National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Phishing

May 2016

Introduction:

The purpose of this document is to provide an analysis of the most prevalent trends and characteristics of phishing campaigns in the UK in May 2016. The analysis is based on the information reported to Action Fraud via the Attempted Scams or Viruses (ASOV) Reporting Tool, as well as on the data obtained from the NFIB phishing inbox, which consists of phishing emails reported by members of the public. This report is a sanitised version of the protectively marked document.

Phishing is the attempt to acquire sensitive information (e.g. usernames, passwords and credit card details) or steal money by masquerading as a trustworthy entity in an electronic communication such as email, pop-up message, phone call or text message. Cybercriminals often use social engineering techniques to trick the recipient into handing over their personal information, transfer money or even download malicious software onto their device. Although some phishing scams can be poorly designed and are clearly fake, more determined criminals employ various methods to make them appear as genuine. These techniques can include:

- Identifying the most effective phishing 'hooks' to get the highest click-through rate.
- Including genuine logos and other identifying information of legitimate organisations in the message.
- Providing a mixture of legitimate and malicious hyperlinks to websites in the message – e.g. including authentic links to privacy policy and terms of service information of a genuine organisation. These authentic links are mixed in with links to a fake phishing website in order to make the spoof site appear more realistic.
- Spoofing the URL links of genuine websites – The most common tricks are the use of subdomains and misspelled URLs as well as concealing of malicious URLs under what appears to be a link to a genuine website which can be easily revealed upon hovering the mouse over it. More sophisticated techniques rely on homograph spoofing which allows for URLs created using different logical characters to read exactly like a trusted domain. Some phishing scams use JavaScript to place a picture of a legitimate URL over a browser's address bar. The URL revealed by hovering over an embedded link can also be changed by using JavaScript.[1]

WARNING: THIS DOCUMENT MAY CONTAIN LINKS TO MALICIOUS WEBSITES OR EMAIL ADDRESSES, DO NOT CLICK ON ANY HYPERLINKS CONTAINED IN THIS DOCUMENT.

[1] http://searchsecurity.techtarget.com/definition/phishing

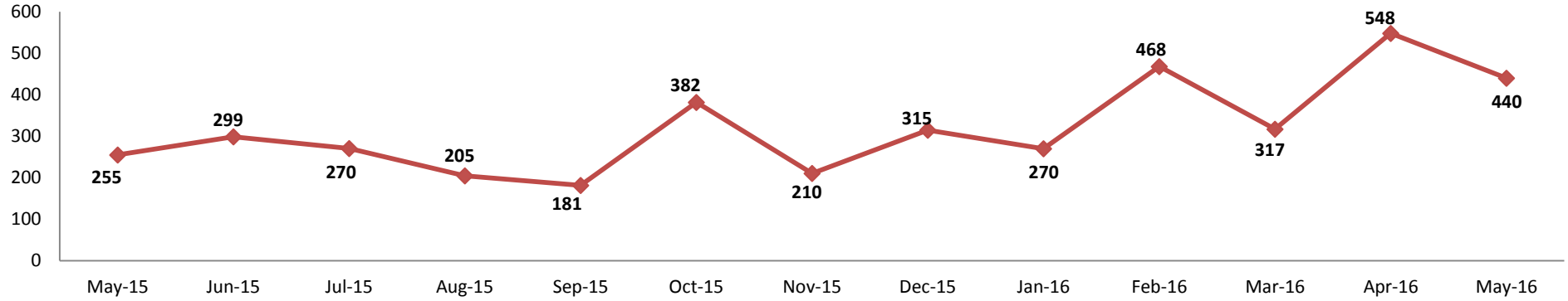
1. Action Fraud: Attempted Scams or Viruses (ASOV) Reporting Tool

The ASOV reporting tool, which is operated by Action Fraud, allows members of the public to report instances of an attempted phishing in which someone has been approached with a scam message (via email/text/or phone) but has not suffered a financial loss as a result of it and has not exposed their personal details to a fraudster.

