NFIB Special Operations
Cyber Monthly Threat Update – April 2024

Welcome to the new Cyber Monthly Threat Update for the City of London Police. This document provides an overview of cybercrime trends using Action Fraud data for the period 1st – 30th April 2024.

Contact: If anyone has any information they wish to put forward to be considered for this document, please contact the Cyber Intelligence Team on: NFIB Cyber Intel NFIB-CyberIntel@cityoflondon.police.uk

Overall Reporting	ECRS	Subject Areas

Contents:

A local service with a national role, trusted by our communities to deliver policing with professionalism, integrity and compassion

CITY of LONDON POLICE

Key Findings

- Cyber Crime reporting figures have decreased only slightly in April by 0.5%. A decrease is therefore not surprising as last April also had a more substantial decrease of 15%.

- NFIB52C (Hacking – Social Media and Email), continues to be the most prolific fraud type, accounting for 62% of cyber reporting. This is followed by NFIB52B (Hacking – Personal) – 25%, consistent with the previous 4 months.

- Social Media Hacking (SMH) reported to Action Fraud has marginally decreased in April compared to March, decreasing by 2.9% to 1,141 reports. Over the last 14 months, SMH reporting is starting to stabilise, with the trendline increasingly level month-to-month. SMH reporting accounted for 42.3% of overall cybercrime reporting in April 2024, a very minor decrease from 43.4% in March. SMH therefore remains the most highly reported single cybercrime type within Action Fraud reporting.

- In the first four months of 2024, there have been 68 reports of social media hacking within which the victim has also had online delivery accounts compromised. This most frequently occurs as a result of a compromise of the victim's email address, leading to all accounts linked to this being taken over.

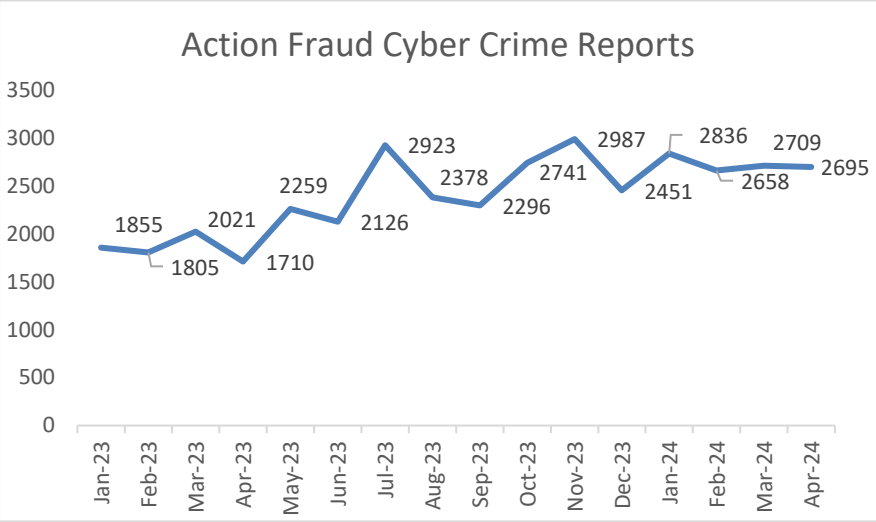
- Action Fraud have published an alert on the WhatsApp OTP vishing attacks following analysis by the Cyber Intelligence team over the last four months. This attack type continues to remain the single most prevalent attack type within all SMH reporting.

- A slight decrease in reports from organisations were made in April. Hacking and Business Email Compromise of (BEC) were the most reported incidents in April. Ransomware was the third most reported incident, consistent with the previous three months.

- 40 ransomware reports were identified in April 2024, this is a 37% increase compared to March's Action Fraud reported data. One new variant, "HsHarada/Rapture" was identified in April 2024 but first seemed to have appeared in March 2023, however not much is known about this variant or its operational history and characteristics.

- In April, two Phishy Friday alerts were published. The first was a campaign which asked recipients to participate in a loyalty programme to claim the newest model of "KitchenAid". The second Phishy Friday alert was regarding a lure which notified recipients that their subscription service had expired and offered them the chance to extend their membership for free as part of a loyalty scheme.

Overall Reporting



64% (1,732) of reports were classified as cyber-dependent, with 10% (279) classified as cyber-enabled.[1]

Compared to March 2024, there has been a small decrease of 0.5% in reporting. NFIB52C (Hacking – Social Media and Email), continues to be the most prolific fraud type, accounting for 62% (1,679) of cyber reporting. This is followed by NFIB52B (Hacking – Personal) – 25% (675 reports). This follows the same pattern as the previous four months and these findings are also consistent with April 2023 with social media hacking accounting for 58% followed by personal hacking at 23%.

Organisations

Organisations made 202 cyber reports to Action Fraud in April 2024, a 2% decrease on the 198 reports made in March 2024.

