



# **'Do Not Reply'**

## **Phishing and Malware Alert**

November 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.

## 'DO NOT REPLY' PHISHING CAMPAIGN AND MALWARE ALERT

The information contained within this alert is based on information 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 well-known malware, through an email attachment believed to be malicious.

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 pretending to come from 'donotreply' followed by the victims' own email extension (for example [donotreply@city-of-london.pnn.police.uk](mailto:donotreply@city-of-london.pnn.police.uk)).

The subject line currently is shown as a series of random numbers and letters; 'RNP0024D5D73B3A' and 'KMBT\_C220' have both been seen. The emails include an attachment – a .zip file, usually with the current date followed by random digits in the file name.

These attachments typically contain a password stealing component, with the aim of stealing your bank, PayPal or other financial details along with your email or FTP (web space) log in credentials. Many of them are also designed to specifically steal your Facebook and other social network log in details.

Similarly, a very high proportion also contain Locky ransomware, that once downloaded will encrypt files and demand money (typically about £350) to recover the files.

### PROTECTION / PREVENTION ADVICE

Having up-to-date virus protection is essential; however it will not always prevent you 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 too.
- Don't pay extortion demands as this only feeds into criminals' hands, and there is no guarantee that access to your files will be restored if you do pay.
- 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 scam, report it to Action Fraud by calling **0300 123 2040**, or visiting [www.actionfraud.police.uk](http://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](mailto: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.

<b>Protective Marking:</b>	<b>Not Protectively Marked</b>
<b>FOIA Exemption:</b>	NO
<b>Suitable for Publication Scheme:</b>	NO
<b>Version and Date:</b>	V1
<b>Storage File Location:</b>	G:\OPERATIONAL\Fraud_Intel\Cyber Crime Desk\Alerts
<b>Purpose:</b>	Alert on do not reply phishing scam
<b>Owner:</b>	NFIB Cyber
<b>Author:</b>	105098P
<b>Reviewed By:</b>	DS Paul Jones