Murray Edwards College
University of Cambridge

From the Tutorial Office
Murray Edwards College
Cambridge
CB3 0DF

Email: tutorial@murrayedwards.cam.ac.uk
www.murrayedwards.cam.ac.uk

All Undergraduate Freshers

7 September 2022

Dear All

This is relevant to everyone, even if you will not be getting a loan from Student Finance.

Please take care when you get your student loan or other sums of money in your bank accounts. Fraudsters will target bogus emails on students and text messages around loan payment dates each year and Student Finance has already been made aware of some students receiving scam messages this autumn. Please do not be tricked into passing on your personal details or clicking on links in the text or email as these may then install malware on your machine.

The Student Finance Customer Compliance Team has compiled the following list of tips to help you avoid falling victim to phishing emails.

1. Check the quality of the communication. Misspelling, poor punctuation and bad grammar are often tell-tale signs of phishing.

2. Keep an eye out for any emails, phone calls or text messages you think are suspicious, especially around the time you're expecting a payment.

3. Scam emails and text messages are often sent in bulk to many people at the same time. They're unlikely to contain both your first and last name. These commonly start 'Dear Student' so be on guard if you see one like this.

4. 'Failure to respond in 24 hours will result in your account being closed' - these types of messages are designed to create a sense of urgency to prompt a quick response.

5. Think before you click. If you receive an email or text that contains a link you're not sure of, hover over it to check it goes where it's supposed to. If you're still in any doubt, do not risk it. Always go direct to the source rather than following a potentially dangerous link.
   Also, you can send any email you are not sure about to phishing@murrayedwards.cam.ac.uk and our IT team will check it for you.

6. Scammers can use a variety of methods to try get students to pay money or share their personal details. These include fraudulent phone calls, social posts and direct messaging on digital platforms. If you're suspicious, always use official phone numbers, your online account and other official communication channels to verify the contact you received is genuine.

7. Be mindful of the information you share about yourself on social media and elsewhere online. This will help to guard against identity theft. Identity theft happens when fraudsters get enough

information about a person to impersonate them online and over the phone. This can include their name, date of birth, customer reference number, course information and current or previous addresses.

8. Check out **our guide to identifying a phishing scam** for more information.

For those of you who will have a student loan, please be aware that if the bank details the Student Finance holds for you are changed, they will send you a text message from Student Finance England or Student Finance Wales to confirm the change. If you get one of these messages but you have not changed your details, please sign into your online account to review your information and then, if necessary, contact them using an official telephone number.

With best wishes

Tutorial