National Fraud Intelligence Bureau

NOT PROTECTIVELY MARKED

CITY OF LONDON POLICE
National Policing Lead For Fraud

PHISHING

July 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 July 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. The names of companies being subject of analysis in this document have been replaced by general naming which reflects a type of services the respective companies provide or a type of industry they belong to. Where the name of the company is contained within the email address or URL link, it has been replaced with * symbol.**

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.
- **Enclosing 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 to make the scam email appear genuine.
- **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 CONTAINS LINKS TO MALICIOUS WEBSITES AND EMAIL ADDRESSES; DO NOT CLICK ON ANY HYPERLINKS CONTAINED IN THIS DOCUMENT.

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

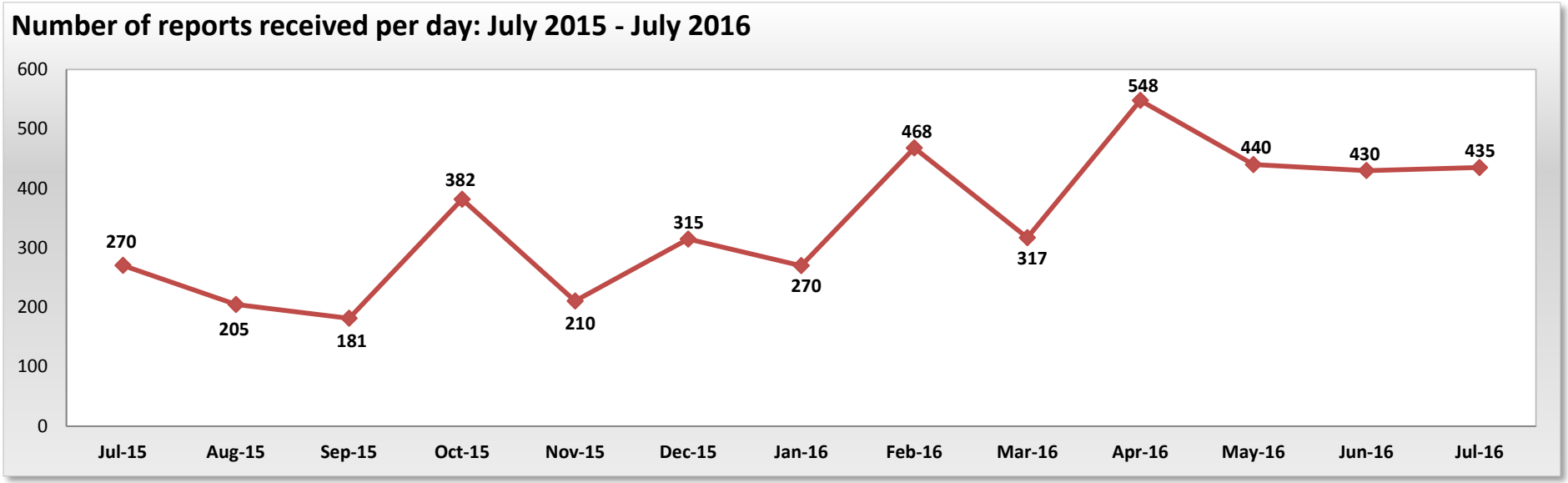
Section 1: Action Fraud: Attempted Scams or Viruses (ASOV) Reporting Tool

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

1.1 Volume of Phishing Reports Received

In July 2016, there were a total of **13,515 phishing reports** submitted via the ASOV reporting tool by members of the public, which is a **61.2% increase compared to July 2015**

With 435 reports made per day, July 2016 marked the first period since at least November 2013, in which the reporting figures have reached a stable level for the third consecutive month.

