Freshers: avoid the phisher's net!

The Student Loans Company (SLC) is warning Freshers and all students to be on their guard as the new term starts, and not be tricked into disclosing any financial details or clicking on links in emails or text messages, as they could be installing malware.

Fraudsters often target students with bogus emails and SMS around the three loan instalment periods in September, January and April each year. In the last two academic years alone SLC's dedicated counter fraud teams have prevented almost 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 themselves are the best and first line of defence.

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

- Be suspicious of any requests for personal or financial information. SLC or Student Finance England (SFE) will never ask you to confirm your bank details or login 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 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.

Steven Darling, Director for Repayment and Counter Fraud Strategy at the Student Loans Company, said: "We're reminding all students that we'll never request their personal or banking details by email or text message.

"Online fraudsters are well aware that students are receiving their first instalment of the year soon. They will try to target them and their parents

or partners with emails and texts requesting personal and banking details to access their accounts.

Anyone who receives a suspicious email should send it to phishing@slc.co.uk. SLC can investigate the site and ensure it is shut down, to help protect other students.”

Find out more about online safety by watching our phishing video