Takes around **9 min read**

General

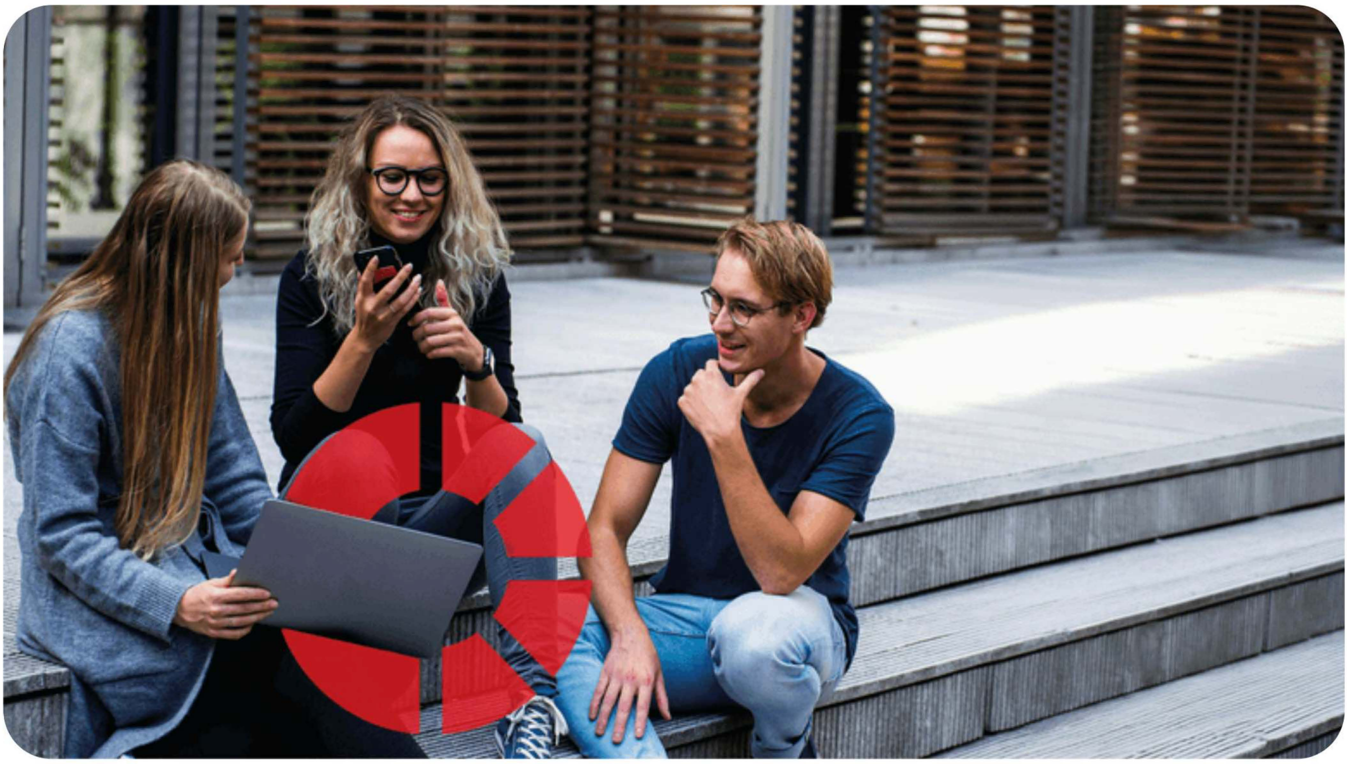
Published

20 July 2026
Last update 20 July 2026

Click to exit site

University students booklet

Protecting yourself from cyber crime and fraud: A guide for university students.



Jump to a section

- Online safety checklist

Students, particularly international students, in the UK are a common target for criminals.

Criminals use a wide range of tactics to steal your money or obtain personal information that can be used later in a fraud attempt.

They operate on websites and apps, by email, text, phone, post or in person, including on your doorstep.

This booklet will explain some steps you can take to secure your personal and financial information.

Common frauds targeting students

Students are often targeted by fraud which can include calls, emails, or social media messages pretending to be from legitimate organisations. These may involve demand for money or personal information, often under the guise of immigration fines or other serious issues.

To stay safe, students should be cautious of unsolicited offers of easy money, research job offers from overseas and avoid sharing personal details unless absolutely certain of their legitimacy. If in doubt, it’s best to end the communication and report any suspicious contacts – find out more on the Report Fraud page.

