Keeping Student Communities Safe Across Scotland

#Online Student Safety Guide 2022

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Experiencing student life for the first time is exciting. Making new friends, living away from home and the joys of student life are life changing experiences but can expose you to risk of becoming a victim of crime.

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

Common frauds 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 more easily carry out day-to-day tasks which are frequently exploited by fraudsters interested in your personal information and money.

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

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Inside the Online Student Safety Guide **2022**

What is a Scam?

#1 Phishing
When criminals use scam emails, text messages or phone calls to trick their victims.

#2 Rental Fraud
Where students looking for properties are asked to pay a fee in advance without viewing the property.

#3 Money Mules
A person agrees to share their bank details so that sums of money can be deposited into their account.

#4 Ticket Fraud
Thinking of buying tickets for an event? Look out for the signs of ticket fraud.

#5 Fake Job Scams
Fake advertising targeting job seekers to steal personal information or money.

#6 Purchasing Essays
Paying a third party to write your essay? It's unethical and you could easily be scammed.

#7 Sextortion
Scammers target students and manipulate them into sharing sexual images.

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

What is a **Scam?**

A scam is an attempt to get you to part with your money or information through deception.

This type of crime is under-reported and scammers can be difficult to trace because they often operate across international waters and as part of large, criminal international organisations which require complex and co-ordinated investigations.

The fraudsters behind these crimes do not discriminate, they will prey on anyone and have a complete disregard for the impact or consequences of their actions.

Act with caution when online. Your name, birthday and address can at times be enough to expose you to potential harm if they fall into the wrong hands.

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Scam #1

Phishing

‘Phishing’ is when criminals use scam emails, text messages or phone calls to trick their victims. The aim is often to make you visit a website which may download a virus onto your computer or steal bank details or other personal information. Student specific phishing scams include:

Fake tax refunds from HMRC

When you receive a text message or email from HMRC advising you are due a tax refund and you need to provide your personal details.

HMRC is warning university students to be wary of potential scams, especially if they 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 claiming to be from HMRC to phishing@hmrc.gov.uk and texts to 60599

Student Loans Company Phishing Scam

When you receive an email from what appears to be the Student Awards Agency Scotland (SAAS) asking for their bank details.

The email claims accounts have been suspended due to incomplete student information, therefore, urging the recipient to update their details using a web link which then leads to a fake website with the aim of harvesting personal details.

Don’t assume anyone who has sent you an email is who they say they are. If an email asks you to make a payment, log in to an online account or offer you a deal, be cautious. No bank would email you for passwords or any other 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 usually have poor-quality spelling, grammar, graphic design or image quality.

They may use odd ‘spe11lings’ or ‘cApiTals’ in the email subject to fool your spam filter.

If they know your email address but not your name, it’ll begin with something like ‘To our valued customer’ or ‘Dear’ followed by your email address.

Scam #1

Phishing

UK Visa / Fake Home Office / Fake Police Scam

Fake Police or Home Office officials contact the student and tell them they did not complete the correct paperwork upon entry into the country and that they must pay a fine or be deported.

Other scams involve callers pretending to be the Police and demanding students pay taxes, quoting HMRC and the courts.

Some scammers may persuade students that they are talking to Law Enforcement officials or direct them to fake websites showing an extradition page with their pictures and details.

Tuition Payment Scams

Where students are contacted and offered discounts or 'help' to pay their tuition fees. They may be told they can have a bursary if they supply their bank details.

Scammers represent themselves as government agencies and demand payment of an 'international student tariff.' They threaten to revoke a student's 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 make a tuition payment 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 that are not listed on the universities 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 who you are speaking with.

Always be vigilant about *how* (in person, by phone, via social media) and *where* (immigration lines, international admitted students meetings and so on) you may be approached by scammers. When in doubt, contact the university. Never be pressured by any proclaimed deadline or threats of retaliation.

