CITY OF LONDON POLICE
National Policing Lead For Fraud

National Fraud Intelligence Bureau

Current Trends in Phishing Campaigns Landscape in the UK

Business Email Accounts Targeted with Phishing Emails to Distribute Malware

May 2017

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.

CURRENT TRENDS IN THE PHISHING CAMPAIGNS LANDSCAPE IN THE UK

The information contained within this alert is based on intelligence collated by the Cyber Protect Team at the National Fraud Intelligence Bureau (NFIB). The purpose of this alert is to raise an awareness of the recent trends in phishing campaigns targeting Internet users in the UK, and to provide advice on how to protect against the risks associated with phishing. The alert is particularly aimed at private and public sector organisations as they have been found to be the primary target of a number of mass phishing campaigns which recently emerged in the UK.

ALERT CONTENT

In recent months, the NFIB has seen a large increase in new mass phishing campaigns which **specifically targeted business email accounts of employees of SMEs, large enterprises and public sector organisations**, as opposed to private email accounts provided by free webmail providers.

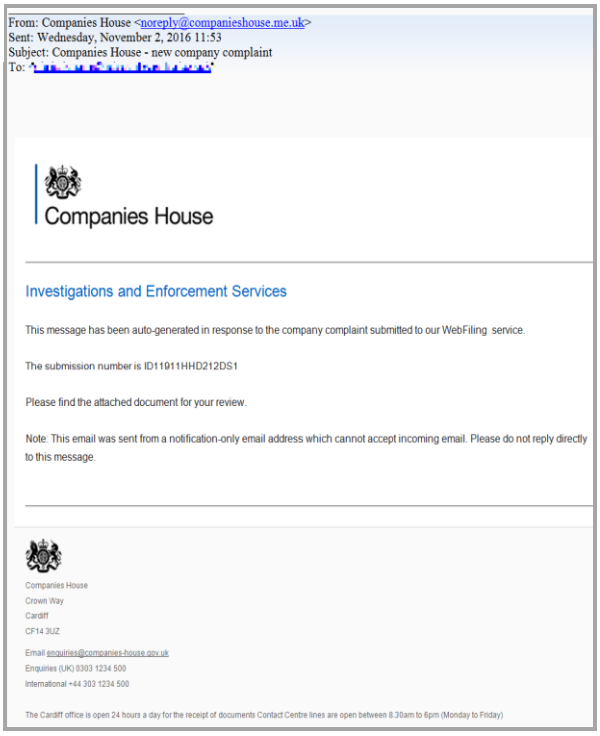
The **'phishing hook' tactics applied in the identified campaigns often focus on brand exploitation of British public sector organisations** such as police and local government authorities, Crown Prosecution Service and Companies House. Other identified campaigns were found to impersonate various business suppliers, debt collectors and parking management companies. The choice of the phishing hook and the content of the message are often highly relevant in nature to a business environment, therefore increasing its chance to deceive recipients.

Typically, **the function of the campaigns is distribution of malware such as banking Trojans and ransomware,** as opposed to campaigns designed to trick recipients into handing over their sensitive information on spoofed websites. Cyber criminals may potentially perceive the targeting of business networks with emails loaded with malware as more profitable than attacking personal computers of members of the public. Firstly, business organisations usually possess far more cash in their bank accounts compared to the public; secondly, companies may be perceived as more likely to pay a ransom to restore their business critical files when they become encrypted as a result of ransomware attack.

The recently observed phishing campaigns indicate the **growing cyber threat on British businesses and organisations**. It is important that companies have strong IT security systems and procedures in place, and employees are thoroughly trained to enable them to accurately identify malicious communication to protect their company infrastructure from risks associated with a cyber attack.

Examples of recent phishing campaigns

1



From: Companies House <noreply@companieshouse.me.uk>
Sent: Wednesday, November 2, 2016 11:53
Subject: Companies House - new company complaint
To: [redacted]

Companies House

Investigations and Enforcement Services

This message has been auto-generated in response to the company complaint submitted to our WebFiling service.

The submission number is ID11911HHD212DS1

Please find the attached document for your review.

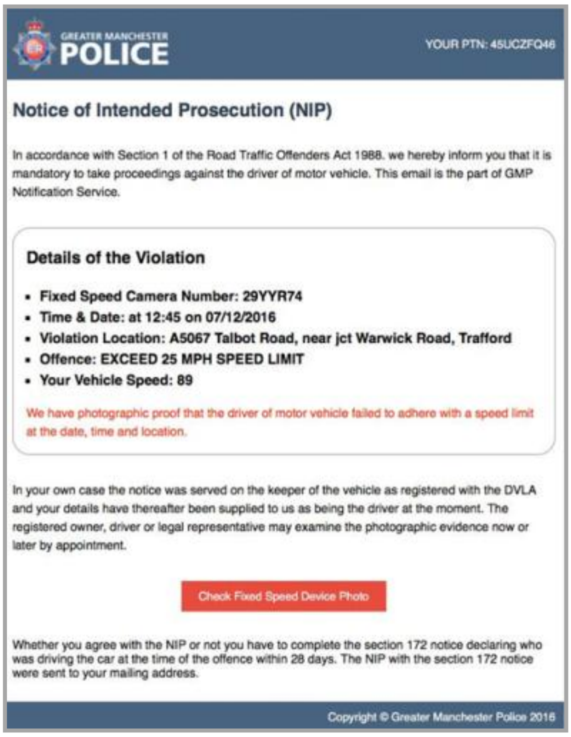
Note: This email was sent from a notification-only email address which cannot accept incoming email. Please do not reply directly to this message.

