STUDENT ONLINE SAFETY GUIDE

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

INTRODUCTION

Police Scotland aims to provide you with important safety advice on how you can avoid becoming a victim of crime.

Common frauds that students are experiencing today can range from the more recognisable face-to-face fraud to those carried out by someone anonymously online.

Advances in technology enable you to carry out daily tasks more easily, but can be frequently exploited by fraudsters interested in your personal information and money.

This guide will equip you with information and advice to increase your awareness, prepare you to identify potential frauds and prevent the loss of your valuable data to those intent on stealing it.

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.

Cyber Aware 6

What are scams and frauds? 7

Fraud Red Flags
Common fraud indicators and warnings 8

Phishing
Fake tax refunds from HMRC
Student loans phishing scam
UK visa / Fraudulent home office / Fake police scam
Tuition payment scams
Bank account at risk 10

Rental fraud 14

Parcel fraud 16

Money muling 18

Ticket fraud 20

Fraudulent job scams
Advance fee scams
Premium rate phone interview scams
Identity fraud and identity theft 22

Purchasing/writing essays online 24

Sextortion
Advice for victims of sextortion 26

Support and wellbeing 30

Further information, advice and guidance 31

CYBER AWARE

Advice on how to stay secure online from the UK's National Cyber Security Centre:

- **Use a strong and different password for your email using three random words**
  Combining three random words that each mean something to you is a great way to create a password that is easy to remember but hard to crack.
- **Turn on 2-Step Verification (2SV) for your email**
  2SV gives you twice the protection, so even if cyber criminals have your password they can't access your email. You won't be asked for this every time you check your email.
- **Save passwords in a Password Manager**
  A password manager can store all your passwords securely, so you don't have to worry about remembering them.
- **Backing up your data**
  A backup is a copy of your important data stored in a separate safe location, usually on the internet (cloud storage) or on removable media (such as USB, SD card, or external hard drive).
- **Update your devices**
  Prompted updates from your device manufacturer includes protection from viruses and other malware and will often include improvements and new features.

Further information
Cyber Aware - NCSC.GOV.UK

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 the police by phoning 101.

FRAUD RED FLAGS

Common fraud indicators and warnings.

- Be wary of any unexpected calls from organisations such as HMRC, the Police or the bank.
- The Police or the bank would never ask you to withdraw and hand over money to help 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 or transfer money on their behalf either – this is money laundering.
- A genuine person or agency would never ask you to lie to friends / family or to keep contact with the 'organisation' private.
- A person may contact you after you have been the victim of fraud, claiming they can get your money back (for a fee of course). This is known as 'Recovery fraud'.
- Criminals may ask you to download a remote access tool which gives them full control of your device, insisting this is to help you 'fix' an issue.
- A genuine person or agency should never rush or panic you.
- It is common for fraudsters to pose as trusted officials. Be wary of any unexpected calls from organisations such as HMRC, the Police or the bank.
- Be extremely cautious of anyone approaching you to make an investment – it's likely a scam.
- Be wary of anyone asking for personal access details over the phone.

PHISHING

The purpose of a scam email is often to get you to click a link. This may take you to a fake website or might download malware to your device. This is known as 'Phishing'.

Fake tax refunds from HMRC

HMRC is warning you to be wary of potential scams, especially if you have a part-time job and are new to interacting with the agency. Nearly half of all tax scams offer fake tax refunds, which HMRC will never offer by SMS or email.

If in doubt, HMRC advises not to reply directly to anything suspicious but contact HMRC through GOV.UK straight away.

Forward suspicious emails to **report@phishing.gov.uk**

Student loans phishing scam

You may receive an email that appears legitimate asking for your bank details.

The email claims accounts have been suspended due to incomplete student information urging you to update your details using a web link. This link may lead to a fake website designed to harvest personal information.

Don't assume anyone who emailed you is who they say they are. Be cautious if an email asks you to make a payment, log in to an online account or offer a deal.

Remember, no bank will email you requesting your password or sensitive information by clicking on a link and visiting a website.

If in doubt, check it's genuine by asking the company itself.

Never follow links provided in suspicious emails, find the official website or customer support number using a separate browser and search engine.