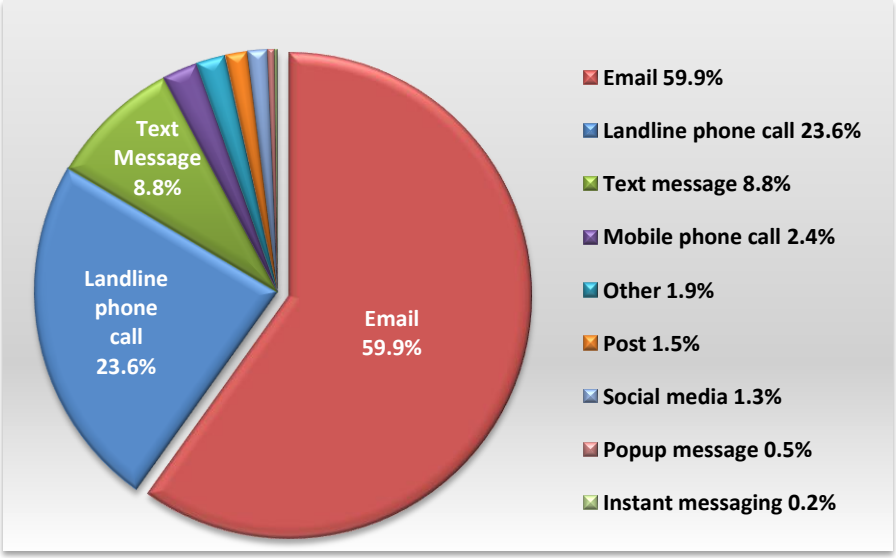


1.2 Communication Channels for Phishing

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 2016, 61.3% in May 2016 and 60.1% in June 2016 to 59.9% in July 2016.

The second most commonly reported communication method was a **landline phone call declared in 23.6% of all reports**. This is an increase by 1.5 percentage points compared to June 2016, 3.4 percentage points as compared to May 2016 and 13.2 percentage points more than in April 2016.

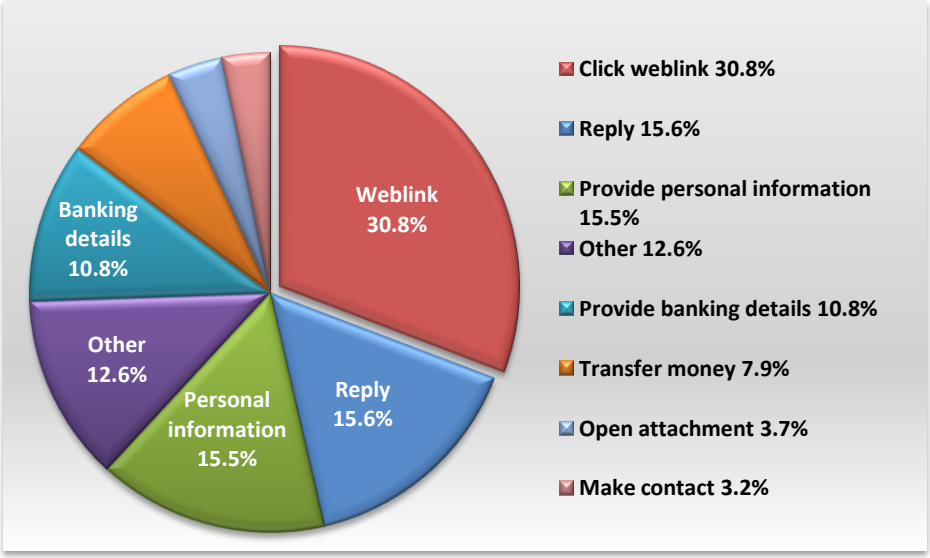
In contrast, the reporting figure for text message has been fluctuating in the recent months between 6.3% in April, 11.3% in May and 10.5% in June 2016 compared to 8.8% in July 2016.



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 (30.8%).** The second most reported type of request was to reply to the phishing message (15.6%), followed by the requests to provide personal information (15.5%) and online banking/bank card details by 'would be' victims (10.8%).

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 weblink' and 'money transfer' type of request.