The Police, Local Authorities and Government Agencies
will never request the transfer of money into other accounts

Scam #2

Rental Fraud

This is where students looking for properties are asked to pay a fee in advance without viewing the property. In reality, the property does not exist, has already been rented out or has been rented to multiple victims at the same time.

The victim then loses the upfront fee they have paid and is not able to rent the property they thought they had secured with the payment. Rental fraudsters often target students looking for university accommodation.

Protect yourself from rental fraud

Do not send money to anyone advertising rental properties online until you are certain the advertiser is genuine.

If you need to secure accommodation in the UK from overseas, seek the help of the employer or university you are coming to or get a friend, contact or relative to check if the property exists and is available.

Do not pay any money until you or a reliable contact has visited the property with an agent or the landlord.

Do not be pressurised into transferring large sums of money. Transfer funds to a bank account having obtained the details by contacting the landlord or agent directly after the above steps have been followed. Be sceptical if you're asked to transfer any money via a money transfer service like Western Union.

Scam #3

Money Mules

This scheme involves a person agreeing to share their bank details so that sums of money can be deposited into their account. These are then withdrawn and transferred onwards – 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 online ads that appear genuine, but don't be fooled, take a moment to consider what is actually being offered.

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

If you have any information about money mules, call Police: 101 for non-emergencies, 999 in an emergency or contact independent charity Crimestoppers anonymously on 0800 555 111 or online at www.crimestoppers-uk.org

Alternatively, support will be available from your student advisor.

For further information visit www.moneymules.co.uk/tips.html

Scam #4

Ticket Fraud

If you are thinking of 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 major events (such as sports, music or theatre) 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 genuine tickets to commit fraud. They may get in touch 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 alone, in an email or in 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 that of a genuine organisation but there are subtle changes to the URL

You're told that a customer representative will be arranged to meet outside the venue

Scam #5

Fake Job Scams

In simple terms, it's fake online job advertising, targeting job seekers with the aim of stealing personal information or money.

What are the main scams I should look out for?

Scams are becoming extremely sophisticated which can make it really 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 con them out of money.

Common Scams

Fake Job Adverts
These are listed to entice people to apply so fraudsters can gain personal information including national insurance details, bank details, date of birth and address to steal your identity.

Advance Fee Scams
Fraudsters ask for money upfront for things like CV writing, admin charges, carrying out background security checks and even claiming to be travel agents when people are looking to work abroad.

Premium Rate Phone Interview Scams
Scammers send texts or missed call messages to victims asking them to call premium rate numbers for an initial phone interview. People are put on hold for a long period of time, making the call last up to an hour. Costs to unsuspecting victims can total hundreds of pounds.

Identify Fraud and Identity Theft
Fraudsters pose as employers and ask for personal information, bank statements, passport details and driving licences as pre-employment checks.

Advice from students who have fallen victim to online fraud

Don't make personal and sensitive information visible on your social media profiles

Never part with money upfront for background checks or admin fees

If invited to do a phone interview, make sure the interviewer phones you –
(you may be at risk of a premium rate number scam)

Don't accept money for anything (Money Mule), for 'working from home' scams

Don't share any information until you have met face-to-face, and then only when you're sure it's a genuine company

Scam #6

Purchasing Essays Online

Students 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 you are likely opening yourself up to be scammed.

It is not uncommon for students to become victims of extortion where criminals will threaten to contact the students respective university making them aware of the attempted purchase in return for payment.

Police Scotland urges students to refrain from using such websites to avoid the risk of becoming victims of any scam and being excluded from their respective place of learning

Tips to stay safe online

Don’t share personal information

Don’t share the name of your educational institutions

Scam #7

Sextortion

This is where scammers target students via social media, text or email and manipulate them into sharing sexual images that they later use to demand payments under threats of public exposure.

How to protect yourself

Do not open attachments from people you do not know. //links can secretly hack your electronic devices using malware to gain access to your private data, photos, and contacts, or control your web camera and microphone without your knowledge

Turn off your electrical devices and web cameras when not in use.

