2013 ANTI-PHISHING CAMPAIGN

TECHNOLOGY & INFORMATION SERVICES WITH PLYMOUTH UNIVERSITY

What is Phishing?

Phishing is the name given to the practice of sending emails purporting to come from a genuine company or organisations operating on the Internet. These scam emails attempt to deceive the recipients into entering confidential information such as credit card or bank details, passwords and account data. The links contained within the message are false, and often redirect the user to a fake website. Many fake emails can look very convincing, complete with company logos and links that seem to take you through to the company website, although this too will be a fake.

The Guardian recently reported that the UK was the most phished country in 2012 with business and consumers losing in excess of £600m. The HE sector hasn't escaped such attacks and most university employees and students will have at some point received a fake email claiming to be from the IT support desk or an account manager asking for a username, password or perhaps some other personal information. Often, such emails claim that an individual's email storage quota has been reached or that their account will suspended if there is no response to the email.

What happens if I respond to a phishing email?

If you unsuspectingly divulge your University account username and password to a third party, you could be putting yourself and the University at risk.

EFFECTS ON YOU	EFFECTS ON THE UNIVERSITY
Your email address may be hacked, resulting in email being sent from your address.	Genuine Plymouth University email may be delayed due to a step up in security.
Once access has been gained to your email address, the hackers could access the HR systems to steal your bank details, home address, national insurance number and employment details – all of the ingredients needed to commit financial fraud and identity theft.	The University's public image could be damaged if vital information is hacked.
	Other students and staff are at risk from hacking.

How can I tell if an email is genuine or fake?

There are often common clues that may help you identify a phishing email. For example, you may find that the email:

- has come from an unexpected email address (eg @hotmail.com, @gmail.com or @yahoo.com) instead of one associated with the organisation that is claiming to be contacting you (eg @santander.co.uk, @plymouth.ac.uk)
- may contain poor spelling and grammar, and/or a lot of capital letters
- warns of a big change but has no email address or phone number for further information.

What should I do if I think I have mistakenly responded to a phishing email?

If you think you have responded to a phishing email, you are advised to:

- change your University account password immediately. You can do this through the staff portal **https://staff.plymouth.ac.uk**
- then telephone the TIS Service Desk on 01752 588588. You may be asked to forward a screen shot of the suspect email to **support@plymouth.ac.uk**; you must never forward the original email to anyone.

How can I stay safe?

Use the following tips to protect yourself and the University.

- Never disclose personal information in response to an email. University staff will never ask you to reveal your login details via an email.
- Treat your University IT account details as highly confidential and a way of accessing sensitive information – never disclose your login ID or password to anyone outside the University.
- Avoid using your University account password on other internet services outside the University.
- Look carefully at who the email is from. If it is not clearly from Plymouth University (eg it shows an external email address) then it hasn't come from the University. However, even if it has been sent from a Plymouth University email address, you must not respond to any request for your password or confidential details as the account may have been compromised.
- Even if you suspect an email message may be genuine, do not click the links within the mail message. Open a new page from your internet browser and visit the relevant web page directly.
- If in doubt, seek advice – forward a screen shot of the suspect email to the TIS Service Desk, support@plymouth.ac.uk.
- Remember, the only person who needs to know your password is you. Any email that asks for your password is a hoax.

What are TIS doing to help protect account?

Technology and Information Services runs blocking filters and software designed to prevent this type of email from getting to users. However, it is inevitable that a small percentage of this constantly evolving phishing threat will make it through before being identified and blocked.