Fraud Facts for Freshers

Press release

The Student Loans Company (SLC) is encouraging students to be on their guard for phishing scams as payments start

The Student Loans Company (SLC) is encouraging students to be on their guard for phishing scams as the company is preparing to pay Maintenance Loan funding to around 1.1 million students throughout September. As payments make their way to students, the company is warning Freshers and returning students to not be tricked into disclosing personal details or clicking on links in emails or text messages, as they could be installing malware.

Fraudsters can target students with bogus emails and SMS around the three loan payment dates in September, January and April each year. In the last two academic years alone, SLC's dedicated Customer Compliance teams have prevented over half a million pounds from being phished from students' loans. The expert teams have a range of methods and fraud analytics to stop scammers in their tracks, but students need to know that they are the best and first line of defence.

Spotting a phishing email or SMS isn't always easy, but the Student Loans Company has six fraud facts to help:

Be suspicious of any requests for your personal information. SLC or Student Finance England (SFE) will never ask you to confirm your login information or personal information by email or text message.

- 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.

- ‘Failure to respond in 24 hours will result in your account being closed’ – these types of messages are designed to convey a sense of urgency to prompt a quick response.

- 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.

- Check out our guide to identifying a phishing scam

Phishing video on YouTube

Steven Darling, Director for Repayment and Customer Compliance at the Student Loans Company, said:

“We work hard to help our customers stay safe, but fraudsters are persistent and will try to target them and their parents with emails and texts requesting personal details to access their accounts.

“We’re reminding all students to be vigilant for online scams and phishing attempts as the new academic year gets underway this September. Although things may be a bit different for some freshers this year, we want them to know that scammers are still working full time to steal their funding.

“Students can keep their account safe by following our simple tips and anyone who receives a suspicious email or SMS should send it to phishing@slc.co.uk. SLC can investigate the site and ensure it is shut down, to help protect other students.”

Published 8 September 2020