FRAUD PREVENTION

ADVICE FOR CHINESE STUDENTS

CHINESE COMMUNITY WELLBEING SOCIETY 華康會

Devon & Cornwall POLICE

FRAUD PREVENTION

The Chinese community lose a significant amount of money to fraud, with Chinese students being a particular target. This document outlines the main fraud types affecting the Chinese community and advice on what to do should you become a victim of fraud.

TYPES OF FRAUD

We have seen many Chinese students be defrauded after seeing things advertised on WeChat. This can include exchanging sterling into Chinese Yuan at an attractive rate, or cheap flight tickets to China. Below are some more specific types of fraud to be aware of.

CHINESE EMBASSY SCAM

The victim is contacted by a fraudster impersonating someone from the Chinese Embassy or Chinese Police. They will usually say that the victim has been involved in money laundering or other illegal activity and that they need to pay a significant amount of money, or else they will be imprisoned or deported.

IMPERSONATION FRAUD

Fraudsters may pretend to be trusted officials, such as the bank or police. They may request your help with an 'investigation' or insist that there is fraud occurring on your account. They will convince you to transfer your money into a 'safe account', which will belong to the criminal, or hand it over to the criminal in person.

RENTAL FRAUD

Victims are tricked into paying an upfront fee to rent a property which does not exist, has already been rented out, or has been rented to multiple victims at the same time.

VIRTUAL KIDNAP

International students are instructed to cease contact with their relatives overseas, check into a hotel room, and take pictures/videos of themselves bound and blindfolded. These are then sent to relatives who are asked to send ransom payments for the safe release of their loved one.

MONEY MULING

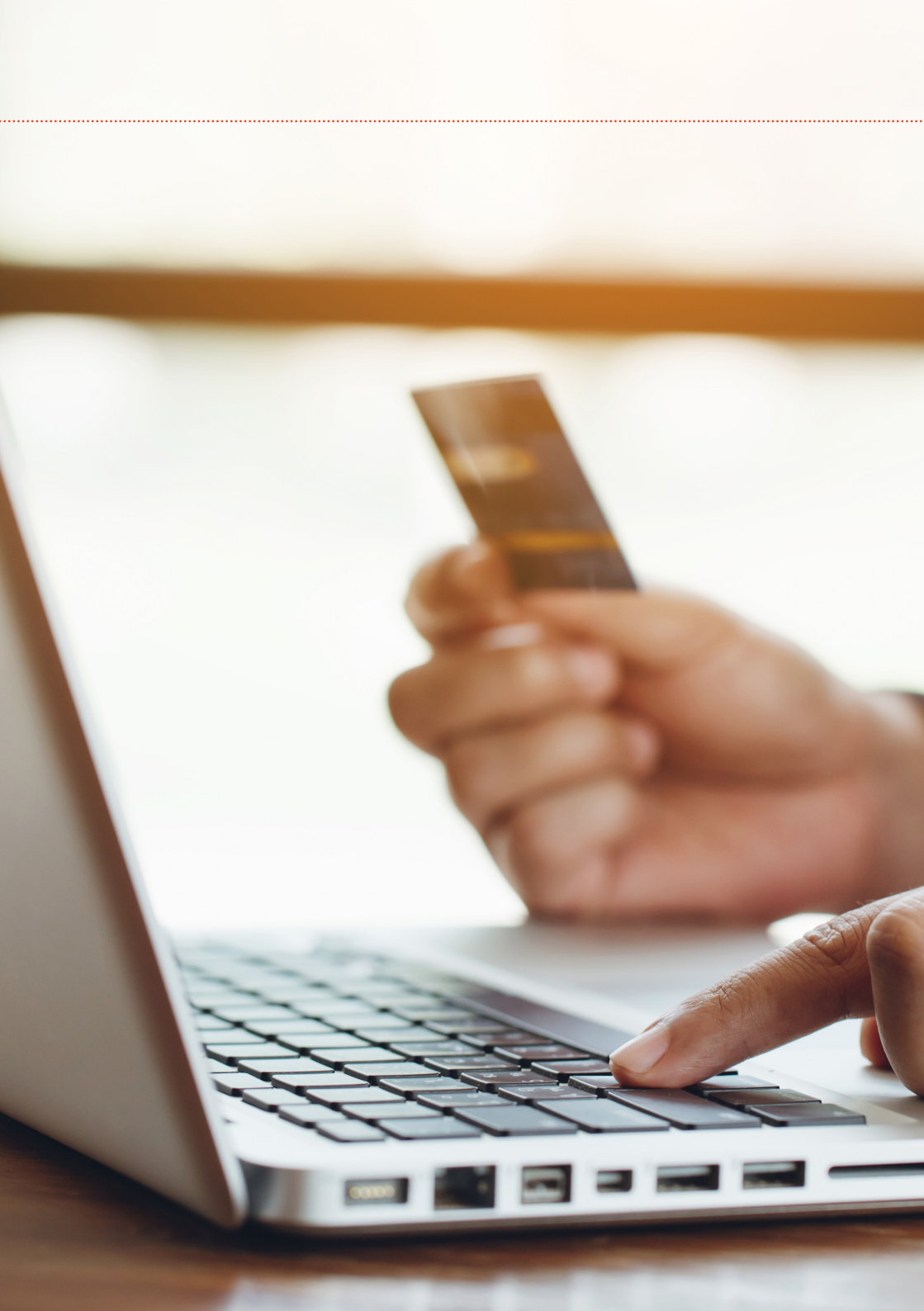
Students are often recruited by criminals to launder money through their bank accounts. This will be advertised as a risk free and easy way to make money. In reality, they are being enticed into committing a criminal offence.

