





CONTENTS

Phishing

When criminals use deceptive emails, text messages, or phone calls to defraud unsuspecting individuals.

Rental Fraud

When students are requested to submit advance fees without inspecting the property, indicating potential rental fraud.

Parcel Fraud

When students receive notifications alleging the discovery of an illicit package addressed to them, under investigation by the police.

Money Muling

Individuals agree to disclose their bank details enabling the deposit of illicit funds into their accounts.

Ticket Fraud

When purchasing event tickets, exercise caution and be vigilant for indicators of fraudulent activity.

Fake Job Scams

When job seekers are targeted by fraudulent advertisements aimed at stealing personal information or money.


Purchasing Essays

Engaging with a third party to write your essay exposes you to potential scams.


Sextortion


Criminals manipulate victims into sharing explicit images or believing they have nude images, using them as leverage for extortion.

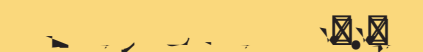
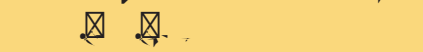
FURTHER INFORMATION, ADVICE AND GUIDANCE


www.ncsc.gov.uk/guidance/sextortion-scams-how-to-protect-yourself



www.takefive-stopfraud.org.uk


www.ncsc.gov.uk/collection/phishing-scams


www.nationalcrimeagency.gov.uk/moneymuling



www.revengepornhelpline.org.uk


www.getsafeonline.org


www.victimsupport.org.uk/



... – many victims who have paid have continued to get more demands for higher amounts of money.

... – note all details provided by the offender, for example, the email address, number, social media account you have been contacted from, Money Transfer Control Number (MTCN), any bank account details, any photos/videos sent, etc.

... – sometimes criminals will include your password in the correspondence to make it seem more legitimate. They have probably discovered this from a previous data breach. You can check if your account has been compromised and get future notifications by visiting – www.havebeenpwned.com

... – report them to the platform they have contacted you on and block the individual on the platform / in your contacts.



If you or someone you know has been a victim of sextortion, don't feel embarrassed because help and support are available. Don't panic. It can be very distressing for some people, but there is help, advice and guidance available. You are not alone.

WHAT ARE SCAMS AND FRAUDS?

Scams and Frauds are crimes in which deception is used for personal gain. It is usually to make money or obtain information through deception. With technology improving, fraudsters are becoming more sophisticated. Many types of scams and frauds exist.

By understanding the motives and signs of various scams, you can protect your personal information from scammers who may operate across international borders. The criminals behind these frauds do not discriminate; they will target anyone and have a complete disregard for the impact or consequences of their actions.

When online consider your actions, if something doesn't seem right then it probably isn't.

Any fraud and other financial crime should be reported to Action Fraud by visiting www.actionfraud.police.uk, or by calling 0300 123 2040. If you live in Scotland, please report it to Police Scotland by calling 101.



Social media catfishing refers to the deceptive practice of creating a false online identity to deceive and manipulate you. To minimise the risk of encountering potential scammers, you can make

PHISHING





To fool your spam filter, they may use odd 'spe11ings' or 'cApiTals' in the email subject.

Spam emails may also be addressed 'To our valued customer' or use your email address instead of your name.



Criminals pretending to be the Police or Home Office officials may contact you by email and tell you that you did not complete the correct paperwork upon entry into the country and must pay a fine or be deported.

Other scams involve Vishing which is making phone calls or leaving voice messages claiming to be the police, HMRC or courts and demanding payment of a fine to avoid prosecution.

Some scammers may persuade you that you are talking to Law Enforcement officials or direct you to

fake websites showing an extradition page with your pictures and details. In order to verify the identity of a police officer, call 101.



These scams are where you are contacted and offered discounts or 'help' to pay your tuition fees. You may be told you can have a bursary if you()cs.a]TJa5mwith your



