Example Phishing Emails - and how to spot the signs

The emails below are live examples of phishing emails received by the University recently. Please note the signs to assist in distinguishing them as a phishing attempt.

Example 1

From: Rae Blair [mailto:Rae.Blair@utsa.edu]

While addresses can be 'spoofed' and caution should still be applied, this example is clearly not from a University of Ulster email address.

Sent: 10 October 2011 01:52
To: undisclosed-recipients
Subject: IT Services (Warning Code: ID67565434)????

No such legitimate error code exists. Tip: you could check this via a web search – this example is listed as a phish by several security websites.

IT Service,

The email is addressed generically to 'undisclosed-recipients' and has no personal greeting – why would someone greet you as 'IT Service'? This should raise suspicion when combined with other factors.

You have exceeded the limit of 23432 storage on your mailbox set by your WEBCTSERVICE/Administrator, and you will be having problems in sending and recieving mails Until You Re-Validate. To prevent this, please click on the link below to reset your account.
CLICKHERE:
Failure to do this, will result in limited access to your mailbox Warning !!! Do not send your username and password via email.

Note the poor spelling, capitalization and grammar in the paragraph. Also note that if you hovered your mouse over the 'Click Here' link (without clicking on it!) – the preview of the link in this example showed it not to be an 'ulster.ac.uk' address – so it was obviously 'spoofed'.

Regards,
IT Service
System Administrator

The central IT Department within the University of Ulster is called "Information Services" and we **NEVER** request personal or account details via an email or online link as seen in this phish. Also, there is no such legitimate process as "re-validating" a mailbox.

Example 2

From: Student Finance Company [mailto:sfd_webmaster@slc.co.uk]

This address may *look* legitimate at first glance, but why is it Student Finance Company, instead of Student Loans Company? Some spammers pay more attention to 'fine detail' than others, but this should raise suspicion in this case. Why also would a 'webmaster' email address be used?

Sent: 04 January 2011 13:52
To: Service Desk
Subject: Student Loan Payment Processing Update

Dear Student,
Your student loan account need to be upgraded to match the details we hold on record for you.
Failure to upgrade means that your next student loan payment and maintenance grant will be delayed.
Thanks for your co-operation.

SIGN ON HERE

Why is this email generically addressed 'Dear Student' instead of your own name? Note also the poor grammar. Threatening consequences as a result of not doing as requested is also a common phishing tactic, trying to panic you into action.

The "Sign On Here" hyperlink – by hovering your mouse over any hyperlink, you can see the web address previewed. In this example it was clearly not the legitimate Student Loans Company website but in any case you should NEVER follow ANY link in an unsolicited email. ALWAYS go direct to the legitimate site via your web browser by typing the address or using a stored favourite.

Yours sincerely,
Student Loan Finance England.