Student Loans Company’s phishing guide, top tips and details on what to do if you receive a suspicious email can be found at: bit.ly/e3E2xT

TOP TIPS
Student Loans Company's Top Five Tips to Avoid Phishing:

1. Be suspicious of any urgent requests for personal or financial information.
2. Be aware: Phishing scams are common at the three main instalment payment dates in September, January and April.
3. Always ensure that you're using a secure web site when submitting credit card or other sensitive information.
4. Prevention: Your email details may have been taken from a social networking site so avoid disclosing your email address or make sure you hide it on your page.
5. Check the quality of the communication. Misspelling, poor punctuation and bad grammar are often tell-tale signs of phishing.

WHAT WE WON'T ASK YOU

The Student Loans Company will NEVER:

- ask you to update your bank details
- ask you to verify your account details
- ask you to click a link, always type the address yourself: www.direct.gov.uk/studentfinance
- ask you to answer combinations on the same screen i.e Your Customer Reference Number and Password on the same screen
- provide you with a choice of secret questions. We will only ever ask you the question you gave us.
- ask you to update items such as date of birth or provide your email address password.