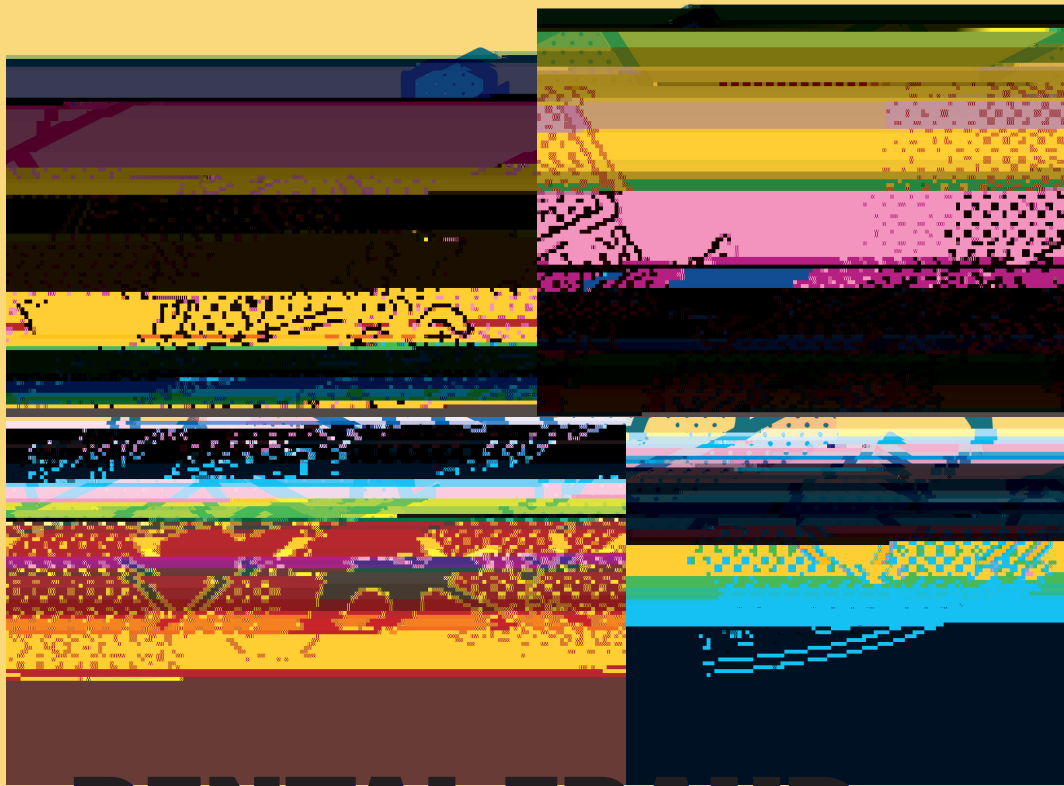
PURCHASING/ WRITING ESSAYS ONLINE

Avoid individuals and companies in your home country advertising tuition payment services not listed on the university website or endorsed by the university.

Always check with the university before agreeing to process any payment through a third party.

Never share personal, banking or financial information with anyone who lacks a verifiable relationship with the university. Always verify whom you are speaking with.

Always be vigilant about how (in person, by phone, via social media) and



RENTAL FRAUD

Fake job adverts are designed to target job seekers in order to steal their personal information or money.

Scams are bestusq 1q 1n order toa 0 0 2112262 0.06 /1002 T cultr to Scw [potstuirsovictims'r to





FRAUDULENT JOB SCAMS



You may be asked to pay a fee in advance without viewing the property. In reality, the property may not exist, may already be rented out or have been rented to multiple victims simultaneously.

You would then lose the upfront fee you have paid and cannot rent the property you thought you had secured.



Only send money to people advertising rental properties online once you are sure the advertiser is genuine. If you need to secure

accommodation in the UKw (advertising



☒ ☒ ☒ ☒ ☒ ☒ ☒



MONEY MULES



Students are a target because younger people are less likely to have a criminal history and their clean account is less suspicious to banks.

Recruitment is often through:

- Unsolicited e-mails asking for assistance
- Contact via social networking sites
- False vacancies on websites posing as legitimate businesses
- Classified adverts in the press and online which look legitimate.

You might see genuine online adverts but don't be fooled.

Take a moment to consider what is being offered.

Terms such as 'earn from the comfort of your own home', 'must be willing to provide bank details' and 'make £250 a week – no experience necessary' are red flags that could indicate you are being targeted as a money mule.

If you have any information about money muling, call the Police on **101** for non-emergencies, or **999** in an emergency.

You can also contact Crimestoppers anonymously on **0 800 111** or online at www.crimestoppers-uk.org

Remember, do not share or hand over your bank account details to family/friends when returning to your home country.

Transferring criminal money is a crime. While it may appear to be a simple way to make money, engaging in such activities could result in acquiring a criminal record.

For further information, visit www.nationalcrimeagency.gov.uk/moneymuling