Companies House
Crown Way
Cardiff
CF14 3UZ

Email enquiries@companies-house.gov.uk
Enquiries (UK) 0303 1234 500
International +44 303 1234 500

The Cardiff office is open 24 hours a day for the receipt of documents Contact Centre lines are open between 8.30am to 6pm (Monday to Friday)

2



GREATER MANCHESTER POLICE

YOUR PTN: 45UCZFQ46

Notice of Intended Prosecution (NIP)

In accordance with Section 1 of the Road Traffic Offenders Act 1988. we hereby inform you that it is mandatory to take proceedings against the driver of motor vehicle. This email is the part of GMP Notification Service.

Details of the Violation

- **Fixed Speed Camera Number: 29YYR74**
- **Time & Date: at 12:45 on 07/12/2016**
- **Violation Location: A5067 Talbot Road, near jct Warwick Road, Trafford**
- **Offence: EXCEED 25 MPH SPEED LIMIT**
- **Your Vehicle Speed: 89**

We have photographic proof that the driver of motor vehicle failed to adhere with a speed limit at the date, time and location.

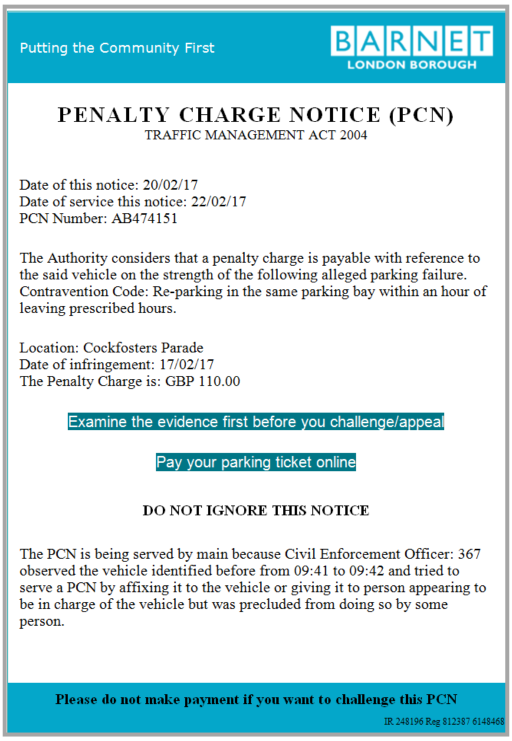
In your own case the notice was served on the keeper of the vehicle as registered with the DVLA and your details have thereafter been supplied to us as being the driver at the moment. The registered owner, driver or legal representative may examine the photographic evidence now or later by appointment.

Check Fixed Speed Device Photo

Whether you agree with the NIP or not you have to complete the section 172 notice declaring who was driving the car at the time of the offence within 28 days. The NIP with the section 172 notice were sent to your mailing address.

Copyright © Greater Manchester Police 2016

3



Putting the Community First

BARNET LONDON BOROUGH

PENALTY CHARGE NOTICE (PCN)
TRAFFIC MANAGEMENT ACT 2004

Date of this notice: 20/02/17
Date of service this notice: 22/02/17
PCN Number: AB474151

The Authority considers that a penalty charge is payable with reference to the said vehicle on the strength of the following alleged parking failure. Contravention Code: Re-parking in the same parking bay within an hour of leaving prescribed hours.

Location: Cockfosters Parade
Date of infringement: 17/02/17
The Penalty Charge is: GBP 110.00

Examine the evidence first before you challenge/appeal

Pay your parking ticket online

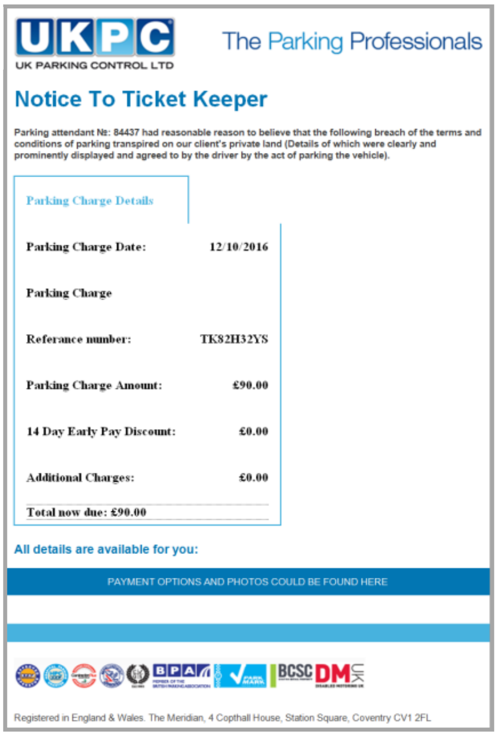
DO NOT IGNORE THIS NOTICE

The PCN is being served by main because Civil Enforcement Officer: 367 observed the vehicle identified before from 09:41 to 09:42 and tried to serve a PCN by affixing it to the vehicle or giving it to person appearing to be in charge of the vehicle but was precluded from doing so by some person.

