Fraud warning from SLC as new academic year approaches

SLC will pay more than £2billion to 2 million students over the coming weeks and is reminding people to be vigilant. 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.

In the last three years alone, SLC's dedicated Customer Compliance teams has stopped £1.2million being lost to fraudsters from students' bank accounts. 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 some fraud facts to help:

- Check the quality of the communication – misspelling, poor punctuation and bad grammar are often tell-tale signs of phishing.
- Keep an eye out for any emails, phone calls or SMS messages you think are suspicious, especially around the time you're expecting a payment.
- Scam emails and text messages are often sent in bulk to many people at the same time and are unlikely to contain both your first and last name. These commonly start – 'Dear Student' – so be on guard if you see one like this.
- '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 hover over it 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.
- Scammers can use a variety of methods to try get students to pay money or share their personal details, including the use of fraudulent phone calls, social posts and direct messaging on digital platforms. If you are suspicious of being contacted, always use official phone numbers, your online account and official communication channels to verify the contact you received is genuine.
- Students should also be mindful of the information that they share about themselves on social media, and elsewhere online, to help guard against identity theft. Identity theft happens when fraudsters access enough information about a person's identity, such as their name, date of birth, customer reference number, course information or their current or previous addresses to impersonate them online and over the phone.
- Check out our guide to identifying a phishing scam at www.gov.uk/guidance/phishing-scams-how-you-can-avoid-them

Bernice McNaught, Executive Director, Repayments and Customer Compliance at the Student Loans Company, said:

“It’s no surprise that at this time of year students, especially Freshers, have a lot on their minds – getting to grips with classes and campuses, making new friends or exploring new surroundings.

“With so many things taking attention, it’s easy for students to drop their guard when it comes to mindfulness over online scams and fraudulent phishing. Unfortunately, digital scams, phishing and identity theft have become an everyday part of modern life, and scammers are all too aware that the three student finance payment periods in September, January and April each year are a prime time for them to try to trick students.

“Keeping money in students’ pockets is a high priority for SLC. Our Counter Fraud teams work to keep on top of the constantly evolving digital scams, to support students who may be in danger of losing their funds to fraudsters. The first line of defence against fraudsters is always students themselves. They can keep their account safe by following our simple tips.”

Customers in England should be aware that whenever their bank details are changed, they will receive an SMS from Student Finance England (SFE) to confirm the change. If a customer hasn’t changed their details but receives a message, they should log into their online account to review their information and also get in contact using an official telephone number as they could be the victim of identity theft and future payments may be blocked if they don’t.

There is also a range of additional advice and information on recognising and avoiding scams from Take Five, a national campaign aimed at stopping fraud: Take Five – To Stop Fraud