National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

HR Department Pay Rise University Spear-Phishing Alert

February 2017

UNIVERSITY SPEAR-PHISHING ALERT

The information contained within this alert is based on information received from various sources. The purpose of this alert is to increase awareness of this campaign still in circulation. The campaign's primary function appears to be harvesting financial details via a link contained within an email.

The alert is aimed at higher education establishments; however police forces and governmental agencies have also been targeted

ALERT CONTENT

Fraudsters are sending out a high number of phishing emails to university email addresses claiming to be from their own HR department. These email addresses are either spoofed or in some cases using compromised university email accounts.

The email claims that the recipient is entitled to a pay rise from their department and to click on a link to claim the pay rise.

This link then takes you to a spoofed university website telling you to enter to your personal details (including university login details and financial information). These financial details can then be used by criminals, and the login details are usually passed around and sold for future fraud campaigns.

PROTECTION / PREVENTION ADVICE

It is advisable that all universities prompt all staff and students change any password associated with their university email/IT accounts. Due to potential data breaches, it is recommended that universities discuss with the IT departments about issuing a mandatory password reset for all users.

Please also consider the following actions:

- Don't click on links or open any attachments you receive in unsolicited emails or SMS messages. Remember that fraudsters can 'spoof' an email address to make it look like one used by someone you trust. If you are unsure, check the email header to identify the true source of communication. Information on how to locate email headers can be found at https://mxtoolbox.com/Public/Content/EmailHeaders/
- Use strong passwords which include a mixture of letters, numbers and special characters, and include both upper and lower case characters. Furthermore, it is encouraged that random words as opposed to passwords with personal meanings (e.g. children's names)
- Always install software updates as soon as they become available. Whether you are updating the operating system or an application, the update will often include fixes for critical security vulnerabilities.
- If you think your bank details have been compromised, you should **immediately** contact your bank**.**
- If you have been affected by this, or any other fraud, report it to Action Fraud by calling **0300 123 2040**, or visiting www.actionfraud.police.uk.

FEEDBACK

The NFIB needs feedback from our readers to evaluate the quality of our products and to inform our priorities. Please would you complete the following NFIB feedback survey through: https://www.surveymonkey.com/r/FeedbackSDU. This should take you no more than 2 minutes to complete. If you have other feedback or additional information that you would prefer to provide by email please send to NFIBfeedback@cityoflondon.pnn.police.uk.

Handling Instructions

This report may be circulated in accordance with the protective security marking shown below and caveats included within the report. The information contained in this report is supplied by the City of London Police in confidence and may not be shared other than with the agreed readership/handling code without prior reference to the City of London Police. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 1998.

The cover sheets must not be detached from the report to which they refer.

Protective Marking:	**Not Protectively Marked**
FOIA Exemption:	NO
Suitable for Publication Scheme:	NO
Version:	V1
Storage File Location:	G:\OPERATIONAL\Fraud_Intel\Cyber Crime Desk\Alerts
Purpose:	Fraud Alert
Owner:	NFIB Management
Author:	105098P, Researcher
Review By:	DI FELTON