1.1 Volume of Phishing Reports Received

In May 2016, there were a total of 13,630 phishing reports made to the ASOV reporting tool by members of the public. This is on average 440 reports made per day, which is a **72.6% increase compared to May 2015** and a 19.7% decrease compared to April 2016.

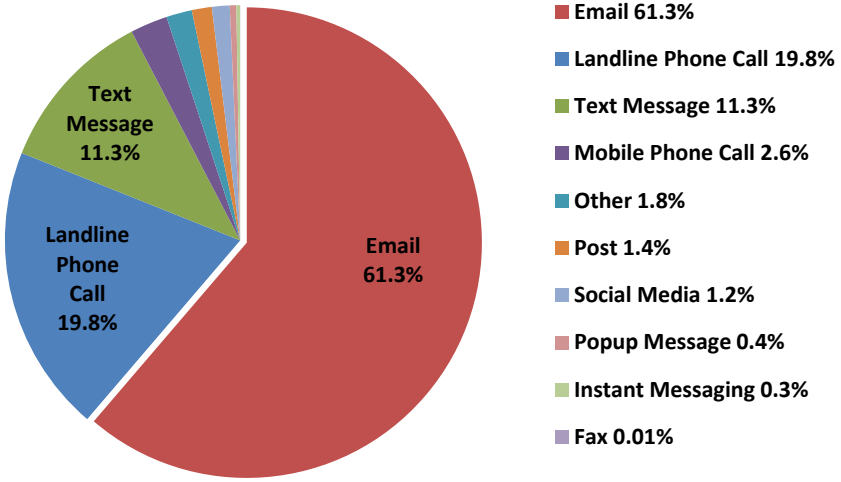
Average Number of Phishing Reports Received per Day: May 2015 - May 2016



1.2 Communication Channels for Phishing

In May 2016, although the most commonly reported communication channel used for phishing distribution continued to be email, there has been a drop in reporting in relation to this method of communication from 78% in April, 73% in March and 72% in February 2016 to 61.3% in May 2016.

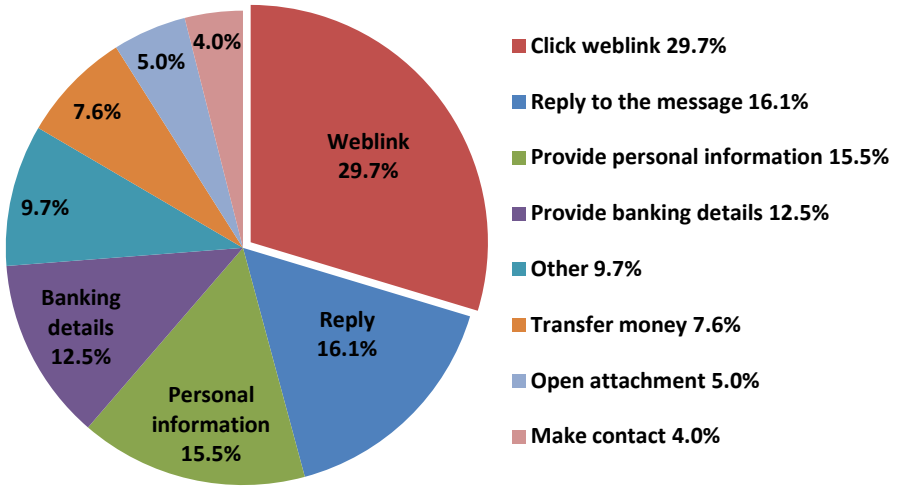
The second most commonly reported communication method was a landline phone call (19.8%) which is an increase of 6 to 9 percentage points compared to the previous three months. The reporting figure for text message has also increased to 11.3%, which is 2 to 5 percentage points higher compared to the previous months.



1.3 Type of Phishing Request

Similarly to the previous months, the most commonly reported phishing request was to click on a potentially malicious hyperlink contained in the message (29.7%). The second most reported type of request was to reply to the phishing message (16.1%), followed by the requests to provide personal information (15.5%) or online banking/bank card details by 'would be' victims (12.5%).

