Delivering payments and keeping students safe online

News story

The second in a series of blogs as the Student Loans Company continues to make Maintenance Loan payments to students. A blog by Derek Ross Executive Director, Operations

Since the start of the pandemic we at SLC have been working hard to support new and returning students with their student finance applications. This week, large numbers of students have registered on their courses and learning is underway. This will be a great relief to many, and I am delighted that we have supported a further 143,000 students with maintenance loan payments of approximately £323 million this week.

We continue to do everything we can to ensure that as many students as possible receive their maintenance loan at the start of term. To help us to process any outstanding applications as quickly as possible we ask that:

- Any evidence we may have requested from you to support an application is submitted immediately via the online account.
- We are immediately notified of any changes to the course being studied, or the university or college being attended via the online account.
- Students access their online account to check their payment status or visit our Frequently Asked Questions. Our contact centres are extremely busy at present, especially on a Monday, so try a quieter time if you can’t find the information you are looking for online.

Some students, who applied after the finance deadline, may not immediately receive their full entitlement. In these cases, a basic funding package is made available to those that are eligible with a top-up payment made as soon as their full application is processed.

As students return to study, we are also urging them to watch out for phishing e-mails and text messages. Just as students and their learning institutions know that payments are arriving into students’ bank accounts, so

too do the online scammers who want to intercept and steal those payments. The easiest way for a student to become a victim is by falling for a phishing email or text that allows scammers to access their personal, financial and account information in order to steal or reroute a payment.

There are a few important tips that students can follow to help them identify a phishing scam:

- Phishing emails are often sent in bulk and are unlikely to contain both your first and last name; they commonly start, ‘Dear Student’ so be on guard if you see one like this.
- Check the quality of the communication – misspelling, poor punctuation and bad grammar are often tell-tale signs of phishing.
- Look out for messages that are designed to convey a sense of urgency to prompt a quick response, such as ‘Failure to respond in 24 hours will result in your account being closed’
- Think before you click. If you receive an email or SMS that contains a link that you’re not sure of then try hovering over to check that it goes where it’s supposed to. If you’re still in any doubt don’t risk it, always go direct to the source rather than clicking on a potentially dangerous link.

We also urge students to be suspicious of any requests for personal information. SLC, Student Finance England (SFE) or Student Finance Wales (SFW) will never ask students to confirm login information or personal information by email or text message.

For more information on how to spot a phishing scam, students can visit:https://www.gov.uk/guidance/phishing-scams-how-you-can-avoid-them.

phishing video

And please, if you receive a suspicious Student Finance e-mail or SMS, don’t click on the link and send it to phishing@slc.co.uk.

Published 15 September 2020