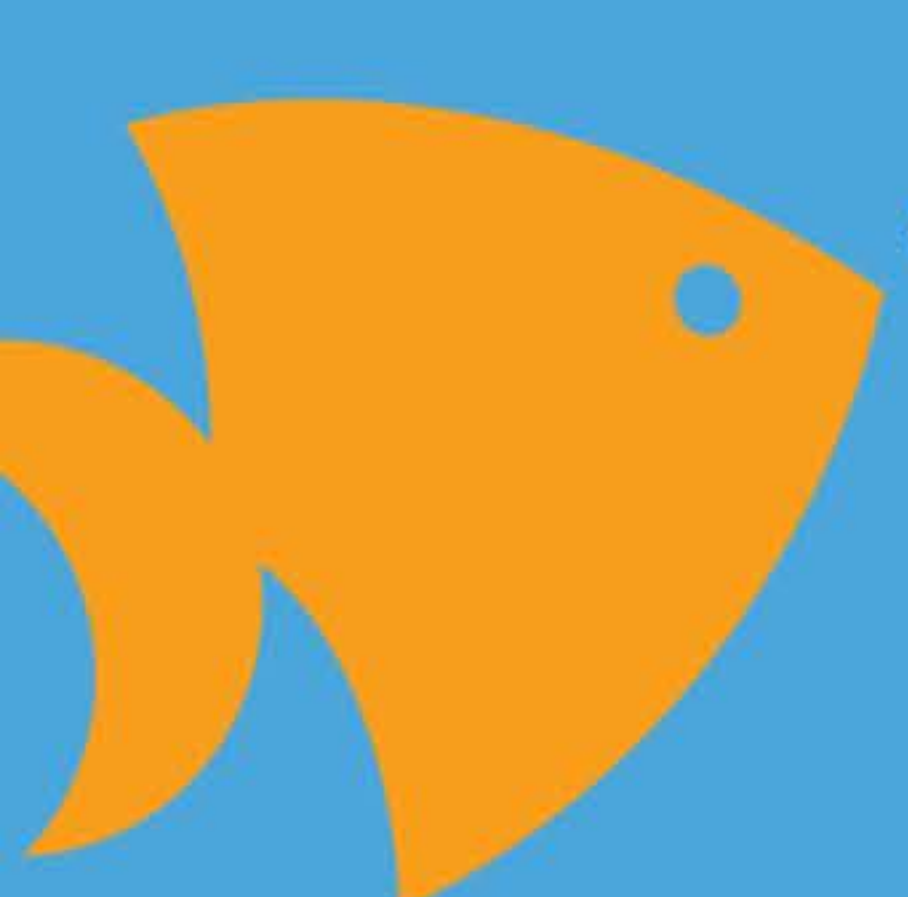



# Don't get hooked!

## How to spot a phishing email

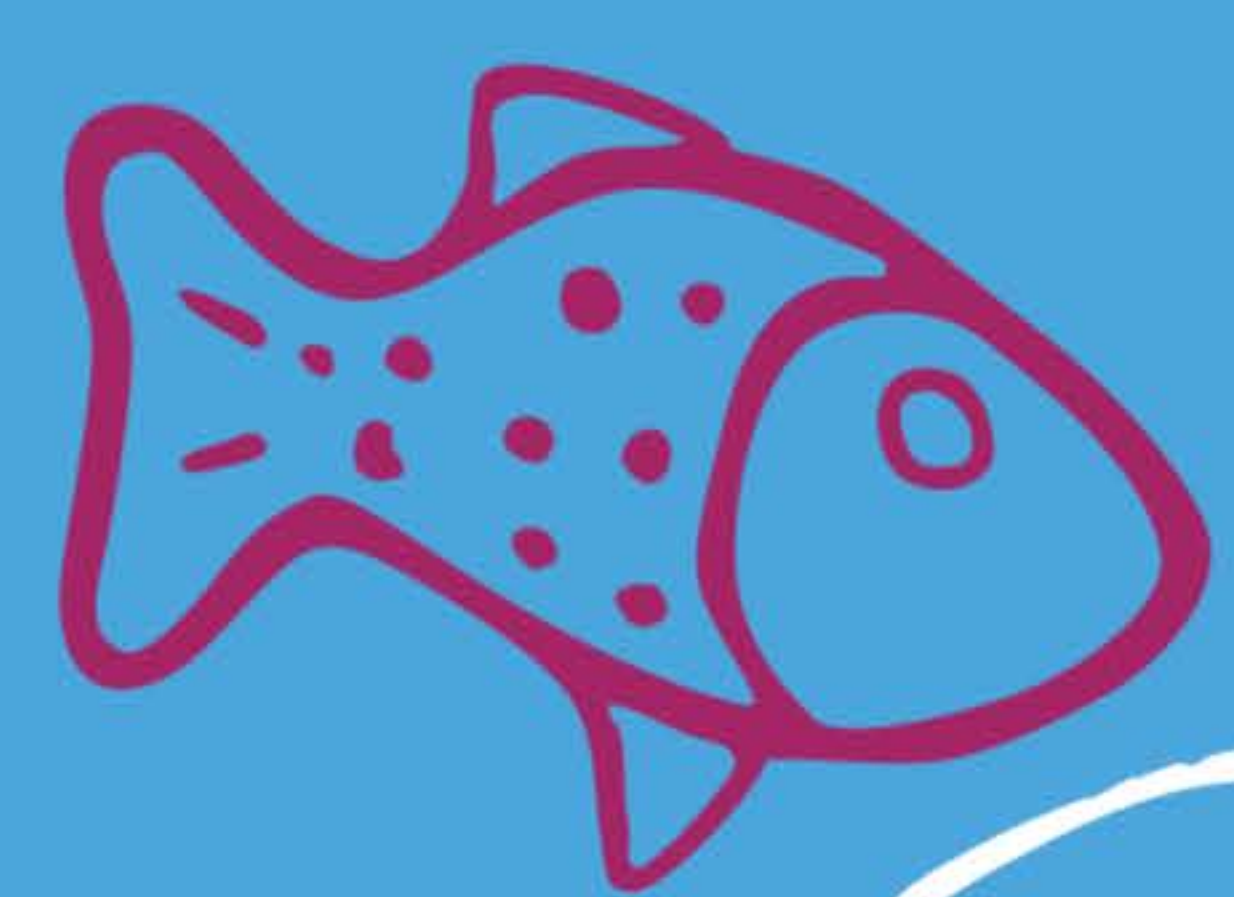
Phishing is the use of fake email messages that claim to be from an institution