Remember, fraudulent emails that pose as an official company or organisation may have poor-quality spelling, grammar, graphic design or image quality.

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.

UK visa / Fraudulent home office / Fake police scam

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.

Tuition Payment Scams

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 supply them with your bank details.

Scammers sometimes present themselves as government agencies and demand an 'international student tariff' payment. They threaten to revoke your visa if payment is not made via money order, wire transfer or other hard-to-track methods.

How to avoid the scam:

Be wary of the person offering to pay tuition on your behalf or promising a discount upon payment. If the offer sounds too good to be true, it almost certainly is.

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 where (immigration lines, international student meetings etc.) scammers may approach you. When in doubt, contact the university. Don't be pressured by a deadline or threats of retaliation.

Bank account at risk

A scammer may phone claiming to be from your bank stating that your accounts are at risk of an attack. They advise you to move your money to a 'safe account' they have set up for you but in reality it is the scammer's bank account.

A bank will never contact you unexpectedly, ask for passwords, PINs, account details or asking you to move money.

Hang up and call your bank from the number on the back of your bank card.

The Police will never request the transfer of money or payment in vouchers.

RENTAL FRAUD

Finding somewhere safe, convenient and affordable to live may be one of your main concerns. Unfortunately, scammers know how important student accommodation is and could try to take advantage of your need to find a home.

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.

Protect yourself from rental fraud:

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 UK from overseas, seek the help of the employer, university or Student Union you are coming to or ask a friend, contact or relative to check if the property exists and is available.

Only make payment once you or a reliable contact has visited the property with an agent or the landlord.

Refrain from being pressured into transferring large sums of money. Be sceptical if you're asked to send money via a money transfer service.

PARCEL FRAUD

Criminals posing as police officers or customs officials may contact you by phone or text. They may claim you are under criminal investigation after a parcel addressed to you was stopped in your home country.

They may send images of fake police warrant/ID cards and instruct you not to tell anyone about the 'investigation'.

They may then instruct you to transfer money to a bank account within your home country so it can be checked to ensure it is legal. This money is not returned; instead, more is demanded.

Protect yourself from parcel fraud:

This scam has left students in severe financial difficulties. Do not assume people are who they say they are on a phone call or text, especially if they ask for personal or financial details.

Police will never demand your bank account details, passport information, address or ask to monitor your movements over the phone.

If you are unsure about any phone calls, emails or messages, do not comply with any requests. Talk it over with someone you trust or the police.

MONEY MULES

This scheme involves a person agreeing to share their bank details to deposit money into their account. Funds are then withdrawn and transferred onward – with the account holder retaining a percentage for their compliance.

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.

Also be wary of persons looking to recruit you, to use a phone's digital wallet to buy large volumes of gift cards at supermarket self-service checkouts. The phone likely contains stolen digital wallets and the purchased gift cards will later be converted into products which can be removed from the country.

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

You can also contact Crimestoppers anonymously on **0800 555 111** 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

TICKET FRAUD

If you are considering buying tickets to a live event, remember to look out for the signs of ticket fraud.

Criminals often set up fake websites or social media profiles to sell tickets to concerts or sports events that are either fraudulent or don't exist.

Websites may even look like genuine organisations, but subtle changes in the URL can indicate that it's fraudulent.

Criminals might have used images of tickets which appear genuine to commit fraud.

They may contact you via text, email or DM to advertise fake tickets. They create fake posts or pages on social media to scam those looking for tickets. It is always safest to book tickets through official sellers that are members of the self-regulatory body, the Society of Ticket Agents and Retailers (STAR), as anything else could be a scam.

How to spot ticket fraud:

- You see an offer for a ticket in an email or a message/DM.
- You're offered tickets for a high demand or sold out event at a 'too good to be true' price.
- You're asked to pay by bank transfer only and not via the secure payment methods recommended by reputable online retailers.
- You see a website that looks similar to a genuine organisation, but there are subtle changes to the URL.
- You're told that a customer representative will be arranged to meet you outside the venue.

FRAUDULENT JOB SCAMS

Simply, it's fake online job advertising targeting job seekers to steal personal information or money.

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

Scams are becoming extremely sophisticated, making it difficult to know what's genuine or fake.