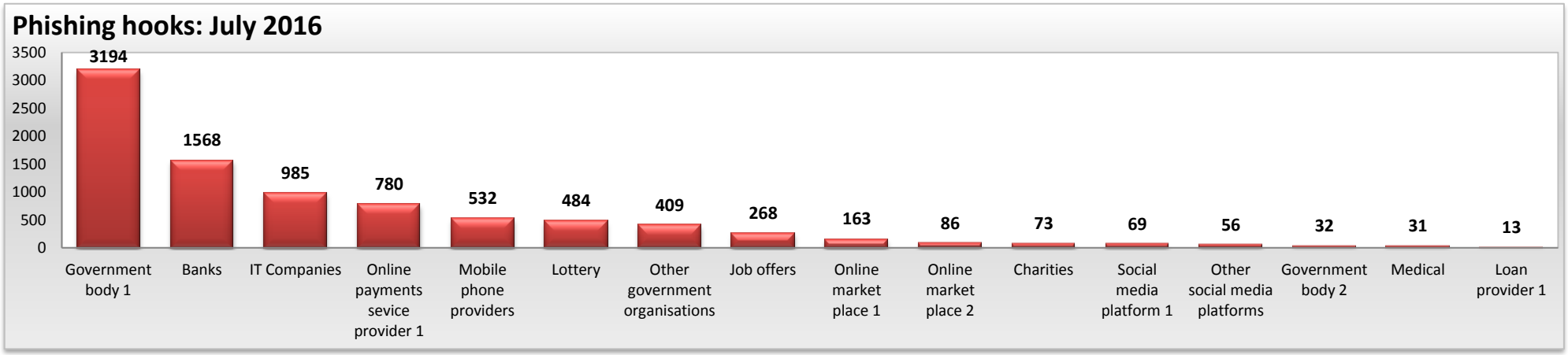


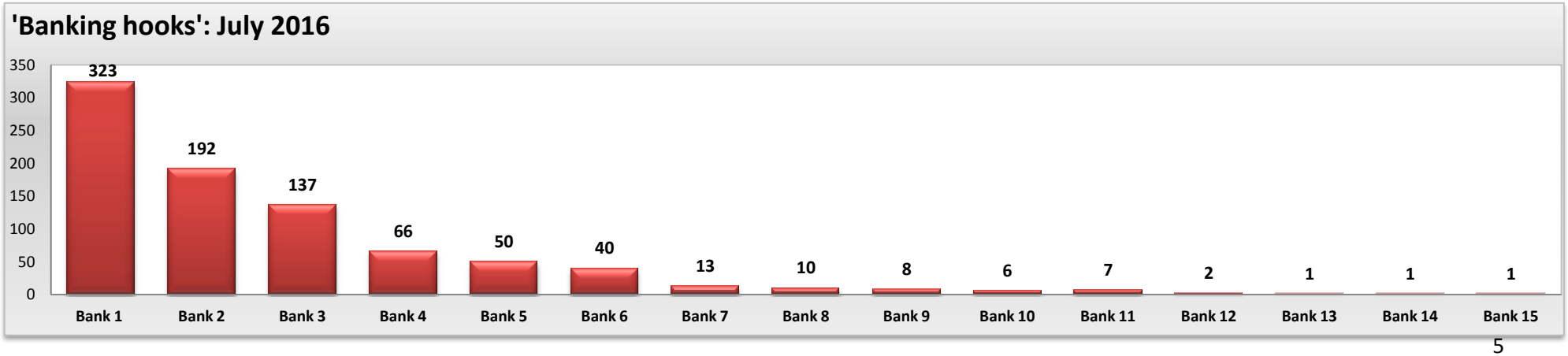
1.4 Phishing 'Hooks'

Phishing 'hook' is a social engineering method which **is used by fraudsters to masquerade as a trustworthy entity** in communication, in order to trick the potential victim to follow an instruction contained in the message for malicious reasons.

Throughout July 2016, the most prevalent phishing 'hooks' identified from the reported data continued to be **Government body 1** and **various retail banks.**

The most popular names reported within the 'banking hooks' category were **three high street banks**, which were declared in 37.7% (Bank 1), 22.4% (Bank 2) and 16% (Bank 3) of reports. These banks have also been the top three 'banking hooks' in the previous months.



