National Fraud Intelligence Bureau

NOT PROTECTIVELY MARKED

CITY OF LONDON POLICE
National Policing Lead For Fraud


# Phishing in the UK

August 2016

# Introduction:

**The purpose of this document is to provide analysis of the most prevalent trends and characteristics of phishing campaigns in the UK in August 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 The names of companies being subject of analysis in this document have been replaced by general naming which reflects a type of services the respective companies provide or a type of industry they belong to.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. Cyber criminals 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 experienced 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 the concealment 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

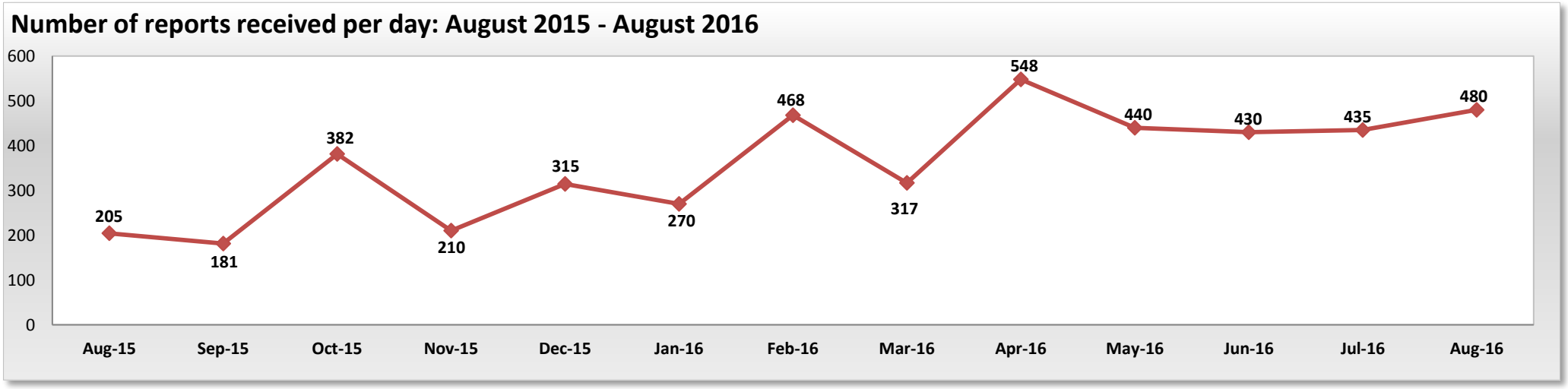
# Section 1: Action Fraud: Attempted Scams or Viruses (ASOV) Reporting Tool

The ASOV reporting tool, which is provided by Action Fraud, allows members of the public to report instances of attempted phishing, where someone has been contacted through 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 August 2016, there were a total of **14,883 phishing reports** submitted to Action Fraud through the ASOV reporting tool by members of the public, which is an **increase by nearly 135% compared to August 2015**.

With 480 reports made a day, August 2016 marked the fourth consecutive month of steady reporting levels.

