**Fraudulent messages**

University students are often targeted with fraudulent messages from scammers. These can be online, via email or social media or by phone, and are common around the time you start university.

The scams attempt to get money from students or use their identity by persuading them to share their financial information or to unintentionally provide a criminal with access to systems. They are often disguised as communications from recognised UK organisations, such as HM Revenue and Customs (HMRC), Department of Education, the Student Loans Company, the Home Office or UK Visas & Immigration (UKVI).

International students have previously been directly targeted by these scams. In some cases, a scammer will pretend to be from the students’ government/ embassy or police. They use a variety of methods including telling students they or their families are under some form of criminal investigation, for example, a money laundering investigation.

Unfortunately some students have lost large amounts of money. If you receive any messages you’re unsure about, please [contact the IT Service Desk](https://uob.sharepoint.com/sites/itservices/SitePages/contacts.aspx) for advice, or visit [Action Fraud’s website](https://www.ukcisa.org.uk/Information--Advice/Studying--living-in-the-UK/Frauds-and-scams) for more information and advice. If you believe you have been targeted already, it is important that you report this as a crime to the UK Police immediately.

**Checking your emails carefully:**

* [Phishing](http://www.bristol.ac.uk/infosec/protectyou/idtheft/phishing/) means fooling people into divulging personal information, such as bank and card details, account passwords, and so on. Generally, it is done via email, messaging or via fake websites.
* Remember, never respond to emails that ask for your personal or financial details or University password.
* Check links carefully before clicking them.
* Links often hide where they take you. Hover over the link to see the full address before clicking.
* Links and websites can be spoofed, so the link may look like a University login page. Check that the URL matches either a bristol.ac.uk, bris.ac.uk or Microsoft site.
* Don’t open attachments within any unsolicited or unexpected emails you receive.
* Check who emails are from. Outlook does not automatically show the full email address to University members. Please check the email address carefully by opening the sender’s contact card or hovering over the name/email address to view the full address. If it doesn’t match the name, or is inappropriate for the message sent, it is probably malicious. If you’re not sure, please do not reply, but [contact the IT Service Desk](https://uob.sharepoint.com/sites/itservices/SitePages/contacts.aspx)

**Payment of fees**

Please be aware of several scams targeting students either offering discounts or reduced exchange rates to make fee payments on your behalf. This may also include online third-party companies (other than those featured on our official website) offering to process online international payments to send to the University of Bristol.

Do not pass or share your username or password to any agent/third parties. Only students should view their financial statements, no one else.

If in doubt, do not proceed with the transaction.

If you believe you have been targeted, please contact action fraud:[www.actionfraud.org.uk/report\_fraud](http://www.actionfraud.org.uk/report_fraud/)

**Accommodation**

Each year a small number of students are cheated or scammed when trying to rent private accommodation.

If you’re looking for properties on the internet you do need to be vigilant. Don’t send money to anyone advertising rental properties online until you are certain the advertiser is genuine.

Please read [our factsheet](http://www.bristol.ac.uk/accommodation/media/docs/factsheets/renting-safely.pdf) on avoiding scams and renting safely before you start looking for accommodation.

**Support if you have been a victim of a scam**

We are very concerned that our students may be targeting and are offering support to anyone who's been affected. If you have been affected and need help from our support teams, you are welcome to contact us to request support via our [online request form](http://www.bristol.ac.uk/students/support/wellbeing/request-support/).