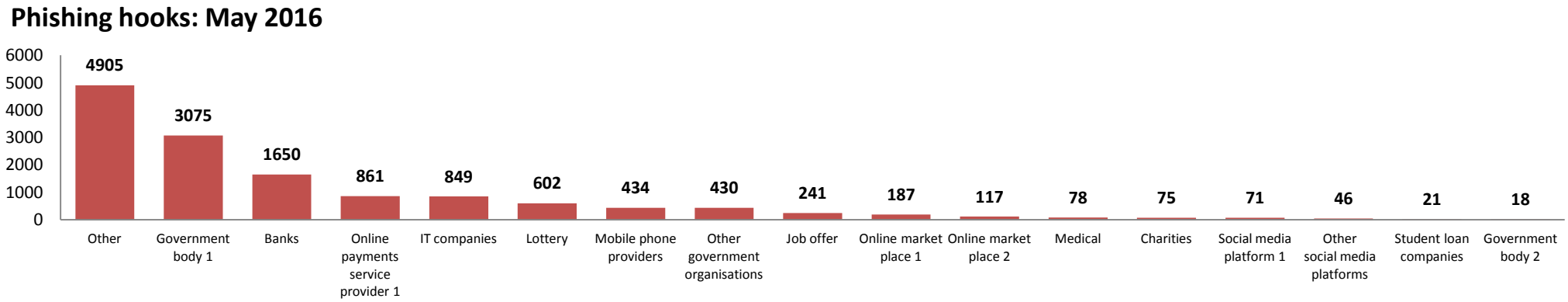
The reported figures largely reflect the trends noted in the previous months with an exception of April 2016, which saw higher than usual number of reports in relation to 'click on the web link' and 'transfer money' type of request.