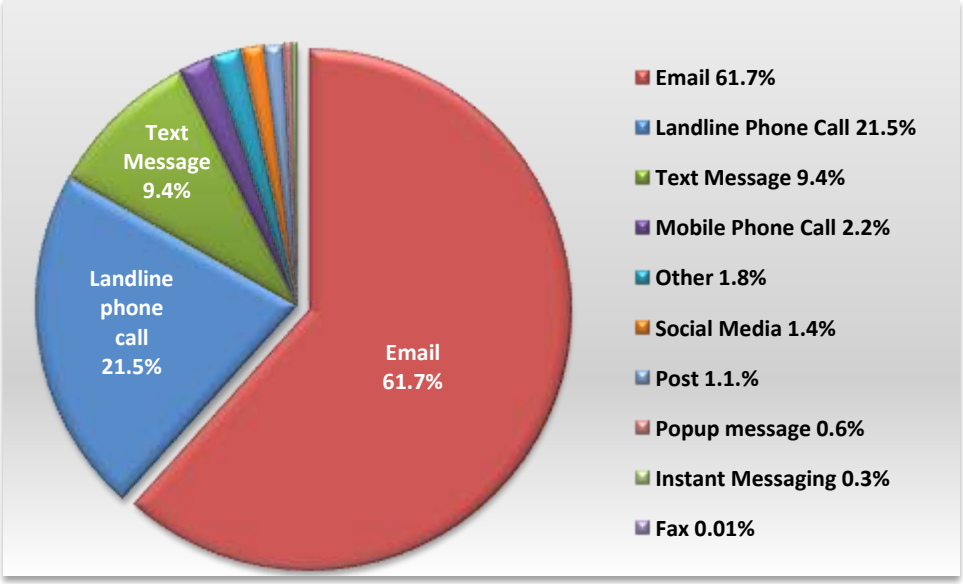


## 1.2 Communication Channels for Phishing

In August 2016, **the most commonly reported communication channel** used for phishing distribution **continued to be an email**, which was stated in **61.7%** reports. The mean figure for this communication method in the previous three months was recorded at 60.4%.

The second most prevalent communication channel used for phishing purposes was a **landline phone call declared in 21.5% of all reports**, which is in line with the mean of 21.8% for the previous three months.

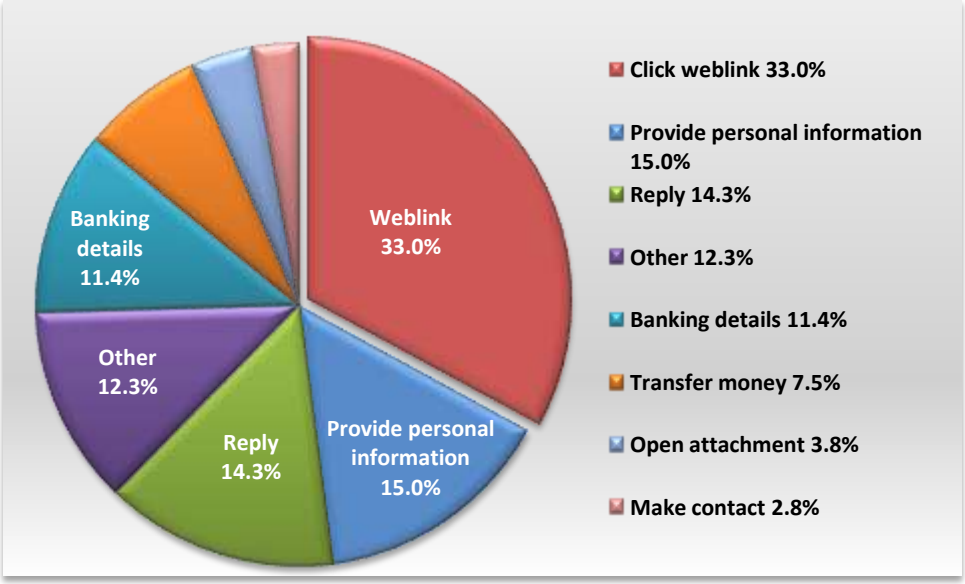
The reported figure for a **text message was 9.4%** and the mean for the past three months was recorded at 10.2%.




## 1.3 Type of Phishing Request

Similarly to the previous months, **the most commonly reported phishing request,** stated in **33%** of reports, was to **click on a potentially malicious hyperlink** contained in the message. This is nearly 3 percentage points more than the mean of 30.3% recorded in the previous three months.

The second most reported type of request was to provide personal details (15%), followed by the requests to reply to the message (14.3%). 11.4% of the reported scams were aimed at obtaining online banking/bank card details from 'would be' victims. The reported figures for these types of requests were slightly lower in August 2016 than their mean values for the past three months.