or company you trust. Their aim? To gather your username and password in order to compromise your account.



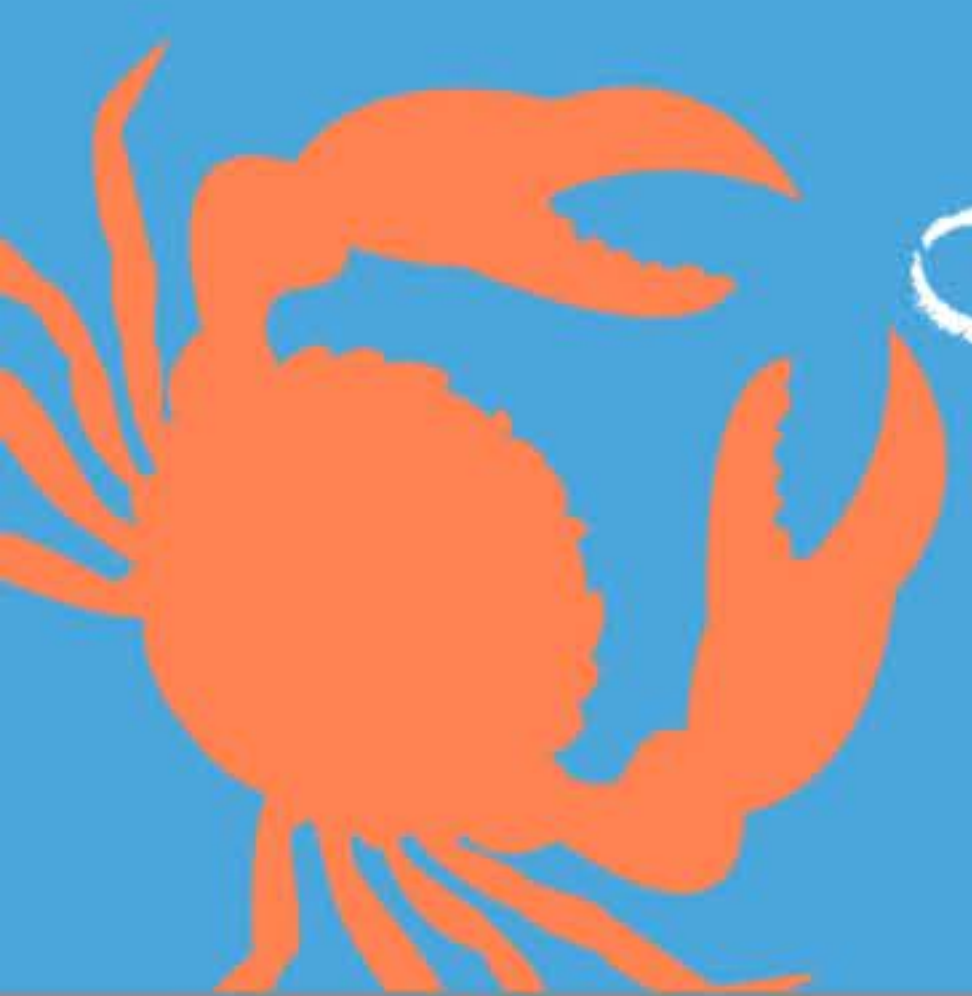
Be wary of emails that ask you to validate or verify your account.



