

What is phishing?

Phishing is fraud. Phishing websites are set up to encourage you to type in your login details. Criminals can then use these details to log in to your account, view your personal information, and, in some cases, change your bank details so that they can steal your loans.

Stay safe

We will **never** email you asking you to confirm your bank account details. If you receive an email that appears to be from us and asks you to visit our site and confirm your bank details or your full account details, then it is probably a 'phishing' email. We will **only** email you about your login details if you've asked to reset these.

Don't get caught out:

- Check the quality of the communication. Misspelling, poor punctuation and bad grammar are often tell-tale signs of phishing
- We will **never** ask you to verify your full secret answer; we will only ask you for characters from your secret answer.

A phishing email - example

From: student_finance@gov.uk

To: a_student@hotmail.com

Date: 01/04/2013 15:38

Subject: Please check your online account details

This message for all students applying for grants and loans this year. The Students Loans Company need you to verify your account details to make sure your account is secure.

www.gov.uk/confirm

Yours sincerely Student Finance

Please do not reply to this email as it has been automatically produced from an address which cannot accept incoming mail.

Phishing websites - example

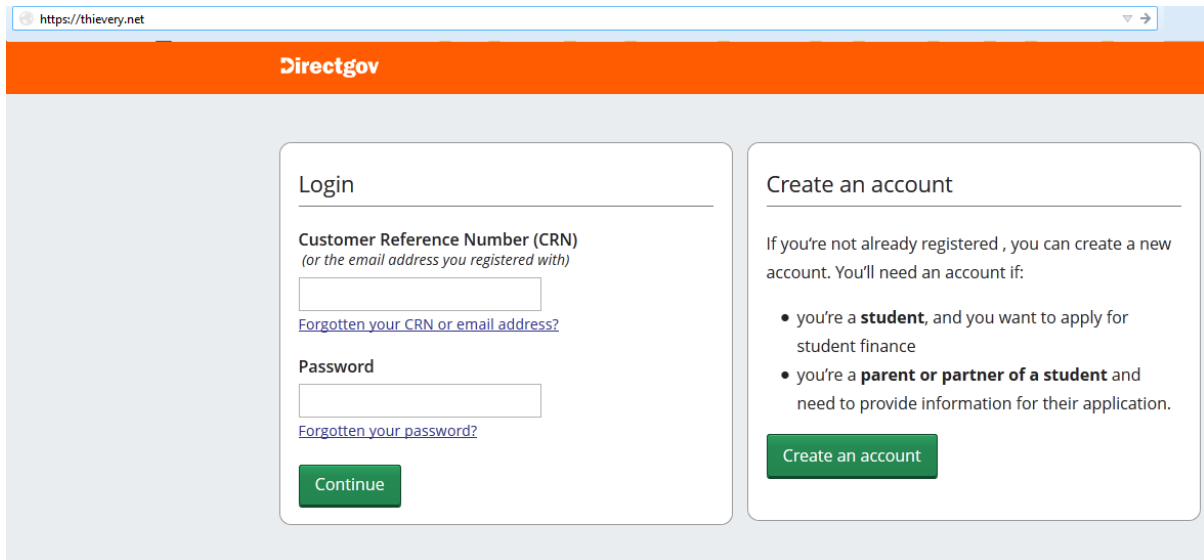
A phishing email will send you to a fake version of a student finance website.

Always check the web address – this can often be a giveaway that all is not as it seems.

In the example above the link www.gov.uk/confirm is shown in your email.

However, when you click the link this may actually send you to a fake website which looks like a student finance login screen but has a different URL.

In the example below the real URL, shown in the browser, is **<https://thievery.net>** –



The screenshot shows a web browser window with the address bar displaying <https://thievery.net>. The website has an orange header with the 'Directgov' logo. The main content area is divided into two columns. The left column is titled 'Login' and contains a form with the following elements: a label 'Customer Reference Number (CRN)' with the subtext '(or the email address you registered with)', an empty text input field, a blue link 'Forgotten your CRN or email address?', a label 'Password', another empty text input field, a blue link 'Forgotten your password?', and a green 'Continue' button. The right column is titled 'Create an account' and contains the text 'If you're not already registered, you can create a new account. You'll need an account if:', followed by a bulleted list: '• you're a **student**, and you want to apply for student finance' and '• you're a **parent or partner of a student** and need to provide information for their application.' Below the list is a green 'Create an account' button.