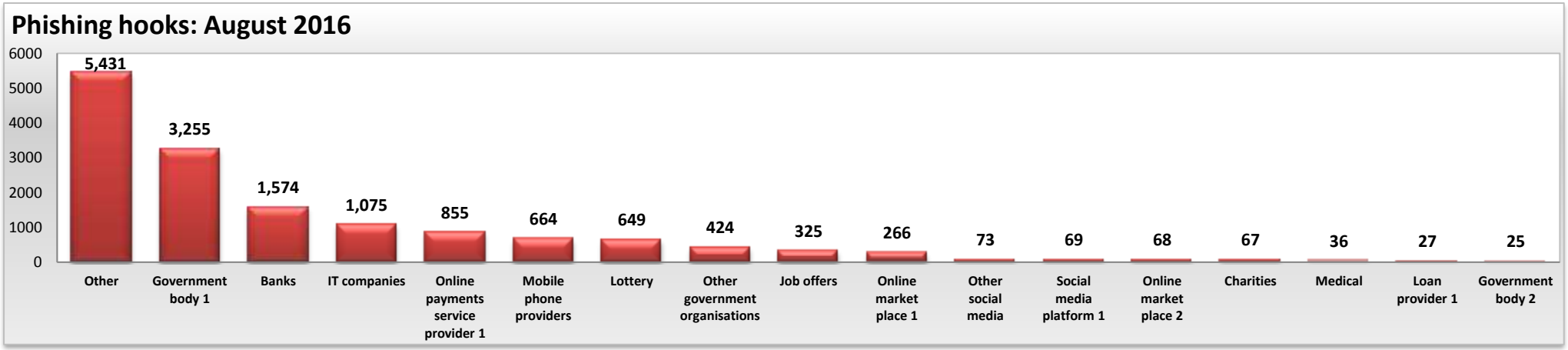
## 1.4 Phishing Hooks

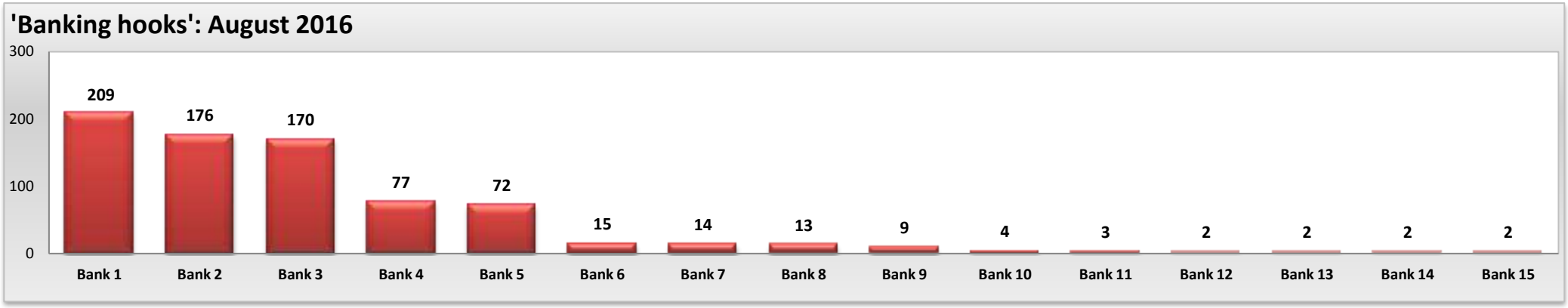
**'Phishing hook'** is a social engineering method **used by fraudsters to masquerade as a trustworthy entity** in communications. The method is used to trick the potential victim to follow an instruction contained in the message for malicious reasons.

Throughout August 2016, the most prevalent 'phishing hooks' identified from the reported data continued to be **Government body 1** and **retail banks**, with 3,255 and 1,574 reports submitted by members of the public, respectively. The reporting levels largely reflect the trends noted in recent months, with the quarterly mean of 3,229 reports for Government body 1 and 1,605 reports for the retail banking sector recorded in the previous three months.

According to the reported figures, fraudsters were most likely to impersonate Government body 1 in scams perpetrated through email (51%), landline phone call (27%) and text message (20%). Nearly three quarters of retail banks phishing scams were communicated via email (73%), followed by text message (12%). IT companies which include software and internet providers were most commonly impersonated in scam landline and mobile calls (80%), followed by mass email campaigns (14%).

**Bank 1, Bank 2** and **Bank 3** have sustained the position of **the top 3 'banking hooks'** for another month. The names were exploited in the mass email phishing campaigns in all reported cases.