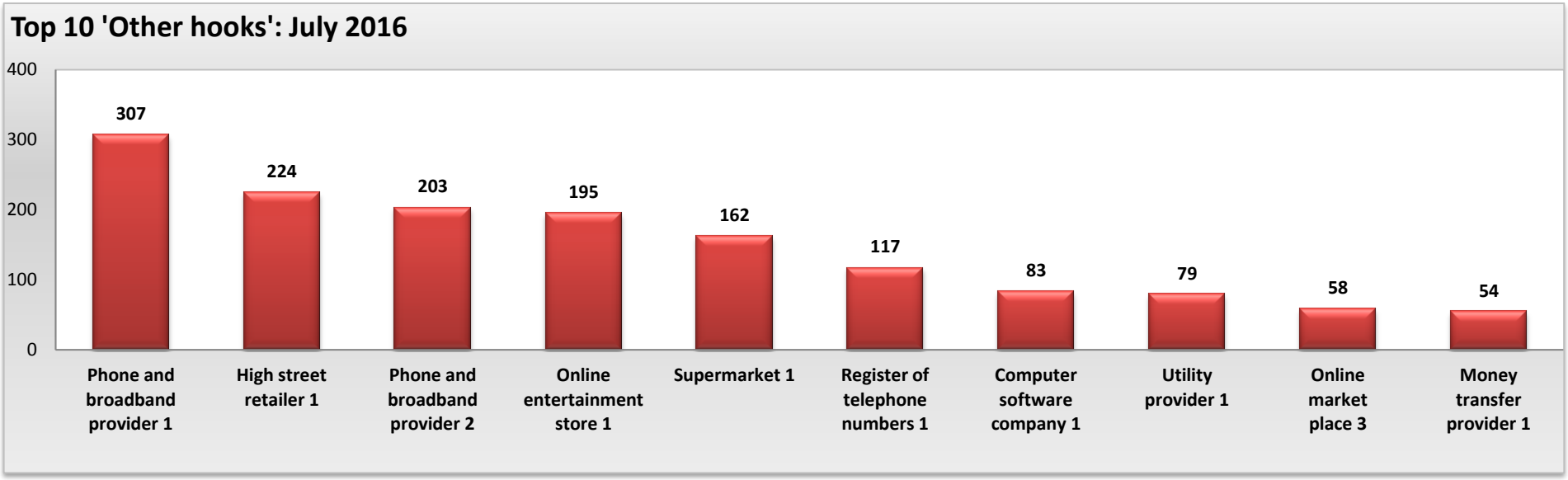


Within the 'Other phishing hooks' category[2], the most reported individual hook was **Phone and broadband service provider 1.**

There has been an increase in reporting of **High street retailer 1** as a phishing hook from 68 reports in April 2016, 55 in May 2016 and 96 in June 2016 to 224 reports in July 2016. Thereby, this retailer became the top reported hook within the retail sector category, by outstripping other retailer named here as Supermarket 1 which has been the most prevalent supermarket/retail hook in the last quarter.

The recent increase in misuse of well known retailers' names is a result of an expansion of phishing campaigns claiming to offer complimentary gift cards and shopping vouchers from major UK stores.

In July 2016, there has also been a new occurrence of a phishing scam in circulation which claimed to originate from **Utility provider 1**, with 79 reports being made to the ASOV tool by members of the public. The campaign purported to relate to an outstanding utility bill and called for payment through a malicious link. Majority of emails originated from the same email address ***@otherserver.com (see section 2.2)[3].



[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] The possible discrepancy in the number of reports relating to the same phishing campaign which are presented in Section 1 and Section 2 of this analysis is caused by the fact that both reporting systems – the ASOV tool and the NFIB Phishing Inbox - are independent of each other.

Section 2: NFIB Phishing Inbox

The findings presented in Section 2 are based on the analysis of **over 28,000 phishing emails** forwarded to the NFIB phishing inbox during the period of 1st to 31st July by members of the public.[4]

2.1 Subject Headings of Phishing Campaigns – Top 15

The table represents the Top 15 most prevalent message subject headings which appeared in exactly the same form in the phishing emails reported in July 2016.

The most commonly reported phishing scam with the same subject line purported to originate from **Online entertainment store 1** and contained **bogus information about an alleged purchase made through the online store**. One third of all subject lines identified within the Top 15, in total **517 emails,** related to the scam, which is the highest proportion noted to date.

The second most common message subject line referred to **free shopping vouchers offering from three well known UK retailers,** which reflects the trend from the previous months.

	Message title	Number of emails reported	Phishing hook
1	Your receipt No ...	132	Online entertainment store 1 scam
2	Order Receipt No ...	128	Online entertainment store 1 scam
3	Your receipt from ***	102	Online entertainment store 1 scam
4	Payment Approved!	100	Money transfer service provider 1 scam
5	*** prize offer – Open immediately	90	High street retailer 1 scam
6	Your *** order receipt	83	Online entertainment store 1 scam
7	Hi, you can get our Grand Prize this week!	80	Supermarket 1 scam
8	Re-activate your voucher :)	77	High street retailer 2 scam
9	Your invoice from ***	72	Online entertainment store 1 scam
10	Account Closure ***	70	Bank 1 online transaction scam
11	We have an important message for you!	66	Bank 1 account scam
12	Your account has been closed	63	Bank 2 account scam
13	You forgot to download your *** Voucher	60	High street retailer 1 scam
14	Good News!...Your Email Has Been Selected as Winner	58	Lottery scam
15	Your voucher has just expired	58	High street retailer 2 scam

[4] 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.

