SECURITY WITH PLYMOUTH UNIVERSITY

Technology & Information Services

SEC-GDL-005 - Anatomy of a Phishing Email

Author:	Paul Ferrier
Date:	01/03/2017

Document Security Level:	**PUBLIC**
Document Version:	1.00
Document Ref:	SEC-GDL-005
Document Link:	blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2014/06/SEC-GDL-005-Anatomy-of-a-phishing-email.pdf
Review Date:	03/2018

SEC-GDL-005 - Anatomy of a Phishing Email

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	Paul Ferrier	Enterprise Security Architect	Created the document	23/08/2014	n/a	n/a	n/a
0.91	Michael Paraseava	TIS Communications Officer	Communications advice	04/09/2014	n/a	n/a	n/a
0.93	PF, Nick Sharratt, Emma Wainman	ESA, BP and DPO	Final comments before wider distribution	08/10/2014	n/a	n/a	n/a
0.94	PF	ESA	Updated document with new template	07/11/2014	tbc	tbc	tbc
0.95	PF	ESA	Following recent phishing campaign	02/12/2014			
0.96	PF	ESA	Following comments from Service Management	04/12/2014 16:15			
0.97	PF	ESA	Final comments from Service Management	09/12/2014 15:30			
0.98	PF	ESA	Reclassified document and added link to Phishing Line on the Blog Site	29/01/2015 08:30			
1.00	PF	ESA	Reviewed and updated document	01/03/2018 09:00			

SEC-GDL-005 - Anatomy of a Phishing Email

Introduction

Your University computer account enables you to access a wealth of software and electronic resources. These resources must be protected from unauthorised use, otherwise the University may lose the ability to access them. Additionally, your account provides access to sensitive personal information held within the Student Records or Human Resource systems. Your account is also necessary in order to carry out your daily work. **Never disclose your password.**

1. Definitions

Phishing	is email fraud method in which the perpetrator sends out legitimate-looking email in an attempt to gather personal and/or financial information from recipients.
Spam	Irrelevant or unsolicited messages sent over the internet, typically to large amount of users, for the purpose of advertising, phishing or spreading malware etc.
Spear Phishing	is aimed specifically at users with an important status at an organisation. They are targeted emails that have combined publically available information from social media sites (LinkedIn, Facebook etc.) to provide a more personal phishing email. The result is still the same; the attacker is trying to gain access to a personal account in order to harvest and use data.
Spoofing	is the ability for one person or a programme to masquerade as another by falsifying data.
Whaling	is a term where a specific spear phishing campaign is launched against a user who is likely to have highly privileged access to corporate or sensitive information within an organisation.

2. Purpose of Phishing Emails

2.1 Phishing emails just fill up your inbox, they are often crafted to get end users to either respond with information the perpetrator requires, or to click an embedded link and be taken to another location to provide account details.

2.2 Once account details, usually username and password, are provided this account is at risk of compromise either immediately, to allow additional phishing attacks to take place or to store your details for future use.

2.3 A successful phishing attack has implications both for you and the University network as a whole. It not only compromises your account but is a security risk and can result in University mail servers being blacklisted by other organisations and therefore prevent legitimate communications being sent or received.

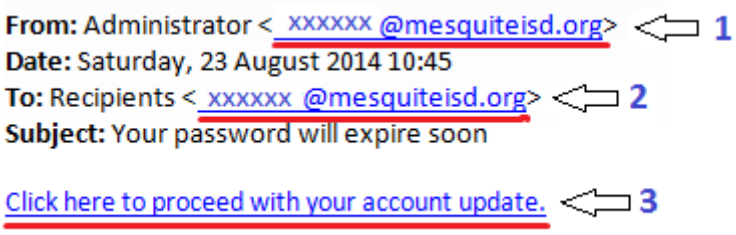
3. How to identify a Phishing Email

3.1 Most phishing attacks contain consistent themes, but they are often subtly different. There are almost always clues that should help differentiate authentic emails from bogus ones.

3.2 A simple checklist is below:

Subject line	Language within the body of the message
Senders email address	Recipient email address
Location of embedded links	Inconsistencies with terminology
Requests for sensitive information (username and password)	Directs you to “login” to a non-official service with your credentials

3.3 The Simple Phish



This is the entire content of the email. Looking closely though you should be able to easily identify it as a phishing email by the highlighted points:

'From address' **(1)** do you know the user, or do you use the domain *mesquiteisd.org*?
The 'recipients' **(2)** have been hidden, but the sender has copied themselves into the email. While this is a legitimate practice often used for distributing emails to large amounts of end users (for example, a Postmaster or News Alert internal email, refer to section 6 for details of such accounts).
There is an embedded link **(3)** provided, hovering over this with a mouse will show the destination of the link. The link itself may redirect you somewhere other than its stated location, this indicates nefarious activity is attempted to be disguised.

The overriding factor here is that there is no information in the email. As such, this would likely be a smash and grab attempt to get a small percentage of a large number of user credentials which the email is sent to.

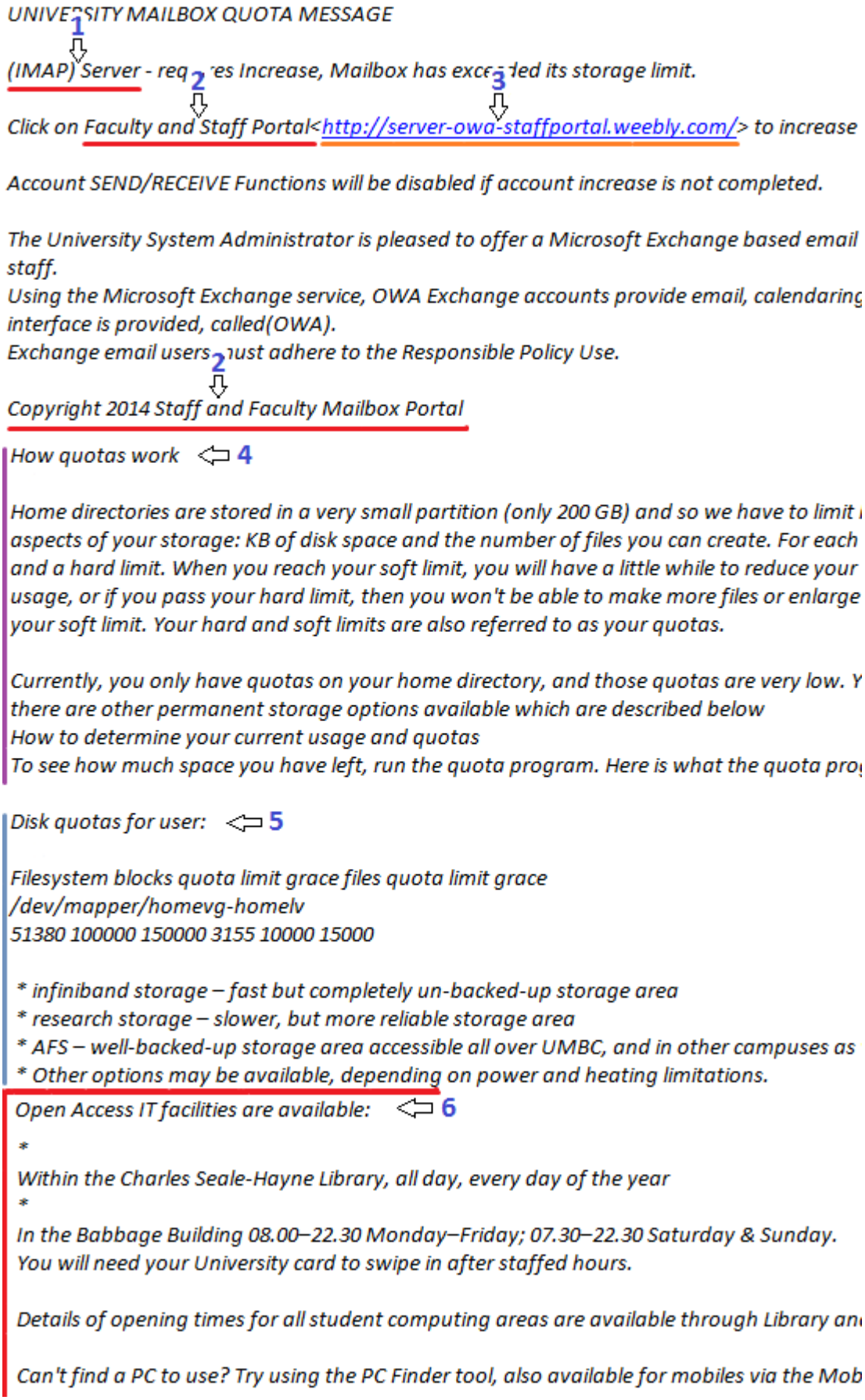
3.4 The Standard Phish

In comparison to 3.3 this email provides slightly more content to examine.

Subject matter **(1)** if your mailbox is full, you may not be able to receive emails.
Incorrect English **(2)**, 'will expires', typos do occur in emails but there is very little punctuation and also a conflict between the subject line 'your mailbox is full' and 'your password will expire'.
Embedded link **(3)**, hovering over this with a mouse will show the destination of the link.
The hyperlink **(4)** would take you to a bravesites.com sub-domain – this is in no way associated with Plymouth University. In addition, the link itself may redirect you somewhere other than its stated location, this indicates nefarious activity is attempted to be disguised.
University emails would not be sent from 'System Administrator' **(5)**.
The email signature **(6)** is not consistent with the University's branding style.

Overall there is no coherent or consistent content throughout the email, and there are enough indicators to identify it as a phishing email.

3.5 **The Full Phish**



UNIVERSITY MAILBOX QUOTA MESSAGE

(IMAP) Server - requires Increase, Mailbox has exceeded its storage limit.

Click on Faculty and Staff Portal<http://server-owa-staffportal.weebly.com/> to increase

Account SEND/RECEIVE Functions will be disabled if account increase is not completed.

The University System Administrator is pleased to offer a Microsoft Exchange based email staff.
Using the Microsoft Exchange service, OWA Exchange accounts provide email, calendaring interface is provided, called(OWA).
Exchange email users must adhere to the Responsible Policy Use.

Copyright 2014 Staff and Faculty Mailbox Portal

How quotas work ⇦ 4

Home directories are stored in a very small partition (only 200 GB) and so we have to limit aspects of your storage: KB of disk space and the number of files you can create. For each and a hard limit. When you reach your soft limit, you will have a little while to reduce your usage, or if you pass your hard limit, then you won't be able to make more files or enlarge your soft limit. Your hard and soft limits are also referred to as your quotas.

Currently, you only have quotas on your home directory, and those quotas are very low. Y there are other permanent storage options available which are described below
How to determine your current usage and quotas
To see how much space you have left, run the quota program. Here is what the quota pro

Disk quotas for user: ⇦ 5

Filesystem blocks quota limit grace files quota limit grace
/dev/mapper/homevg-homelv
51380 100000 150000 3155 10000 15000

** infiniband storage – fast but completely un-backed-up storage area*
** research storage – slower, but more reliable storage area*
** AFS – well-backed-up storage area accessible all over UMBC, and in other campuses as*
** Other options may be available, depending on power and heating limitations.*

Open Access IT facilities are available: ⇦ 6

***
Within the Charles Seale-Hayne Library, all day, every day of the year
***
In the Babbage Building 08.00–22.30 Monday–Friday; 07.30–22.30 Saturday & Sunday.
You will need your University card to swipe in after staffed hours.

Details of opening times for all student computing areas are available through Library an

Can't find a PC to use? Try using the PC Finder tool, also available for mobiles via the Mob

The recipients' details have been removed, so that the example can fit on the page. So there is a lot of information here, in fact there is too much information:

Technical terminology **(1)** or abbreviations without explaining what they mean.

Inconsistent naming of department **(2)** and the service, also copyright notice.
Embedded link **(3)** within the message body that provides the actual URL that clicking will redirect you to. **Still check** the end location by rolling over the link with your mouse, it may be saying one thing and will send you to another location.
Information that may be accurate **(4)**, is added to try and prove the message is more authentic or potentially too long in the hopes that the target user will not read it all and just click the provided link instead.
Figures that back up the additional information **(5)**, there is no need for an end user to be presented with this data. It once more is designed to confuse the recipient of the email into thinking that it is genuine.
Finally, it appears as in this case that some creators of phishing attacks are copying information from the University web pages **(6)** and placing that information into the body of an email.

The important point to consider is does this content fit with the remainder of the body of the email? The example on the previous page suggests not. Why would talking about Open Access facilities be required when the remainder of the email talks about Email mailbox quotas.

3.6 **The Service Phish**

This is the quick and easy route to scare users' into providing details.

Hover over the vaildate link (**1**) will show you the location you will be taken to.
Any new or significantly altered services will be communicated well in advance (**2**), consider the advertising surrounding the new website or the digital learning environment, for example.
The University does not have a (**3**) message center (Americanised spelling).
Legitimate emails are not issued from the University (**4**) **Help Desk**, please refer to section 6.

4. What to do with Phishing Emails

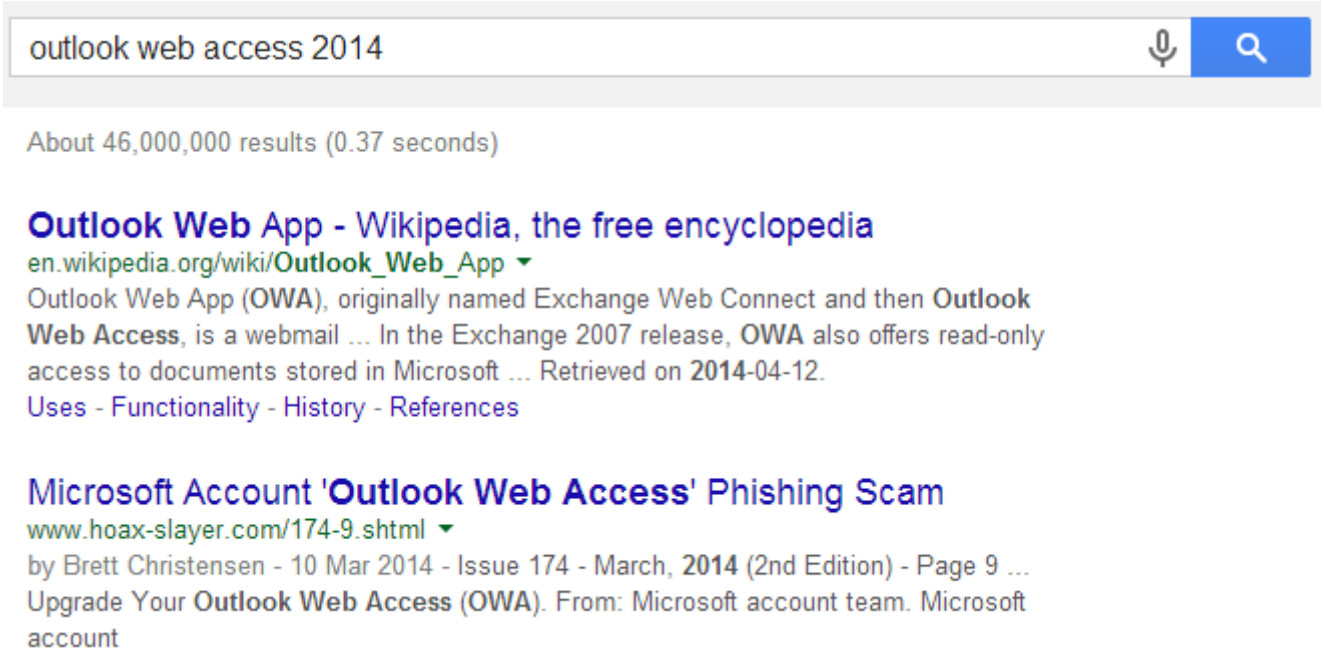
4.1 If you a ***sure*** that the message is a phishing email, just **delete it**. If you are **unsure** about the validity of an email **ask** (see point 4.6).

4.2 It can take up to two full working days (sometimes longer) to resolve problems if a compromised account has been used to start sending further phishing emails.

4.3 **Do not** click on any links. Depending on the code within the target web page, the email address or other tracking information may be passed across and denote that you are susceptible to these type of messages.

4.4 **Do not** reply to the message. It will denote that your email address is live and could be used once more.

4.5 A simple search of the subject line through a web browser may illicit an immediate answer to whether it is a hoax email or not. See the second result in the listing over the page.



4.6 You can also check the Strategy and Architecture Blog Site's Phishing Line (http://blogs.plymouth.ac.uk/strategyandarchitecture/phishing-line) where known about phishing emails received by the Service Desk are published.

4.7 Forward the email to the Service Desk (servicedesk@plymouth.ac.uk) for investigation, or telephone them on 01752 588588 and then delete the email from your Inbox.

5. What to do if you have responded to a Phishing Email

5.1 Change your account password immediately, this will potentially be posted on the Internet in the public domain associated to your email address or username. This password should not be used again for this account.

Additionally, if you have used this combination of username or email address and password on other sites, please change these too …. If someone can see where you have been shopping online – they may try to use the compromised credentials on that site as well.

5.2 Contact the Service Desk (servicedesk@plymouth.ac.uk) (as point 4.6) for investigation.

5.3 Depending on the progress of any subsequent actions undertaken with your account, TIS may be required to provide you with a new email address from which to send emails. You will retain your old email address for receiving legitimate content.

6. Valid Central Communication Addresses

6.1 Please find below a list of valid central email addresses that the University use to email staff and or students:

Service Desk	servicedesk@plymouth.ac.uk
Postmaster	postmaster@plymouth.ac.uk
News Alert	news-alert@plymouth.ac.uk