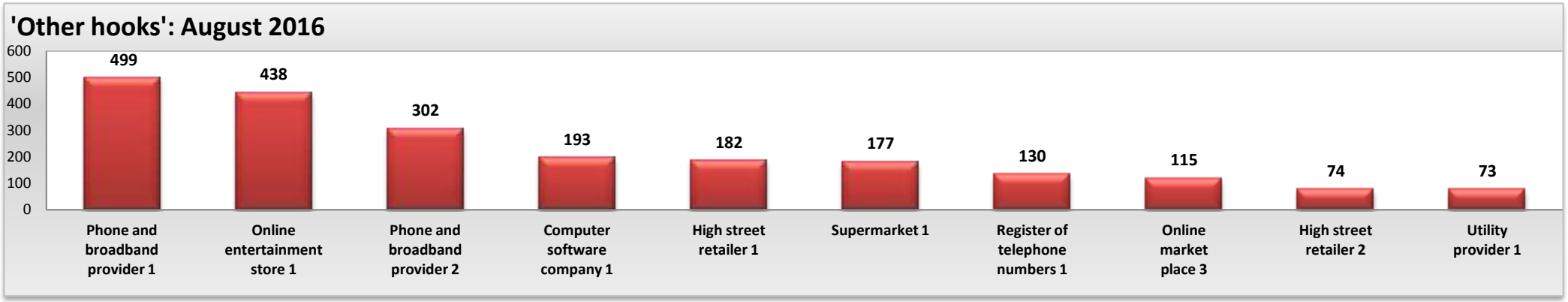





Within the 'Other phishing hooks' category[2], the highest number of reports concerned the phishing scams impersonating **Phone and broadband provider 1** and **Online entertainment store 1.** Phone and broadband provider 1 scams were most commonly perpetrated through landline phone calls, whilst the most utilised communication method for Online entertainment store 1 scams were email and text message.

**High street retailer 1** continued to be the top hook within the retail brands, which is associated with an expansion of email and SMS phishing campaigns claiming to offer free gift cards and shopping vouchers from major UK stores.

The **Utility provider 1** billing campaign identified in July 2016, reappeared for a few days in mid August 2016, which resulted in 73 reports being made to the ASOV tool by members of the public.




[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 for this category within the ASOV reporting tool. Although the best possible effort has been made to identify trends, the presented figures may be understated.

# Section 2: NFIB Phishing Inbox

The findings presented in this section are based on the analysis of **over 30,000 phishing emails** forwarded to the NFIB phishing inbox during the period of 1st to 31st August 2016 by members of the public.[3]

## 2.1 Subject Headings of Phishing Campaigns – Top 15

The adjacent table represents the Top 15 most prevalent message subject lines which appeared in exactly the same format in the phishing emails reported in August 2016.

Similarly to July 2016, the most commonly reported phishing emails with the same subject line purported to originate from **Online entertainment store 1.** The scam emails entitled *'Invoice'*, '*Order receipt'* and *'Your invoice No.18479101'* all contained bogus information about an alleged purchase made through the online facility. The emails prompt the recipients to cancel the purchase not made by them by clicking on the link, which leads to a spoofed webpage of the provider asking to confirm their login and bank card credentials.

The second most prevalent phishing theme referred to **free gift vouchers from UK retailers** such as **High street retailer 1 and 2,** as well as **Airline 1** and **Discount retail warehouse 1**, which have emerged as the new phishing hooks this month.

[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.

| | Message title | Number of emails reported | Phishing campaign theme / Phishing hook |
|---|---|---|---|
| 1 | Invoice | 275 | Online entertainment store 1 purchase receipt scam |
| 2 | Order receipt | 126 | Online entertainment store 1 purchase receipt scam |
| 3 | *** Payment Approved! | 71 | Money transfer provider 1 remittance scam |
| 4 | *** prize offer – Open immediately | 68 | High street retailer 1 prize scam |
| 5 | You have qualified | 67 | Online market place 1 competition scam |
| 6 | Your ***.co.uk Account | 64 | Online market place 1 account scam |
| 7 | Your package order # BHX-74647-UK dispatched | 64 | High street retailer 2 gift scam |
| 8 | Thank you. Your order confirmation has been released | 59 | High street retailer 2 gift scam |
| 9 | Your Invoice No.18479101 | 57 | Online entertainment store 1 purchase receipt scam |
| 10 | Where to next? Enjoy this 2500GBP to get you there! | 56 | Airline 1 voucher scam |
| 11 | FROM THE *** | 54 | Fund beneficiary scam |
| 12 | Wishing you a wonderful trip with this 2500GBP voucher | 54 | Airline 1 voucher scam |
| 13 | Your gift card has been issued | 54 | Discount retail warehouse 1 gift card scam |
| 14 | Validate your gift card | 52 | Discount retail warehouse 1 gift card scam |
| 15 | Thank you for your recent visit! Claim your rewards | 49 | Supermarket 2 prize scam |

## 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 August 2016 phishing campaigns, where the most commonly seen spoofed email addresses appeared to be from **Online entertainment store 1**.