Student loan fraud

Criminals may impersonate the Student Loans Company (SLC) by targeting eligible international students with fake emails or calls. If you are an eligible student and receive a message or call claiming to be from SLC that doesn’t feel right,

- **Break the contact** - Avoid clicking on any links or making any payments.

- **Check if it's genuine** - By logging into your online account or contact SLC directly using an email address or phone number on their official website.

Tuition fee fraud

These types of frauds typically involve students receiving unsolicited messages from individuals or "agents" claiming they can offer discounts on tuition fee payments.

If you receive an offer like this and something doesn't feel right, STOP!

Seek advice from staff at your university before you transfer money or share any personal or financial information.

UCAS fraud

The Universities and Colleges Admissions Service (UCAS) is often impersonated by criminals targeting students.

If you receive an email claiming to be from UCAS and you're not sure that it is genuine, please send it to reportabuse@ucas.ac.uk so it can be investigated. UCAS will then let you know whether or not the email is genuine.

Until they confirm it is genuine:

- Do not reply to the email
- Do not click any links in it
- Do not open any attachments

UCAS will never ask you for your bank or login details via email.

girl_with_headphones_1x.png

Visa and immigration fraud

This type of fraud often involves criminals impersonating Home Office officials or staff from a Visa Application Centre. Criminals may offer to speed up or assist with your visa application in exchange for payment, or use threats such as deportation, visa cancellation, or criminal prosecution to pressure you into complying with their demands. If you receive a message or email regarding your visa application that doesn't feel right, STOP!

Legitimate visa officers will NEVER contact you to ask for money in person or by email or phone.

UK Visas and Immigration (UKVI) will NEVER text you requesting personal details.

Email and social media hacking

Email and social media hacking is the most common form of cyber crime in the UK. If someone breaks into your email account, they could access your other online accounts using the 'forgot password' feature, or access personal information which they can later use to defraud you or people you know.

Use passkeys to secure your online accounts

Passkeys are a more secure alternative to passwords that you don't need to remember as they are created and managed safely by the software on your device(s).

Where passkeys are not an available option, you should continue to use strong passwords, for example generated by a password manager, and enable 2-step verification. This remains a strong defence against online attackers.

man_with_box_1x.png

Rental fraud

Rental fraud involves criminals deceiving students looking for university accommodation. The goal is to deceive potential renters into paying upfront for properties that don't exist. Once the criminals have received payment, they cease contact with the victim.

- **Always view the property:** You, or someone you trust, should view the property in-person before you sign any contracts or make payment.
- **Overseas students:** If you are coming to study in the UK from overseas get advice from the university you are coming to about renting property. If you are unsure about anything a landlord is asking you to do, speak to a trusted friend or family member, or seek professional independent advice.
- **Signs of fraud:** Use the information provided in the property listing, such as the address and photos, to look online for what other information you

can find about the property you would like to rent. Criminals often steal information from genuine listings to create fake listings of their own.

- **Payment:** Where possible, avoid bank transfer payments; use credit or debit cards for better protection.

Recruitment fraud

Criminals create fake job adverts or pretend to be real companies to target international students. Criminals post adverts on social media and recruitment websites or contact you directly about a job opportunity. The criminals usually ask you to pay money before you can start the job. They may say the money is needed for equipment, training, a security check, or other recruitment costs. They often promise to pay the money back later. Once you have sent the money, they will stop responding to your messages.

- Real employers won't ask you to pay for expenses or training in advance.
- Research the hiring company and check their contact details match the details on their website before sharing personal details with them. You can check this via Companies House in the UK.

If at any stage you are concerned about what you are being asked to do, seek advice from staff at your university.

Financial exploitation

Financial exploitation, otherwise known as money muling, is where people, often unknowingly, are recruited by criminals to move money through different bank accounts. They might ask you to move money through your account and onto another, and offer a small percentage in return. This can be through bank accounts, crypto wallets or by withdrawing cash.

They do this under the guise of a job opportunity or a way to get money quickly, but this is linked to criminal activity. Even if you are unaware that the money was illegally obtained, you could still suffer the consequences. It could cause your bank account to be closed or frozen. This could result in prosecution, impact your place at university, and affect your future employment prospects.

- Do not allow others to use your bank account or move money for someone else, especially if you're offered money or rewards.
- Never give your financial details to someone you don't know and trust.

- Be wary of offers on social media or through informal channels that offer you a way to 'get rich quick'.