Please do not make payment if you want to challenge this PCN

IR 248196 Reg 812387 6148468

4



UKPC UK PARKING CONTROL LTD

The Parking Professionals

Notice To Ticket Keeper

Parking attendant №: 84437 had reasonable reason to believe that the following breach of the terms and conditions of parking transpired on our client's private land (Details of which were clearly and prominently displayed and agreed to by the driver by the act of parking the vehicle).

Parking Charge Details

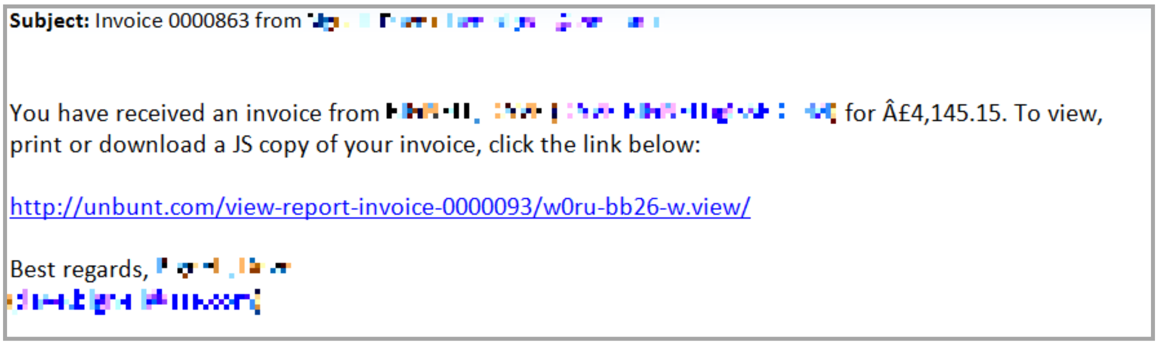
Parking Charge Date:	**12/10/2016**
Parking Charge	
Referance number:	**TK82H32YS**
Parking Charge Amount:	**£90.00**
14 Day Early Pay Discount:	**£0.00**
Additional Charges:	**£0.00**
Total now due: £90.00	

All details are available for you:

PAYMENT OPTIONS AND PHOTOS COULD BE FOUND HERE

Registered in England & Wales. The Meridian, 4 Copthall House, Station Square, Coventry CV1 2FL

5



Subject: Invoice 0000863 from [redacted]

You have received an invoice from [redacted] for Â£4,145.15. To view, print or download a JS copy of your invoice, click the link below:

http://unbunt.com/view-report-invoice-0000093/w0ru-bb26-w.view/

Best regards, [redacted]
[redacted]

PROTECTION / PREVENTION ADVICE

Although it is essential for all business organisations to have up-to-date virus protection, it will not always prevent the devices and networks from becoming infected with malware.

Please consider the following actions:

- Employees should not click on links or open any attachments they receive in unsolicited emails and SMS messages. Remember that fraudsters can 'spoof' an email address to make it look like one used by a trusted organisation. If the message is unexpected or unusual, then a contact should be made with the sender directly via another method to confirm that they sent it.
- Organisations should ensure that software updates are installed on all devices used by the business as soon as they become available. Whether updating the operating system or an application, the update will often include fixes for critical security vulnerabilities.
- Organisations should create regular backups of important business files to an external hard drive, memory stick or online storage provider. Remember that external memory storage must be disconnected from the device after the backup to prevent malware being spread out in case of infection.
- Organisations should consider obtaining UK government approved Cyber Essentials certification to protect the business against the most common internet threats. More information can be found at http://www.cyberaware.gov.uk/cyberessentials/.
- If an employee clicked on a link or opened an attachment within a suspicious email, the matter should be reported as soon as possible to the company's IT specialists for investigation.
- If your company's bank details have been compromised as a result of a phishing attack, it should be immediately notified to the bank.
- If your company has been a victim of fraud or cyber crime, please report it to Action Fraud online at http://www.actionfraud.police.uk/report-a-fraud-including-online-crime or by calling **0300 123 2040**.
- If your company has been targeted with phishing communication but it has not been responded to, please report the attempt via Action Fraud's Attempted Scams or Viruses reporting form available at https://reportlite.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 and Date:	V1
Storage File Location:	G:\OPERATIONAL\Fraud_Intel\Cyber_Protect_Team \Alerts
Purpose:	Alert: Current Trends in The Phishing Campaigns Landscape in the UK
Owner:	NFIB Management
Author:	103804, Analyst
Reviewed By:	105433, Senior Analyst