LESS RISK MORE REWARD

MAINTAINING YOUR FINANCIAL WELLBEING AT UNIVERSITY

Cryptoasset Crime 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:

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

METROPOLITAN POLICE

NASMA
National Association of Student Money Advisers

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.

METROPOLITAN POLICE

NASMA
National Association of Student Money Advisers

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.

METROPOLITAN POLICE

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

CrimeStoppers.
Speak up. Stay safe.

NASMA
National Association of Student Money Advisers

2. Crypto Crime

What are Cryptoassets?

Cryptoassets, also commonly referred to as ‘cryptocurrency’, ‘tokens’ or ‘coins’, are digital representations of value or rights which can be stored, transferred and traded, often using **distributed ledger technology**. They are so called as they use **cryptography** to secure communications. Cryptography is the practice of protecting information through encryption and decryption.

There are thousands of coins and tokens currently in existence including well-known coins such as Bitcoin, Ethereum and Ripple. Cryptoassets differ from each other by the way they operate, including scope, value, processing time, transaction, functionality and the use of smart contracts.

Cryptoassets tend to be volatile, speculative and their use comes with a number of risks. Within the UK, although certain laws and regulations apply to them, they are **not regulated** as strictly as banks or the stock market and **losses are unlikely to be covered** by the Financial Services Compensation Scheme (FSCS) so you may struggle to obtain reimbursement if your assets are lost, even to fraud.

2. Crypto Crime

How are digital assets used in crime?

The benefits of decentralised financial structures (decreasing fees for services, quick transfers of assets, relative anonymity and lack of centralised authorities) are also attractive to criminals for illicit means.

- Criminals utilise the ability to remain **pseudo-anonymous** as a way of avoiding detection.
- **Ransomware** attackers often demand payments in cryptoassets as this eliminates the need to use financial institutions and allows the rapid dissipation of funds.
- Cryptoassets have been used as a method of payment on **Darknet** marketplaces for a number of years as a way to promote and sell goods including drugs, weapons, extreme material and even criminal contracts.

It is important to use caution, conduct thorough research and to follow legal guidelines while using crypto and digital assets to avoid inadvertently participating in, or supporting, criminal activities including money laundering and terrorist financing.

2. Crypto Crime

Golden rules for preventing digital asset crime

Digital Assets are a volatile market in which prices can rise or fall rapidly. Criminals utilise the 'high risk, high reward' investment advertising for crypto as an opportunity to facilitate fraud.

1. **Don't be rushed into decisions** and take time to **do your research**. Seek advice from family, friends or independent assistance from an advisor accredited by the Financial Conduct Authority with knowledge of cryptoassets.

2. **If it sounds too good to be true, it probably is.** There are no guaranteed get-rich-quick schemes. Any taglines or phrases which can 'guarantee returns' or promise 'consistent profit' should be treated with caution.

3. **Be wary of unsolicited contact which prompts you to act or divulge information**; even if you are a customer with the company contacting you or know the person requesting it. **Log in to your accounts directly rather than clicking on links in messages, emails or on social media.**

4. **Look for subtle differences in URLs (web addresses), contact numbers and email addresses** to identify fraudulent activity.

METROPOLITAN POLICE

NASMA
National Association of Student Money Advisers

2. Crypto Crime

Primary messages

Primary messages

- Take your time — criminals will try to pressure you into making quick decisions; often describing or implying the situation is 'time sensitive' so you do not have the time to research and make an informed decision.
- Be aware of what personal information you are providing about yourself online and never provide copies of your personal documents to anyone you haven't met.
- Be aware of your physical surroundings when accessing your device, particularly when entering your PIN number or passcodes.
- Use additional biometric data such as a face or fingerprint ID, or enable multi-factor authentication (MFA) to secure high-value applications within devices. Use different PIN numbers and passwords for your phone to any digital wallet or banking applications.
- Use a strong and separate password for your email. The Metropolitan Police have created a video to help create a strong password which can be found at met.police.uk/littlemedia

2. Crypto Crime

Secondary messages

Secondary messages

- Don't store passwords or recovery seeds to any digital wallets on your phone.
- There are no 'get rich quick' schemes and, as with other investments, investments can go down as well as up. Your capital is at risk and you should avoid investing what you can't afford to lose or borrowing any money to do so.
- Block and report profiles to social media platforms from individuals who create a sense of obligation to respond. No matter how long you've been speaking to someone online and how much you trust them, never send them any money or allow them access to your bank account or digital wallet. Do not transfer money on their behalf, invest your own money on their advice or take out a loan for them.
- Cross-reference account names, even those with authentication marks, against official sites or independent platforms to make sure that you are viewing genuine accounts instead of near-identical copies. Research whether celebrities or influencers are genuinely promoting content and whether they have received any benefits for advertising.
- Check the legitimacy of businesses by referring to the FCA's warning list of unauthorised firms.

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.

METROPOLITAN POLICE

NASMA
National Association of Student Money Advisers

3. Templates

Long copy

Criminals committing fraud will try to create an emotional response in us and will pose as people we trust, respectable businesses, potential love interests, experts and charities. They add time pressure to make us react to the emotional response instead of stopping to think.

Research has found that there are four common linguistic strategies which criminals use to target people including requesting confidentiality or secrecy, appealing for urgency, attempting to establish credibility and referencing or implying trust.

Criminals are incredibly persuasive and use techniques to make us feel at ease and disguise any cause for concern. The language used is skilfully designed to abuse vulnerabilities, undermine people's confidence and manipulate decision making in a similar way to domestic abuse and psychological grooming. It will make requests seem reasonable and expected instead of a cause for concern. Criminals can seek out and isolate individuals, who may not even realise that they are being targeted.

Anyone can be the victim of fraud.

Stop, challenge and protect yourself from crime online.

3. Templates

Short copy

Criminals committing fraud will try to create an emotional response in us. They will pose as people we trust and add time pressure to make us react to the emotional response instead of stopping to think.

Criminals are incredibly persuasive and use social manipulation techniques to make us feel at ease and disguise any cause for concern. The language used is skilfully designed to abuse vulnerabilities, undermine people's confidence and manipulate decision making. It will make requests seem reasonable and expected instead of a cause for concern.

Anyone can be the victim of fraud.

Stop, challenge and protect yourself from crime online.

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/

METROPOLITAN POLICE

NASMA
National Association of Student Money Advisers

4. Assets

Social media - 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 assets 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. #LessRiskMoreReward

4. Assets

Social media - 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:

- Do your own research- Cryptoassets are incredibly volatile and values can go down as well as up. Do not purchase more than you are prepared to lose. #CryptoProtect
- Be wary of unsolicited contact which prompts you to act or divulge information. Log in to your accounts directly rather than clinking on links in messages, emails or on social media. #CryptoProtect
- Keep the keys to your digital wallet private. Providing the private key to others gives access to the assets in your wallet. Exchanges and banks will never ask for these. #CryptoProtect

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)

METROPOLITAN POLICE

NASMA
National Association of Student Money Advisers

5. 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.

METROPOLITAN POLICE

NASMA
National Association of Student Money Advisers

THANK YOU FOR YOUR SUPPORT

METROPOLITAN POLICE

NASMA
National Association of Student Money Advisers