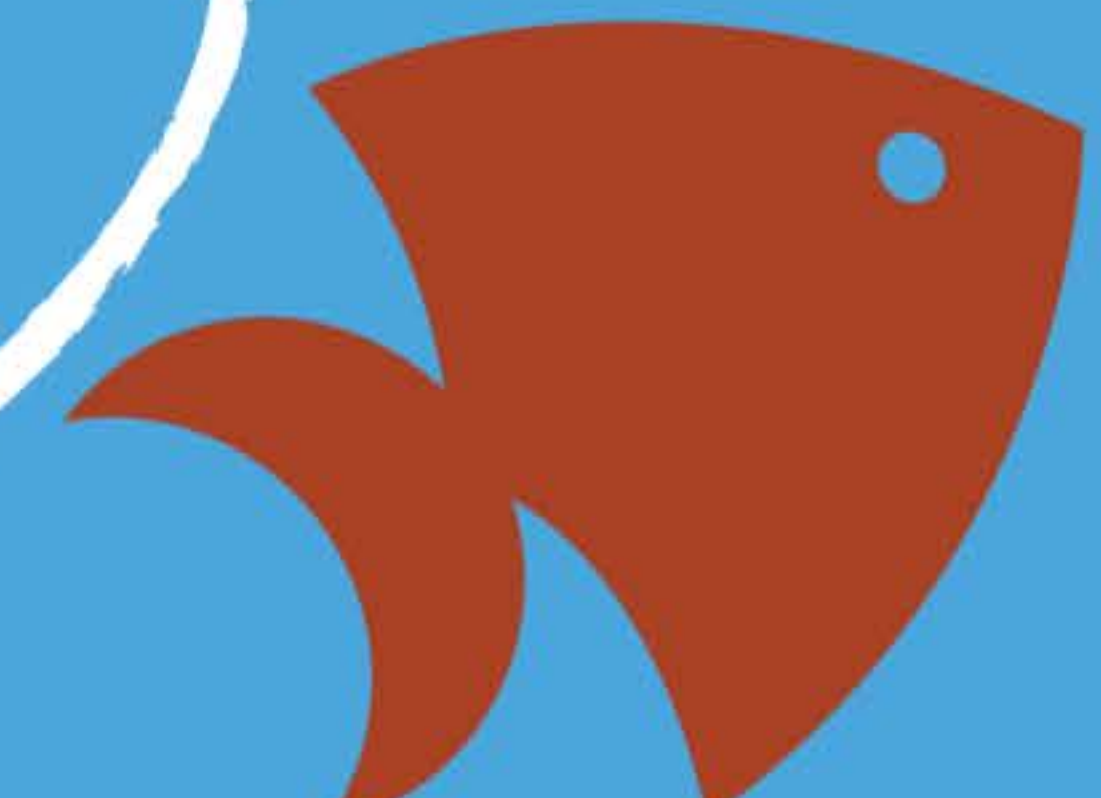
Phishing emails tend to be poorly written and may include spelling mistakes and odd formatting.




Look out for emails which have a sense of urgency and imply you might lose access to your account.



Be wary of links in emails. Is the destination the same as the link you see? Try hovering over the link to check.



They may appear to be from someone you know or an official source at the University.



Please remember:

IT Services staff will never ask you to reveal your password by email, in person, or on the phone. For more information on spam and phishing emails, see:  
[www.york.ac.uk/it-services/it/security/spam](http://www.york.ac.uk/it-services/it/security/spam)