Opportunists are tailoring scams to potential victims' backgrounds before targeting them with convincing lies, attempting to collect personal information and conning them out of money.

Common Scams

Advance fee scams
Fraudsters ask for money upfront for things like CV writing, admin charges or carrying out background security checks. They can also claim to be travel agents when people are looking to work abroad.

Premium rate phone interview scams
Scammers send you texts or missed calls asking you to call premium rate numbers for an initial phone interview.

You are put on hold for an extended period, making the call last up to an hour. Costs to unsuspecting victims can total hundreds of pounds.

Please, remember:

- Never part with money upfront for background checks or admin fees.
- If invited to a phone interview, ensure the interviewer phones you – you may be at risk of a premium rate number scam.

Identity fraud and identity theft
Fraudsters pose as employers and ask for personal information, bank statements, passport details and driving licences as pre-employment checks.

Please, remember:

- Don't make personal and sensitive information visible on your social media profiles.
- Don't share any information until you have met face-to-face and only when you're sure it's a genuine company.

PURCHASING/ WRITING ESSAYS ONLINE

You may be tempted to use a paper writing service to fulfil assignments. This is not only unethical but is also a market for scammers and fraudulent activity.

If you are tempted to use essay mills, be aware that you are likely opening yourself up to being scammed.

It is not uncommon for students to become victims of extortion, where criminals will threaten to contact the student's university and inform them of the attempted purchase in return for payment.

SEXTORTION

Online sextortion is a form of sexual blackmail. It involves criminals targeting you through dating apps, social media, text or email and manipulate you into sharing sexual images/videos that they later use to demand payments under threats of public exposure.

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 your profiles private, limiting access to personal information and making yourself a less attractive target.

Criminals may use a false identity to befriend you online and then threaten to send images to your family and friends.

How to protect yourself:

- Be cautious when using the internet. Only activate your camera when you want to. Make sure it is 'off' at all times when not in use or use a webcam cover. Never allow yourself to be duped into activity that you will later regret.
- If using video chat apps, be alert to the fact that 'contacts' are not always who they say they are. If you allow a relationship to develop be wary if unusual requests are made of you.
- If you are chatting with somebody using a webcam be guarded on what you say and do.

Advice for victims of sextortion

Contact your local police immediately. The police will take your case seriously, deal with it in confidence and not judge you for being in this situation.

Don't communicate further with criminals – take screenshots of all your communication.

Deactivating your account temporarily rather than shutting it down will mean the data is preserved and will help police to collect evidence. Please note, mass phishing emails about sextortion are common, and should be forwarded to the NCSC's Suspicious Email Reporting Service (SERS) at report@phishing.gov.uk.

Don't pay – many victims who have paid have continued to get more demands for higher amounts of money.

Preserve evidence – 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.

Secure your accounts – 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.haveibeenpwned.com

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

Do not delete any correspondence.

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.

SUPPORT AND WELLBEING

Please, seek help from your university/college wellbeing services for assistance and guidance.

Samaritans
A free, confidential emotional support service available 24/7, 365 days a year for anyone in the UK and Ireland
Call 116 123
www.samaritans.org

Breathing Space
A free, confidential service for anyone in Scotland experiencing low mood, depression or anxiety. It has a helpline and a webchat; see the website for times available
www.breathingspace.scot

Papyrus
Provides confidential advice and support and works to prevent young suicide in the UK
www.papyrus-uk.org

CALM
A campaign to try to reduce suicide rates, particularly in men. CALM has a helpline and webchat available 5 pm – midnight, 365 days a year
www.thecalmzone.net

FURTHER INFORMATION, ADVICE AND GUIDANCE

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

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

Revenge Porn Helpline - Sextortion
www.revengepornhelpline.org.uk

Get Safe Online
www.getsafeonline.org

Victim Support Scotland
www.victimsupport.scot

Take Five
www.takefive-stopfraud.org.uk

Money Mules
www.nationalcrimeagency.gov.uk/moneymuling

Police Scotland
www.scotland.police.uk/advice-and-information/internet-safety

POLICE
SCOTLAND
Keeping people safe
POILEAS ALBA

Created by Police Scotland on 01/08/2023

16916_25_psm