The phishing scam originating from a spoofed email address ***@otherserver.com, which purported to contain a utility bill from **Utility provider 1**, maintained its presence in August 2016, although the reporting number fell to 32 from 86 reports received in July 2016. It is believed that the hyperlinks contained within these emails led the victims to downloading malicious files which infected their devices with a ransomware malware.

The most commonly reported phishing campaign originated from careers@***.com email address. The scam, with the total of 114 reports submitted to the NFIB phishing inbox, related to the **bogus offers of employment contract.**

| | Email address | Number of emails reported | Phishing campaign theme / Phishing hook |
|---|---|---|---|
| 1 | careers@***.com | 114 | Employment offer scam |
| 2 | ***.***@***.gov | 69 | Fund beneficiary scam |
| 3 | info@***online.co.uk | 62 | Online entertainment store 1 purchase scam |
| 4 | ***mtaccess44@aol.com | 48 | Money transfer provider 1 remittance scam |
| 5 | ***.***@***.net | 48 | Employment offer scam |
| 6 | suppcenter@archdesign.***.edu | 45 | Online entertainment store 1 purchase scam |
| 7 | customapp@atc.***.edu | 40 | Online entertainment store 1 purchase scam |
| 8 | service@***onlineservices.co.uk | 40 | Online payments service provider 1 online account scam |
| 9 | yourbill@***.co.uk | 39 | Phone and broadband provider 2 online account scam |
| 10 | info@***groups.com | 38 | Internet related service provider 1 competition scam |
| 11 | Generation***@email.***.com | 35 | Bank 2 online account scam |
| 12 | in857@myaccess.***.com | 35 | Online entertainment store 1 purchase scam |
| 13 | swilliams@natomas.***.ca.us | 35 | Donation beneficiary scam |
| 14 | account-update@s19395345.onlinehome-server.info | 34 | Online market place 1 account scam |
| 15 | ***@otherserver.com | 32 | Utility provider 1 bill scam |

## 2.3 Phishing URLs – Top 15

The adjacent 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 during August 2016.

Four of the most persistent URLs identified in the Top 15 set appeared in the phishing campaigns impersonating **Online entertainment store 1**, with the total number of 143 reports received from different members of the public.

The second most prolific URLs were found in **Bank 2** scams, with three phishing hyperlinks utilised across 90 reported emails.

At least half of the URLs presented in the Top 15 data set belong to legitimate domains, which may have been compromised to host a malicious content.

| | Phishing URL | Number of emails reported | Phishing campaign theme/ Phishing hook |
|---|---|---|---|
| 1 | h*tp://rebrp.com/news_feed/ | 44 | Online entertainment store 1 purchase scam |
| 2 | h*tp://bit.ly/2bOaO2F | 38 | Bank 2 online account scam |
| 3 | h*tp://www.sgjl.gzport.com/asp/index.htm | 37 | Online entertainment store 1 purchase scam |
| 4 | h*tp://sll-srv03.com//en/ | 36 | Online entertainment store 1 purchase scam |
| 5 | h*tp://bit.ly/2b33Tiy | 30 | Bank 2 online account scam |
| 6 | h*tp://sva.co.at/payments@***.co.uk.zip | 29 | Phone and broadband provider 2 online account scam |
| 7 | h*tp://www.nissanzseatcovers.com/asp | 26 | Online entertainment store 1 purchase scam |
| 8 | h*tp://skinpush.com/?Im9mZj03NTci | 23 | High street retailer 1 gift card scam |
| 9 | h*tp://www.qgtfw.com/l | 23 | Online payments service provider 1 online account scam |
| 10 | h*tp://usebasica.com.br/mbn | 23 | Bank 1 online account scam |
| 11 | h*tp://bjjgwy.com/2015217 | 22 | Online payments service provider 1 online account scam |
| 12 | h*tp://bit.ly/2bdh9Ta | 22 | Bank 2 online account scam |
| 13 | h*tp://www.charrua.agr.br/naw.htm | 19 | Credit card provider 1 online account scam |
| 14 | h*tp://ankamedya.com/***.co.uk/index.php | 19 | Phone and broadband provider 2 online account scam |
| 15 | h*tp://www.hnfdf.org/l | 18 | Online market place 1 account scam |