmfulcontent.com/

5. Signposting support

Support agencies

Get Safe Online

Get Safe Online is a UK based internet safety website. They provide easy-to-understand information on online safety for both individuals and businesses. They have pages on online behaviour, artificial intelligence, digital legacies, privacy, protecting yourself online and victim support. They also have a website checker to determine whether a website is likely to be legitimate or not prior to visiting it. They can be contacted via an online form on their website for questions, general advice or concerns relating to online safety.

Website – https://www.getsafeonline.org/

Thinkuknow

The Child Exploitation and Online Protection (CEOP) Command, run by the National Crime Agency, aims to help protect children and young people from online child sexual abuse. They do this through an education programme; providing training, resources and information to professionals, young people and their families. They also run an online reporting programme and signposting to further support which can be accessed via https://www.ceop.police.uk/ceop-reporting/

Website - http://www.thinkuknow.co.uk/

5. Signposting support

Support agencies

The CyberSmile Foundation

The CyberSmile Foundation is a non-profit organisation committed to digital wellbeing and tackling all forms of bullying and abuse online. They offer professional help and support services to empower those affected and their families to regain control of their lives. They offer a Global Support Service with online advisors who signpost you to the support you may need. They also have a CyberSmile AI Assistant which can help you immediately or you can email them with information about your situation and wait for allocation of an advisor who will assist you in identifying practical next steps.

Website - https://www.cybersmile.org/

Email - help@cybersmile.org

Hub of Hope

The Hub of Hope is a mental health support database provided by Chasing the Stigma which brings local, national, peer, community, charity, private and NHS mental health support services together. They signpost people towards support in times of crisis, when you're in need of extra support or you notice you are starting to struggle. They also provide support and services for family members and friends.

Website - https://hubofhope.co.uk/

6. Ways to support

We encourage you to support the campaign in the following ways:

- Sharing our assets on your social media channels with our hashtags #CryptoProtect, #CryptoPrevent and #LessRiskMoreReward
- Signposting our crime prevention material
- Using the templates provided in your communications with young people
- Issuing a press release to announce your support for this campaign
- Letting us know if there are opportunities to work with you to provide better support to young people in this area. We can create bespoke content for such opportunities.

THANK YOU FOR YOUR SUPPORT

METROPOLITAN POLICE

NASMA
National Association of Student Money Advisers