Phishing emails

How to spot them and what to do with them

Phishing is a scam that uses an email pretending to be from the University or another organisation. The scams try to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

Phishing at LSBU

Like all institutions, LSBU is subject to thousands of email phishing attacks every day.

In 99.9% of cases we’re able identify these emails and prevent them from landing in your mailbox. However, on some occasions these emails will slip through our spam filters and reach your mailbox. To protect your account and to prevent any phishing attack spreading across the University please remember the following:

We never, ever ask for your password, card details, etc. either verbally or in an email

Honestly that first one is really important

If something is too good to be true it probably is - the Chief Finance Officer will never send you an email offering a £1000 grant or bursary – any details of grants, loans or financial settlements are confirmed with students directly, usually followed by a phone call and/or a letter

Phishing emails will often appear to come from a fellow student or an academic you know, so if the content, signature or email address seems unusual do not click on any links and inform ICT

In fact, if anything seems a bit unusual or ‘off’ do not click on links
How to spot a phishing email

How to spot signs of phishing

- Look out for these giveaway signs that can help you spot a potentially fraudulent email.

- Poor or unusual spelling and grammar - if the email is riddled with errors, it’s probably a scam

- Email doesn’t address you by your name, or doesn’t follow a usual convention of ‘Dear Student’ but instead uses phrases like ‘To our valued customer’ or ‘Dear account user’

- The message carries a disproportionate warning eg. ‘update immediately’ or ‘urgent action required’ but there is no email address or phone number for further information

- The message warns of big change, update or good news (eg. prize won, grant awarded) but there is no email address or phone number for further information

- Email asks you to provide your password, financial information, national insurance number or passport numbers

- Email comes from an unexpected email address (e.g. @hotmail.com, @gmail.com, @live.com) instead of one associated with the organisation that is claiming to be contacting you (e.g. @hsbc.co.uk or @lsbu.ac.uk

- When a fraudulent email asks you to follow a link or respond, the website or email address usually doesn’t look right. Authentic website addresses are usually short and don’t use irrelevant words or phrases

What to do if you click on a link in a phishing email

If you have clicked on a link in a phishing email make sure you reset your password straight away - You can change your password by logging into an LSBU computer, pressing CTRL+ALT+DELETE and choose change password. Contact the Student IT Support help desk on 0207 815 6678 or llr-ithelpdesk@lsbu.ac.uk, so that we can prevent the messaging spreading to others in your name.
How to report a phishing email

Spam can be forwarded to ICT by emailing ictemail@lsbu.ac.uk.

If you have any issues or require assistance, please contact the Student IT Support help desk on 0207 815 6678 or llr-ithelpdesk@lsbu.ac.uk.

For further information and support contact:
Tel: 020 7815 6678
Email: llr-ithelpdesk@lsbu.ac.uk
Visit: Student IT Support, 1 West, Perry Library.