Police impersonation fraud

International students from mainland China and Hong Kong are often targeted by criminals impersonating Chinese law enforcement and government agencies. In most cases, the criminals will falsely accuse the victim of committing money laundering or other illegal activity and then claim that a significant payment is required in order to avoid imprisonment or deportation.

If you receive a call or message like this, **STOP!** This is likely a fraud.

- Seek advice from staff at your university before you make any payments or share personal information.
- You can also seek advice from the Chinese embassy in the UK by contacting them using the details on their official website.

How to spot a phishing email

With the rise of artificial intelligence (AI), fake emails are getting more convincing all the time. But there can be some signs that an email isn't genuine, so look out for:

- an amazing, time-limited offer or strong encouragement to 'click here/now' – encouraging you to respond quickly
- an email that doesn't use your name – perhaps they don't really know who you are
- spelling and grammar mistakes (though phishing emails are getting more sophisticated than they used to be)
- imagery or design that looks familiar but doesn't feel quite right
- an unusual email address – it might look a bit similar, but does it really match the official company's email address?
- encouragement to click on an unknown link – if you're not sure, visit the organisation's website directly rather than clicking through
- a request for you to share personal data.

Phishing: How to report fraudulent emails, texts and calls

“Phishing” is when criminals use 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 device, or steal bank details or other personal information.

If you’ve received a text, email or call that doesn’t feel right, STOP!

- Break the contact: don’t reply, don’t click on any links, don’t call any phone numbers or make any payments. If it’s a phone call, hang up.
- Check if it’s genuine: contact the organisation directly. Don’t use the numbers or address in the message – use the details from their official website or app.
- Remember, your bank (or any other official source) will never ask you to supply personal information via email or call and ask you to confirm your bank account details.
- Government departments, including the police, would also never ask you for payment to help with an investigation. They would not ask for payment of a fine over email, text or call.

How to report

- Report suspicious emails by forwarding them to report@phishing.gov.uk
- Report suspicious text messages by forwarding them to 7726 (it’s free of charge)
- Report suspicious calls by sending a text to 7726 with the word ‘Call’ followed by the caller’s number onto your computer.

Have you been a victim of cyber crime or fraud?

If you have been a victim of cyber crime or fraud, you can tell the police by making a report online at reportfraud.police.uk or by calling 0300 123 2040.

You can report a fraud in your preferred language here.

In Scotland, contact Police Scotland at 101. In an emergency, always call 999.

Notify your bank

If you’ve lost money or you think a criminal has access to your bank account, tell your bank or payment service provider as soon as possible, so they can protect your account and help you get your money back.

Always contact them directly using a number you know is correct, such as the one on your bank card and statements, or call 159.

You can also always reach out to your university for help and support. Universities often offer dedicated teams and networks for issues addressed in this booklet from accommodation and tuition fees, to settling into the country and meeting fellow students and support networks

Information and advice on how to protect yourself against cyber crime and fraud

- Stop! Think Fraud: Learn more on how to stay safe from scams
- Report fraud: A-Z of fraud and cyber crime
- The National Cyber Security Centre

Information and support relating to mental health

- Student Minds
- Victim Support

More useful information

- Interested in a career in Cyber Security? Look here for further information: CRC Cyber Path
- UKCISA - Charity supporting International Students in the UK
- Study UK
- Universities UK - International

More information on updates to Renters' rights with the Rental Reform Bill can be found here:

- The Renters' Rights Act Information Sheet 2026

Online safety checklist

Follow these simple steps to help protect yourself online:

- Secure your accounts, especially your email and bank account
- Set up a passkey wherever possible

- Use strong, separate passwords - you can use 3 random words or have a password manager suggest a password
- Enable 2-step verification
- Keep devices and software up to date
- Back up your important data
- Check your account recovery options

Download the digital version here.

There is a printable version available, you can download it here. Please be aware that this booklet will be updated when new intelligence becomes available.

We are continuously looking to improve this product. Do you have any feedback? Please leave a comment in the box below.

Download / Print article PDF

Share article

Tags

Was this article helpful?

Yes No

B&W

Language

A- A A+

English

Call Us

0300 123 2040

Find us

Reporting

Make a report
Report a phishing attempt

Types of fraud

A-Z of cyber crime & fraud

Useful links

FAQs
Press & media
Sitemap

Sign up to Report Fraud Alert

Subscribe

Privacy Information

Accessibility statement

Terms & conditions