Use a camera cover for your laptop and other devices

Never send compromising images of yourself to anyone no matter who they are

Scam #7

Sextortion

Advice for victims of Sextortion

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

Don't communicate further with the 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. Be aware that mass phishing emails about sextortion are common and if you were contacted by email, you can forward the email to the NCSC's Suspicious Email Reporting Service (SERS) at report@phishing.gov.uk and then delete it.

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

Preserve evidence
Make a note of all details provided by the offenders, for example; the email address, number or social media account that you have been contacted from; the Western Union or MoneyGram Money Transfer Control Number (MTCN); any bank account details; any photos/ videos that were sent, etc.

Secure your accounts
Sometimes they will include your password in the correspondence to make it seem more legitimate. They have probably discovered this from a previous data breach.

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, help and support are available.

Don’t panic. It can be a very distressing situation for some people but there is lots of help, advice and guidance out there. You are not alone.

Essential Advice

Don’t risk losing your assignments. From trusty memory sticks to the cloud, there are plenty of ways to save your hard graft. From the cloud to external hard drives and memory, there are plenty of options.

Cloud Storage
Good method to back up your computer without having to copy your stuff to a disc or hard drive. Easy access to lesson plan notes to share across several devices.

Offline Backup Storage
The purpose of an ‘offline backup’ is to remain unaffected should an incident impact your live environment. Never have all backups connected (or ‘hot’) at the same time. With at least one backup offline an incident cannot affect all of your backups simultaneously.

Streaming (Malware)
Beware of websites offering free stream or downloads. These websites can be rife with malware. Downloading from these may end up infecting your device and can steal personal information and passwords stored on your device.

Strong Passwords
Your password should be strong and different. Combining 3 random words is a great way to create a password that is easy to remember but hard to crack. Do not use words that can be guessed (like your pet's name).

You can include numbers and symbols if needed. For example, "Hippo!PizzaRocket1"

Turn on 2-Step Verification (2SV)
This gives you twice the protection so even if cyber criminals have your password they can't access your email. For example, getting a code sent to your phone when you sign in using a new device or change settings such as your password.

Update your Device
Applying security updates promptly will help protect your devices and accounts. Updates include protection from viruses and other kinds of malware and will often include improvements and new features. If you receive a prompt to update your device (or apps), don't ignore it.

If you ever need to speak to us, you can contact us online or by calling 101.

This form can be used to get in touch with Police Scotland for issues of a non-serious nature:

https://www.scotland.police.uk/secureforms/contact/

In an emergency, always call 999.

SEXTORTION IS A CRIME

MANY PEOPLE USE WEBCAMS FOR FLIRTING AND CYBERSEX

BUT SOMETIMES PEOPLE AREN'T WHO THEY SAY THEY ARE

Criminals befriend victims online then persuade them to perform sexual acts in front of their webcam.

These webcam videos are recorded by criminals who then threaten to share the images with friends and family.

THINK BEFORE YOU BARE ALL

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Support and Wellbeing

Samaritans
www.samaritans.org/how-we-can-help-you/contact-us
A free, confidential emotional support service that is available 24/7, 365 days a year for anyone in the UK and Ireland.

Breathing Space
http://breathingspace.scot/
A free, confidential service for anyone in Scotland experiencing low mood, depression or anxiety. Has a helpline and a webchat, see the website for times available.

Papyrus
Provides confidential advice and support and works to prevent young suicide in the UK.

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

Choose Life
www.chooselife.net/ask
Provides links to a list of services for anyone feeling low, or struggling in a crisis.

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Further information, advice and guidance

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

Phishing - Spot and report scam emails, texts, websites
www.ncsc.gov.uk/collection/phishing-scams

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

Get Safe Online
www.getsafeonline.org/

Victim Support Scotland
https://victimsupport.scot/

Take Five
www.takefive-stopfraud.org.uk/

Money Mules
www.moneymules.co.uk/

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Keeping Student Communities Safe Across Scotland

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA