Information Services - Advice on 'Phishing' Emails

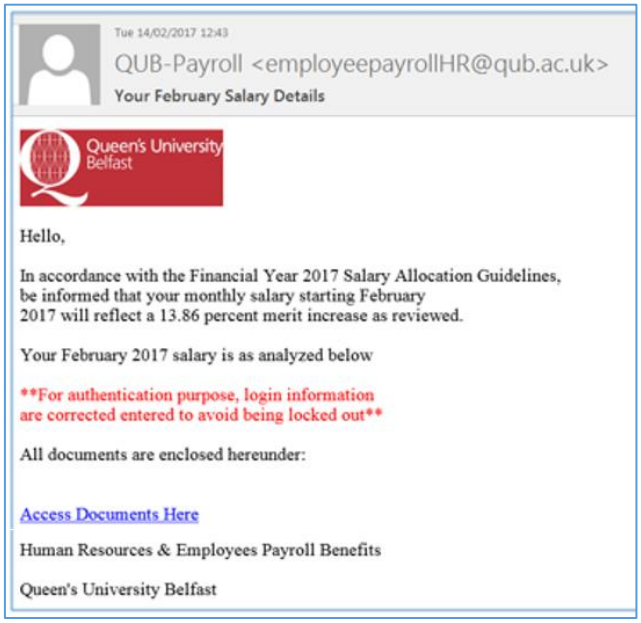
What is Phishing?

Phishing is an attempt by criminals to steal your information. Phishing emails try to trick you into disclosing sensitive personal or financial information such as your University login name and password, your credit card details or your bank account details.

Please read this advice as it could help prevent you becoming a victim of a phishing attack.

How Phishing Works

1. The criminals send you an email hoping to fool you into responding, typically by directing you to a website where you are asked to provide confidential, personal or financial information. The email appears to come from an organisation known to you (e.g. Fedex, Apple) or even from an internal QUB source such as the IT Helpdesk. The criminals may adopt a 'scatter-gun' approach, sending the email to a large group of recipients, but increasingly we are seeing more targeted attacks. Here are some real life examples of such emails, including one specifically targeted at Queen's:



Tue 14/02/2017 12:43

QUB-Payroll <employeepayrollHR@qub.ac.uk>

Your February Salary Details

Queen's University Belfast

Hello,

In accordance with the Financial Year 2017 Salary Allocation Guidelines, be informed that your monthly salary starting February 2017 will reflect a 13.86 percent merit increase as reviewed.

Your February 2017 salary is as analyzed below

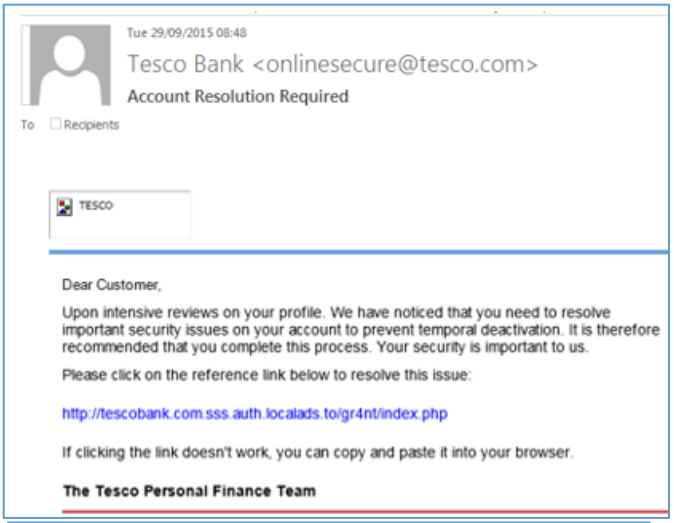
For authentication purpose, login information are corrected entered to avoid being locked out

All documents are enclosed hereunder:

Access Documents Here

Human Resources & Employees Payroll Benefits

Queen's University Belfast



Tue 29/09/2015 08:48

Tesco Bank <onlinesecure@tesco.com>

Account Resolution Required

To Recipients

TESCO

Dear Customer,

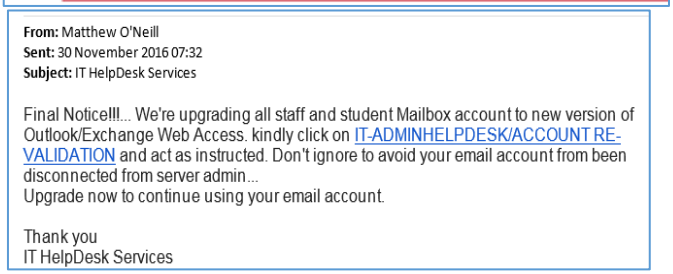
Upon intensive reviews on your profile. We have noticed that you need to resolve important security issues on your account to prevent temporal deactivation. It is therefore recommended that you complete this process. Your security is important to us.

Please click on the reference link below to resolve this issue:

http://tescobank.com.sss.auth.localads.to/gr4nt/index.php

If clicking the link doesn't work, you can copy and paste it into your browser.

The Tesco Personal Finance Team



From: Matthew O'Neill
Sent: 30 November 2016 07:32
Subject: IT HelpDesk Services

Final Notice!!!... We're upgrading all staff and student Mailbox account to new version of Outlook/Exchange Web Access. kindly click on IT-ADMINHELPDESK/ACCOUNT RE-VALIDATION and act as instructed. Don't ignore to avoid your email account from been disconnected from server admin...
Upgrade now to continue using your email account.

Thank you
IT HelpDesk Services

2. The phishing email will ask you to fill out a form or click on a link or button that takes you to a fraudulent website.

3. The fraudulent website mimics the company referenced in the email, and aims to extract your sensitive personal data.

In essence, you think you are giving your information to a trusted organisation when, in fact, you are giving it to a criminal.

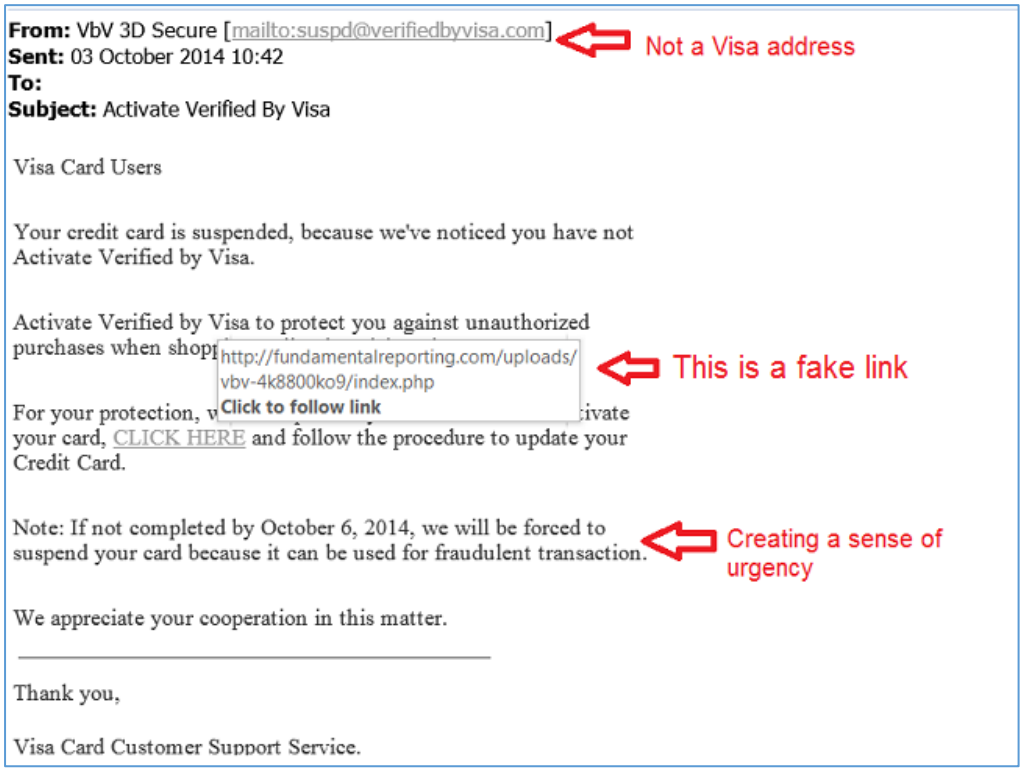
Note that phishing emails can also lure you to open suspicious attachments or visit websites that can infect your computer with malware.

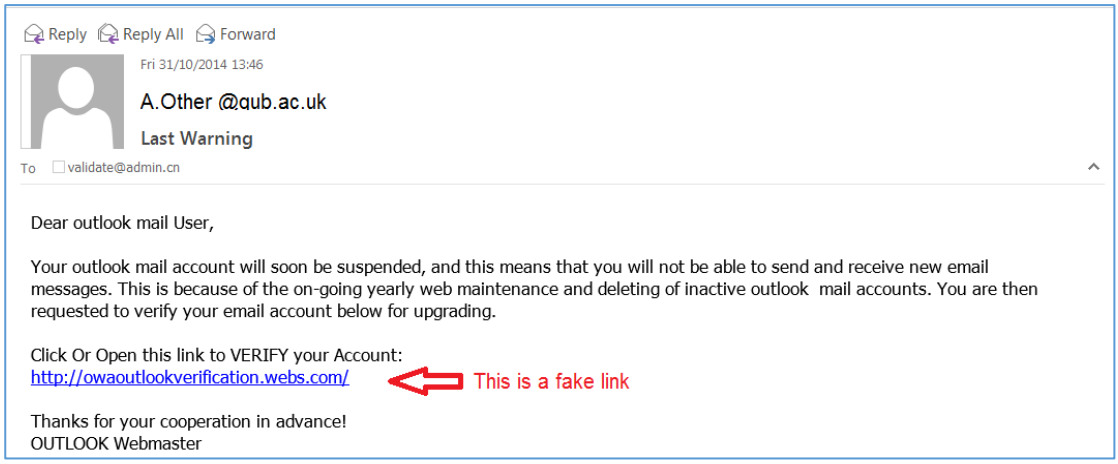
How to Spot a Phishing Email

There are many telltale signs of a fraudulent email:

- **False Sense of Urgency** – Many scam emails tell you that your account will be in jeopardy if something critical is not updated right away.
- **Spelling and grammar mistakes** – Often these emails contain multiple spelling or grammar mistakes or look unprofessional.
- **Fake Links** – The email may contain links that look genuine but are not. Check where a link is going before you click by hovering your mouse over the link in the email, and comparing it to the link that is actually displayed. If the link looks suspicious, don't click on it.
- **Invalid sender email address** – Bear in mind that the sender can disguise their email address to make a fake address seem genuine.
- **Generic greeting** – Phishing emails will often greet you as "Dear email user" or similar.
- **Attachments** – The vast majority of organizations will never send you unsolicited attachments or software. Attachments can contain viruses or malware, so you should never open an attachment unless you are 100% sure it comes from a legitimate source. Be extra careful with zipped attachments. If you do not know the sender, do not open the zipped attachment.

Here are some more examples:





What to do if you receive an unsolicited email from a company you deal with?

Many phishing emails mislead recipients by displaying one URL while taking the visitor to another. If you are ever uncertain of the validity of an email, even where it seems to come from a company you deal with routinely, do not click on any supplied links or attachments. Instead, type the web site address e.g. "www.amazon.com" directly into your browser and follow the regular links to Your Account or other destination.

Will Queen's ever ask you to update or verify your account details in an email communication?

NO – Queen's University Belfast will never ask you to update or verify your account details in an email communication and indeed no reputable company will ask for such details in an email communication. If you get any such email requests for your Queen's account details, even if they look like they came from Queen's, please forward to abuse@qub.ac.uk for advice – **DO NOT RESPOND TO ANY EMAIL ASKING YOU TO UPDATE OR VERIFY YOUR ONLINE ACCOUNT DETAILS**.

Some phishing attacks ask you to follow a link to a web page which then prompts you for your username and password. The attackers may attempt to replicate the "look and feel" of legitimate University login pages. If you are in any doubt, you MUST NOT follow the link in the email but instead use existing bookmarks, type in the address instead or seek assistance.

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

Change your password immediately and report to the organisation which maintains your account - for Queen's this is advisory@qub.ac.uk. Remember to change that same password if you use it for other online accounts and NEVER use that password ever again for any online account.

Remember that you should never use the same password for both your University and private computer accounts, such as on-line banking, Facebook etc.

What could happen if I have replied to a phishing email?

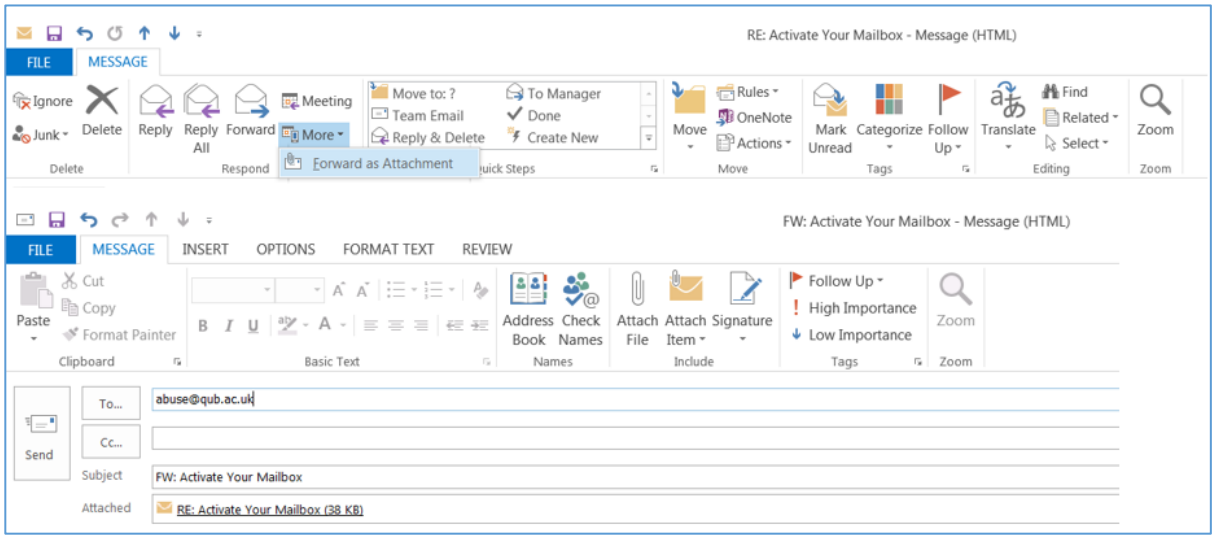
You should be aware that the confidentiality of any information protected by an account password is gone once you respond to a phishing email. This could have serious business consequences both for you personally and for Queen's University Belfast, especially if you have Queen's Corporate

Information[1] or Personal Data[2] about others in the potentially compromised account. If you have any concerns that such information may have been compromised you must report this to your Line Manager or Head of School and to infosec@qub.ac.uk, to help limit any potential damage to the University's business processes.

Report suspected phishing

If you receive an email which you are unsure about, **FORWARD** it as an attachment (see below) to abuse@qub.ac.uk where it will be evaluated to determine if it is a fake. If it is a fake, then we will get the source of the email shutdown as quickly as possible. By reporting these emails you will help to protect yourself and everyone else too.

Note: Please **FORWARD** the suspect email as an attachment as this ensures that valuable tracking information about the source is retained. The example below shows how to forward as an attachment in Outlook:



Phishing Resources

Here are some useful links to more information on phishing:

- **http://www.antiphishing.org/resources/**
- **http://education.apwg.org/**
- **http://www.onguardonline.gov/phishing**

[1] For example Financial Data, Intellectual Property, Research Data etc.
[2] Personal Data as defined by The Data Protection Act 1998