2.2 Email addresses of Phishing Scammers – Top 15

Email address spoofing to impersonate well known companies continued to be the method of choice in July's phishing campaigns, with email addresses appearing to be from **Online entertainment store 1** and **Money transfer service provider 1** being the most popular.

Utility provider 1 has been identified as a new target for email spoofing to perpetrate a phishing scam in their name. A total of 86 fake utility bill emails which appeared to originate from ***@otherserver.com were reported in July 2016 by different members of the public, who were called by their name and surname in the email. The content and format of the emails were identical, but variations in the subject line were noted such as *'(Name and Surname) Your gas & electricity bill'*, *'(Name and Surname) Your July electricity bill'* and *'(Name and Surname) Pay your July bill Online'*.

The **use of a personal greeting in the phishing campaign** impersonating Utility provider 1 appears to be a result of a **data leak**. It is unlikely that the personal details were obtained directly from that company's database as many members of the public stated that they in fact deal with a different utility provider.

	Message title	Number of emails reported	Phishing campaign theme / Phishing hook
1	***@otherserver.com	86	Utility provider 1 bill statement scam
2	***02@citromail.hu	71	Money transfer service provider 1 inheritance payment scam
3	notice@***.org	68	International fund beneficiary scam
4	***@bt.net	66	Bank 1 suspicious online activity scam
5	info@***.com	64	Money transfer service provider 1 inheritance payment scam
6	ID4PR1X2@mobi.***.com	59	Online entertainment store 1 receipt scam
7	careers@***.co.uk	54	Employment offer scam
8	luann.***@colostate.edu	51	Donation beneficiary scam
9	support@***.***.com	46	Online entertainment store 1 receipt scam
10	*eurorafle@btinternet.com*	33	Lottery scam
11	***@***.co.uk*	31	Online payments service provider 1 and Phone and broadband provider 2 account scam
12	*dpmdvpd@mxip1a.gatech.edu*	29	Online entertainment store 1 receipt scam
13	msa@communication.***.com	29	Bank 1 and Computer software account update scam
14	service@***.co.uk	29	Online payments service provider 1 transaction scam
15	*dcmartin1@cox.net*	28	Donation beneficiary scam

2.3 Malicious URLs – Top 15

The table represents the Top 15 most prevalent URLs which appeared, in exactly the same form, in the phishing emails forwarded to the NFIB phishing inbox by the public in July 2016.

The URL h*tp://www.sp-miescisko.org.pl//go.php belonging to the official website of a primary school in Poland, has been the most commonly utilised URL identified in the dataset with **a total of 46 Bank 1 fake account verification emails** reported.

12 out of 15 URLs identified in the dataset were found to belong to legitimate domains which may have been compromised to host a malicious content.

Overall, the most prevalent URLs identified in the Top 15 set were utilised in those phishing campaigns which impersonated the companies named here as **Bank 1, Online payments provider 1 and Online entertainment store 1**.

	Message title	Number of emails reported	Phishing campaign theme/ Phishing hook
1	h*tp://www.sp-miescisko.org.pl//go.php	46	Bank 1 account scam
2	h*tp://lastablasmias.com/?Im9mZj03NTci	29	Various scams including free gift cards
3	h*tp://difusoragoiania.com.br/121/hhaa.html	28	Bank 1 account scam
4	h*tp://latrastiendalibros.com/lj/index.htm	27	Online payments service provider 1 account scam
5	h*tp://www.praulaiglesia.com/ln	23	Online payments service provider 1 account scam
6	h*tp://www.***.co.uk-online-customers-personal-support-privacy-policy.fletcherfarmfoundation.org/wp-includes/	22	Bank 1 account scam
7	h*tp://rdi21redi.com/newsfeed/	21	Online entertainment store 1 purchase scam
8	h*tp://gekkoanimatie.be/membership.php	21	Video on demand service provider 1 membership
9	h*tp://ajanimalservices.co.uk/sod	20	Government organisation 1 tax refund scam
10	h*tp://daizeymay.co.uk/sxx	19	Bank 1 account scam
11	h*tp://ipx313.com/newsfeed/	18	Online entertainment store 1 purchase scam purchase
12	h*tp://www.laflandre.be/Config/***/	17	Online payments service provider 1 account scam
13	h*tp://chinchillasite.be/req.php	16	Phone and broadband provider 2 refund scam
14	h*tp://www.chascojeans.pt/b/	16	Online payments service provider 1 account scam
15	h*tp://www.savirow.com/data/backup/www/empty/bice1.htm	16	Government organisation 1 tax refund scam