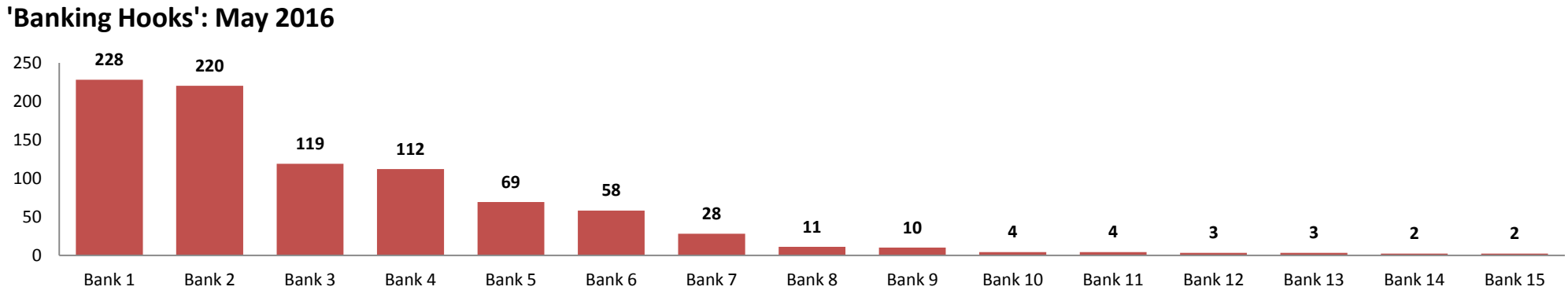


1.4 Phishing 'Hooks'

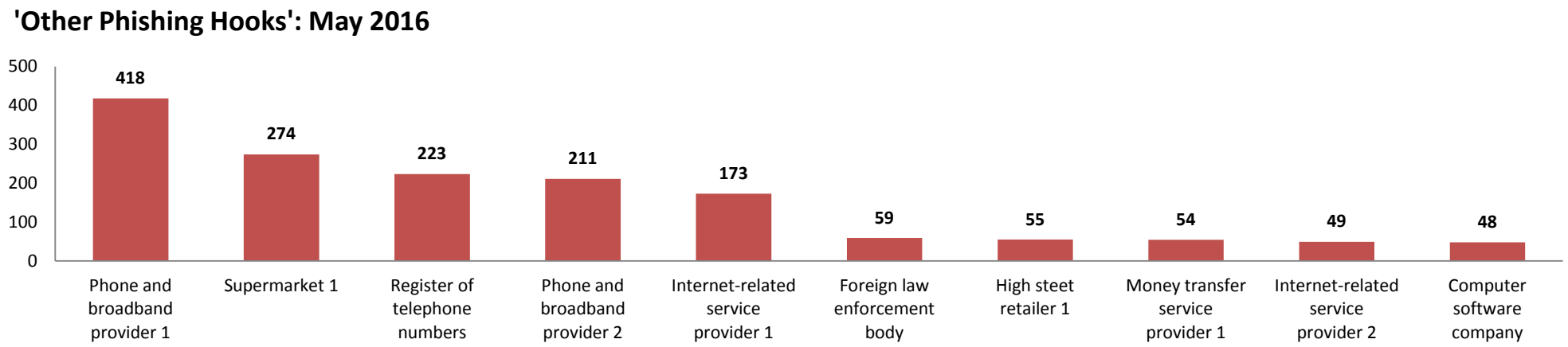
Phishing 'hook' is a social engineering method which is used to masquerade as a trustworthy entity in communication in order to trick the potential victim to follow an instruction or request contained in the message for malicious reasons. Throughout May 2016, the most prevalent phishing 'hooks' identified from the reported data continued to be within 'Other hooks' category, followed by 'hooks' which referred to a certain government body and the banking sector.

Just over half of all reports (51%) within the 'Banking Hooks' category related to just two leading high street banks (Bank 1 - 26%, Bank 2 - 25%).





Within the 'Other phishing hooks' category, the most reported individual hook in May 2016 was associated with the name of a certain phone and broadband provider.[2] There has also been an **increase in reporting in relation to a certain high street supermarket's name from 12 reports in March 2016 and 58 reports in April 2016 to 274 reports in May 2016**. The increase reflects a recently noted expansion of phishing campaigns pretending to offer complimentary shopping vouchers and free gift cards.



2. NFIB Phishing Inbox

The findings presented below are based on the analysis of over **25,000 phishing emails** reported to the NFIB phishing inbox over the period of **1st to 31st May 2016.**[3] The names of companies and organisations utilized by scammers in phishing campaigns have been replaced by *** symbol in this report to protect their brand identity.

[2] It should be noted that the level of analysis of the 'Other phishing hooks' is limited due to the presence of free text fields in relation this category within the ASOV reporting tool. Although the best possible effort has been made to calculate and identify trends in this category, the presented figures may be understated.

[3] Once the reporting person submits their online ASOV form to Action Fraud, they are directed to forward the phishing email to a dedicated phishing inbox of HMRC, DWP, all major banks, PayPal, eBay, Amazon, Facebook or Student Loans Company if the scam message purports to be originating from one of these organisations, or to the NFIB phishing inbox in all other cases

2.1 Subject Headings of Phishing Campaigns – Top 15

The below table represents the Top 15 most prevalent subject headings which appeared in the phishing emails forwarded to the NFIB phishing inbox by members of the public in May 2016. Similarly to the previous month, the most commonly reported phishing campaign theme continued to refer to free shopping vouchers/gift cards offering. The names of four specific retailers and supermarkets seemed to be more frequently targeted compared to other leading retailers. Additionally, there has been an increase in reporting of phishing scams which claim that a certain money transfer services organisation is in receipt of large funds for a recipient.

	Message title	Number of emails reported	Phishing campaign theme / Phishing hook
1	FROM THE *** BUREAU OF ***	81	Consignment scam
2	Important: Your account has received a voucher	78	High street retailer 1 scam
3	From: *** Office Of International *** Services	75	Compensation scam / Money transfer service provider 2
4	Thank you. Your reservation number has been released	75	High street retailer 2 scam
5	Open your *** Complimentary Prizes	73	High street retailer 1 scam
6	Thank you Voucher on your account	72	High street retailer 1 scam
7	Click for your *** Complimentary Prizes	69	High street retailer 1 scam
8	You have received a £500 *** Gift Card	64	Supermarket 1 scam
9	Your reservation # BH0-0089-UK	60	High street retailer 2 scam
10	Call to verification	49	Donation beneficiary scam / Money transfer service provider 1
11	Thank you. Do not forget your *** Package	46	High street retailer 2 scam
12	*** Transaction Approved	45	Donation beneficiary scam / Money transfer service provider 1
13	Pick your Voucher!	44	Supermarket 2 scam
14	Your *** giftcard	44	Supermarket 1 scam
15	*** bill failed direct debit payment	43	Phone and broadband provider 1

