National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

'Thank you for choosing to donate to Migrant Helpline' Phishing and Malware Alert

January 2017

‘Thank you for choosing to donate to Migrant Helpline’ Phishing and Malware Alert

The information contained within this alert is based on intelligence from various sources. The purpose of this alert is to increase awareness of the mass phishing campaign currently in circulation. The campaign’s primary function appears to be distributing a well known Trojan, through a malicious link contained in an email.

The alert is aimed at members of the public, local police forces, businesses and governmental agencies.

ALERT

Fraudsters are sending out a high number of phishing emails to personal and business email addresses purporting to be from ‘Migrant Helpline’.

The email address sending the majority of emails is noreply@yeshivadonations.com, however multiple email addresses have been seen. Although Migrant Helpline is a genuine charity, fraudsters are using it to trick members of the public into becoming victims of this fraud.

It should be noted that this fraud is in no way related to the real charity.

The subject line currently is ‘Thank you for choosing to donate to Migrant helpline’

The message body reads as the following:

Thanks again for donating

We're sending it straight to Migrant Helpline so you'll be making a difference very soon.
Your donation details:
First name: ****
Last name: ****
Tel. *********
Amount: £196
Donation Reference: 09493495

If you have any questions about your donation, please follow this link and download Your (Donation Reference 09493495), with the transaction details listed above.
With your help, YeshivaDonations can continue to work in Syria and neighbouring countries to deliver clean water and life-saving supplies to millions of people.

Your generosity is bringing much-needed assistance to families who have lost everything as a result of the crisis in Syria.

Warm regards,
YeshivaDonation

The first name, last name and telephone number are targeted and appear to be correct for those they are sent to.
Once the link is clicked, a well known Trojan (Ramnit) is downloaded onto the victim’s device. This malware is equipped to target and steal personal and corporate banking details.

PROTECTION / PREVENTION ADVICE

Having up-to-date virus protection is essential; however it will not always prevent your device(s) from becoming infected.

Please 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.
- 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.
- Create regular backups of your important files to an external hard drive, memory stick or online storage provider. It's important that the device you back up to is not left connected to your computer as any malware infection could spread to that as well.
- If you think your bank details have been compromised, you should contact your bank immediately**.**
- 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:	V2
Storage File Location:	G:\OPERATIONAL\Fraud_Intel\Cyber Crime Desk\Alerts
Purpose:	Alert around phishing scam containing Migrant Helpline
Owner:	NFIB Cyber
Author:	105098P
Review By:	103939P