INVESTMENT FRAUD

Fraudsters are advertising fraudulent cryptocurrency investments on social media, promising attractive returns. Seek independent financial advice before committing to any investment as it's difficult to tell a genuine investment opportunity apart from a fraudulent one.

PHISHING

Phishing texts and emails can come in many forms, for example notifying you of an apparent failed parcel delivery. Do not click on any links or attachments you are unsure of within a text or email or provide personal details. Texts can be forwarded to **7726** and emails to **report@phishing.gov.uk**



FRAUD RED FLAGS

Be wary of anyone asking for personal details over the phone.

Criminals may ask you to download a remote access tool which gives them full control of your device, insisting they are helping you 'fix' an issue.

A genuine person or agency should never rush or panic you.

Fraudsters often pose as trusted officials – be wary of any unexpected calls from organisations such as HMRC, the police or the bank.

The police or bank would never ever ask you to withdraw and hand over money to help with an investigation, or hand over your bank card(s).

If someone you are chatting to online or in a relationship with asks for money or gift cards, they are a fraudster. Never receive/transfer money on their behalf either – this is money laundering.

Be extremely cautious of anyone approaching you to make an investment – it's likely to be a fraud.

A person may contact you after you have been a victim of fraud, claiming they can get your money back (for a fee of course). This is known as 'Recovery Fraud'.

STAYING SAFE ONLINE

The National Cyber Security Centre (NCSC) provides some simple tips:

1 Use a strong and different password for each of your accounts. Three random words works best, such as 'HippoPizzaRocket'.

2 Turn on 2-step verification (2SV) where you can. This keeps criminals out of your accounts, even if they possess your password.

3 Protect your email account with a strong password and 2SV – criminals can use your email to access many of your personal accounts, leaving you vulnerable to identity theft.

4 Keep your devices up to date by ensuring you install the latest software and app updates which will include protection from viruses and other kinds of malware.

5 Use a password manager to help create and remember passwords.

6 Protect important data by backing it up to an external hard drive or cloud-based storage system.

TAKE 5 AND TELL 2

In any scenario where you are unsure about the communication you have received, **take 5** minutes away from it to think about what is being asked of you, and then **tell 2** people about it.

It's a simple technique, but it could save you a fortune.

HOW TO REPORT

If you have been a victim of fraud, please report this to Action Fraud.

This can either be done by calling

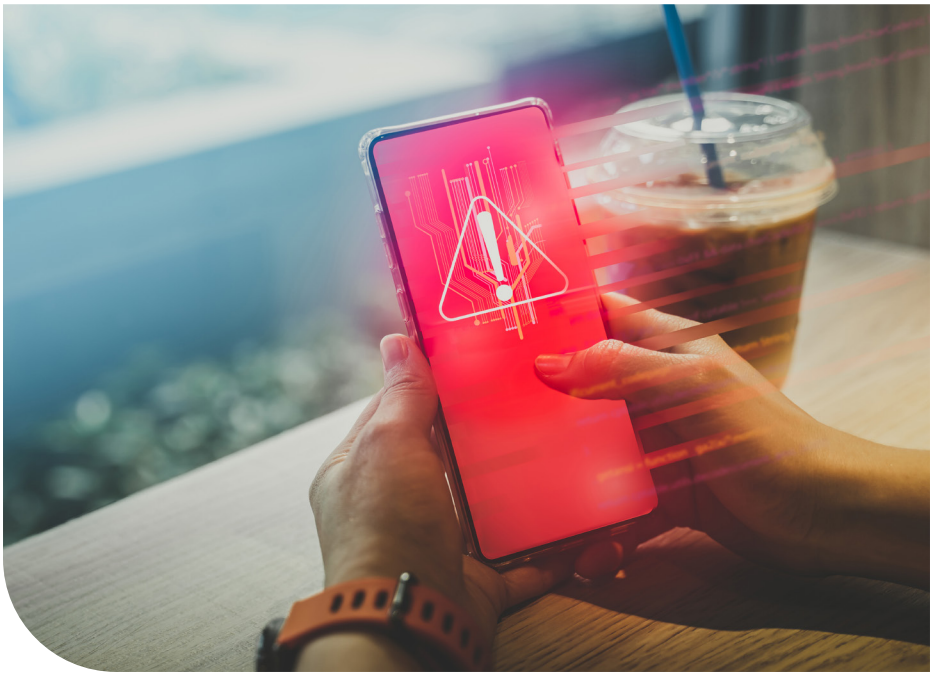
0300 123 2040

or online

www.actionfraud.police.uk

You can follow the link below for instructions on how to report a fraud in your preferred language

www.actionfraud.police.uk/reporting-in-local-language



SUPPORT

Being a victim of fraud can have a significant impact on mental health.

Victim Support

You can contact Victim Support on **0808 168 9111** if you would like additional support.

Chinese Lantern Project

You can also contact the Chinese Lantern Project on **0808 802 0012**, who provide support to members of the Chinese community.