2.2 Email Addresses of Phishing Scammers – Top 15

The table represents the Top 15 most prevalent email addresses used to send out phishing emails to different members of the public. **Email spoofing** to impersonate well known companies continued to be the method of choice in phishing campaigns circulated in May 2016, with the names of a certain money transfer service provider and phone and broadband provider being the most common targets.

	Email address	Number of emails reported	Phishing campaign theme/phishing hook
1	***.***@***.se	**101**	Money transfer service provider 1 scam
2	pbsupdates@act.pbs.org	**83**	Various scams including free supermarket gift cards
3	info10@***.com	**61**	Money transfer service provider 1 scam
4	***@***my.com	**50**	Money transfer service provider 1 scam
5	no.reply@leboncoin.fr	**32**	Various scams including free supermarket gift cards
6	info@ds.curvadiscontinua.com	**26**	Various scams including free supermarket gift cards.
7	ebilling@***.com	**26**	Phone and broadband service provider 2 account scam
8	fremedios@natomas.k12.ca.us	**25**	Donation beneficiary scam
9	***@***.edu	**22**	Retail bank 5 account scam
10	contact@jobijoba.com	**21**	Various supermarkets free gift cards scam
11	***@my.com	**21**	Money transfer service provider 1 scam
12	sssss@***.com	**19**	Various scams including credit report application
13	account@zepeem.com	**19**	Various scams including free supermarket gift cards
14	***services@***.***.com	**17**	Phone and broadband service provider 2 scam
15	account-update@***.co.uk	**16**	Online market place 1 account scam

2.3 Malicious URLs Contained in Phishing Emails – Top 15

The table represents the Top 10 most prevalent URLs (Uniform Resource Locators also known as web addresses), which appeared, in exactly the same form, in the phishing emails forwarded to the NFIB phishing inbox by different members of the public during May 2016. The top URL identified in the dataset h*tp://www.***giveaways.com/*** is closely associated with the name of a certain high street retailer, which has been one of the most heavily utilized phishing hooks in this report's findings.

	Malicious URL	Number of emails reported	Phishing campaign theme/phishing hook
1	h*tp://www.***giveaways.com/***	43	High street retailer 1 free shopping voucher scam
2	h*tp://www.bressanbike.it/sec/Click	19	Retail bank 5 account notification scam
3	h*tp://t.ymlp29.net/mmagaejuhyavahhaiau/click.php	15	Supermarket 3 free gift card scam
4	h*tp://59-127-41-142.hinet-ip.hinet.net/wordpress/custom/pay.php	14	Online market place 1 account scam
5	h*tp://02365.com/l/here	11	Internet-related service provider 1 account scam
6	h*tp://t.ymlp27.net/quazaejuhbaoawjuatau/click.php	10	Supermarket 1 free gift card scam
7	h*tp://dilmahtea.co.uk/tru.htm	10	Supermarket 4 free shopping voucher scam
8	h*tp://187.red-88-9-45.dynamicip.rima-tde.net/wordpress/custom/***.php	9	Internet-related service provider 1 account scam
9	h*tp://***id.strikingly.com/	5	Phone and broadband provider 2 account scam
10	h*tp://t.ymlp44.net/esagaejesuatahseacau/click.php	5	Credit card application scam
11	h*tp://kd111104215033.ppp-bb.dion.ne.jp/wordpress/uk.php	5	Online market place 1 account scam
12	h*tp://tinyurl.com/hytxcmcLog	5	Phone and broadband provider 2 account scam
13	h*tp://ow.ly/DlPp300259R	5	Phone and broadband provider 2 account scam
14	h*tp://tinyurl.com/hu55lxf	3	Phone and broadband provider 2 account scam
15	h*tp://com-verifacc.com/	3	Online payments provider 1 account scam