Common Phishing Prevention Tips

Some things to look out for when receiving a suspicious email:

1) Pay attention to the email address that sent the email in terms of relevance to the subject. For example, why would you be getting an email about your Microsoft office account from an address that does not say Microsoft Office or Microsoft?
2) The body of the message is an image. This may just be a screenshot off of a legitimate email, but the party or person wanting to steal your information input a hyperlink into the image to take you to a website in hopes that you supply your credentials.

Here a link to an email that was copy and pasted (and all links removed so you are safe to explore). The first warning flag is highlighted in yellow. Notice that the email address says ocduk.org and is not a Microsoft related email? Also, the body of the message is an image. If you click and drag (as if you were selecting text to highlight), notice that either nothing is highlighted, or the whole email body becomes highlighted. You will need to download the document from the PDF we have uploaded into Google Drive.