



PHISHING SCAM TARGETING UNIVERSITY STUDENTS

SEPTEMBER 2016

Copyright © City of London Police 2016

NFIB Disclaimer: While every effort is made to ensure the accuracy of the information or material contained in this alert, it is provided in good faith on the basis that the Commissioner, the City of London Police and its police officers and staff accept no responsibility for the veracity or accuracy of the information or material provided and accept no liability for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any information or material herein. The quality of the information and material contained in this document is only as good as the information and materials supplied to the City of London Police. Should you or your police force hold information, which corroborates, enhances or matches or contradicts or casts doubt upon any content published in this Alert, please contact the City of London Police NFIB by return.

Any use of the information or other material contained in this document by you signifies agreement by you to these conditions.




PHISHING SCAM TARGETED AT UNIVERSITY STUDENTS

The information contained within this alert is based on a high number of recent reports made to Action Fraud. The purpose of this alert is to raise awareness of a phishing scam targeted at students enlisted in the UK universities.

ALERT CONTENT

The phishing campaign, which was last highlighted in May 2016, has reappeared yet again. It claims the student has been awarded an educational grant as part of a student support programme. The email purports to have come from the Finance Department of the student's university. It tricks the recipient into clicking on a hyperlink contained in the message to provide personal details on a webpage.

Victims report that after submitting their sensitive information (including name, address, date of birth, bank account details, National Insurance Number and mother's maiden name), they were taken to a spoofed website which appeared to be a genuine representative of their online bank, where they were directed to type in their online banking credentials.

From: 
Sent: Saturday, September 17, 2016 3:55 PM
To: 
Subject:  Grant Information for you.

Dear Student,

It is my pleasure to inform you of the educational grant awarded you as part of the university student support program. This grant is awarded to selected few based on academic and financial standings. You are required to submit your information in order to receive this grant in your bank account. A link has been created for this purpose. Please see below.

[Grant Information Link](#)

Submit your information now to avoid delays.

Sincerely,

University Bursar,



PROTECTION / PREVENTION ADVICE

- Don't open attachments or click on the links within any unsolicited emails you receive, and never respond to emails that ask for your personal or financial details.
- An email address can be spoofed, so even if the email appears to be from a person or company you know of, but the message is unexpected or unusual, then contact the sender directly via another method to confirm that they sent you the email.
- If you receive an email which asks you to login to an online account, go directly to the website yourself instead of using the link provided in the email.
- If you suspect an email is a scam, do not reply to the sender. Where possible, flag the email as spam and then delete it.
- Always install software updates as soon as they become available. Whether you're updating the operating system or an app, the update will often contain fixes for critical security vulnerabilities.
- If you think your bank details have been compromised and/or you have lost money due to fraudulent misuse of your cards, you should immediately contact your bank and report it to [Action Fraud](#).

FEEDBACK

The NFIB needs feedback from our readers to evaluate the quality of our products through continuous improvement and to inform our priorities. Please would you complete the following NFIB feedback survey through: (<http://www.surveymonkey.com/s/nfibfeedback>).

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: | V1.0 |
| Storage File Location: | G:/OPERATIONAL/Fraud_Intel/CYBER_PROTECT_TEAM\Alerts.docx |
| Purpose: | Fraud Alert |
| Owner: | NFIB Management |
| Author: | 103804X, Analyst |
| Review By: | 103987P, Senior Analyst |