NEIGHBOURHOOD WATCH

Subject: "Phishing Campaign Targeting University Students"

This is a message sent via The Neighbourhood & Home Watch Network (England & Wales). This information has been sent on behalf of Action Fraud (National Fraud Intelligence Bureau)

Action Fraud is not an emergency service - dial 999 if you are in immediate danger.

Message sent by Action Fraud (Action Fraud, Administrator, National)

A new phishing campaign which has hit students of UK universities claims that the student has been awarded an educational grant by the Department for Education. The email purports to have come from the finance department of the student's university and tricks the recipient into clicking on a link contained in the message to provide personal and banking details.

One victim reported that after submitting their sensitive information (including name, address, date of birth, contact details, telephone provider, bank account details, student ID, National Insurance Number, driving licence number and mother's maiden name), they were taken to a spoofed website which appeared like a genuine website of their bank, where they were asked to type in their online banking login credentials

Protect Yourself:

- Do not click on any links or open attachments contained within unsolicited emails.
- Do not reply to scam emails or contact the senders in any way.
- If an email appears to have come from a person or organisation you know of but the message is unexpected or unusual, contact them 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 via a link provided in the email, instead of clicking on the link, open your browser and go directly to the company's website yourself.
- If you have clicked on a link in the email, do not supply any information on the website that may open.

If you think you may have compromised the safety of your bank details and/or have lost money due to fraudulent misuse of your cards, you should immediately contact your bank, and report it to Action Fraud by calling 0300 123 2040, or visiting www.actionfraud.police.uk.

==========

*Addition from JC - you can also Report by **Forwarding** to email address "NFIBPhishing@city-of-london.pnn.police.uk" or by telephone **0300 123 2040**...
'**Forwarding**' gives the Police the background information regarding the potentially Fraudulent email so that they can, if necessary, trace it back to the Originator.

Don't 'Reply' to the email since this confirms to the Sender that your email address is indeed 'Live'.
Also, don't automatically trust contact details supplied by the person contacting you.
If you need/want to contact the supposed 'Originator' then look the address up yourself via a known reputable source, such as an independent 'Google Search', Yellow Pages or the like.

Pulham Market Neighbourhood Watch Co-ordinator