Hacking was once again the most reported incident in April with 82 reports made by Organisations, making up 41% of cyber reporting. An 11% decrease from March's 92 reports. Business Email Compromise also remained in second place with 42 reports, a 28% decrease from the 58 reported in March. However, Ransomware whilst still holding its position in third, has seen a slight increase in reporting with 36 reported incidents (18%), up from March's 24 (12%). There has also been a notable increase in reports of DDoS attacks on businesses, going from just 3 in March (2%), up to 10 in April (5%). This appears to be consistent with global trends for Q1 2024.*

Social Media Accounts remain the most commonly hacked resource of businesses in April 2024, occurring in 30% of reports, a slight decrease from the 39% in March, followed by hacking of Other Accounts at 23%.

Invoice fraud was again the most common form of BEC reported, decreasing slightly to 69%, from the 71% seen in both February and March.

[1] The other 26% of reports were classified as the following: 12% were classified as 'Other'. 9% were disseminated for victim care purposes. The small remaining number were not yet classified by the time the data was downloaded.

However, the number of Onward Phishing reports has increased by 12%, from 8 reports in March (14%) to 11 reports in April (26%).

Just over half (59%) of reports did not include an attack vector. Where one was identified, the most commonly reported methodology remains as Insider Threat, accounting for only 24%. This is closely followed by Compromised Email (20%). Occurrences of reports identifying Phishing Email as the mode of ingress remain steady, with 6 reports in both March and April's data.

Only 19% of April's reports did not disclose a sector. Of the 81% where a sector was identified, Retail Trade and Human Health & Social Work activities came in joint first, both with 19 reports, each accounting for 12%.

Micro businesses continued to report the most offences in April 2024 (32%), where the organisation definition was identified, a minor decrease from March's 35%, followed by Small Businesses (14%). This is a continuing trend, following the same pattern as previous months.

Subject Areas

Ransomware

- 40 ransomware reports were identified in April 2024, this is a 37% increase compared to March's Action Fraud reported data (29).
- One new variant, "HsHarada/Rapture" was identified in April 2024.
- HsHarada/Rapture first seems to have appeared in March 2023, however not much is known about this variant or its operational history and characteristics.
- In April, LockBit and BlackSuit were the most reported ransomware variants, with 3 reports each.
- 17 out of 40 (42%) reports received in April contained enough information to identify the ransomware variant. Through either victims naming the variant, linked suspect contact details, or linked file extensions.
- No losses continue to be reported by organisations. As mentioned in previous roundups, this is not indicative of the loss picture but rather, shows victims reluctance to share loss figures with law enforcement

Victims:

- 90% (36) of reports were made by organisations. Organisations continue to be the most likely to report themselves as victims of ransomware.
- In April, 'Other Service Activities' was the most targeted sector, with 9 reports.
- Out of the 36 reports from organisations, those with 250 employees or more were the most likely to report a ransomware attack making up 36% of reporting with 13 reports

Phishing

In April there were 737,847 emails reported into the Suspicious Email Reporting Service (SERS), a 1% reduction since March. This continues the trend seen in 2024 of reports of phishing emails decreasing month on month. As mentioned in the previous CMTU, this could be a continuation of the effects of the changes in DMARC practices (see CMTU March 2024).

Alerts:

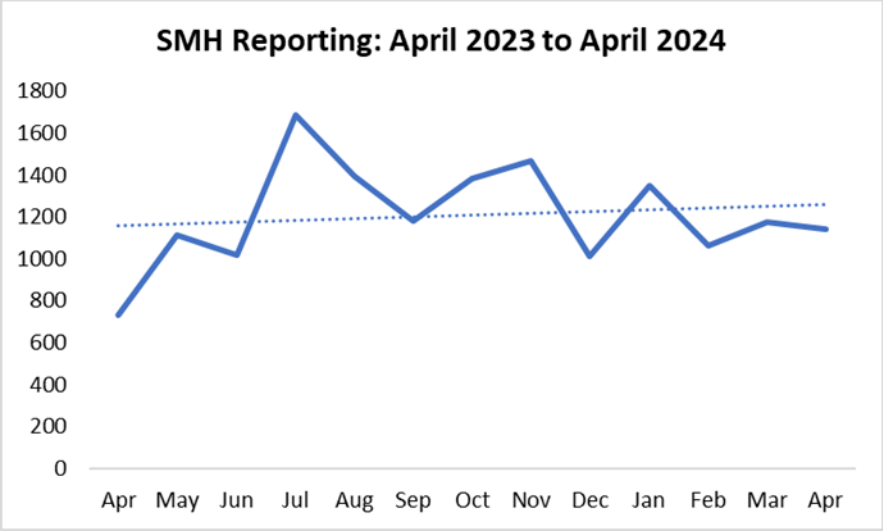
In April, two Phishy Friday alerts were published. The first was a campaign which asked recipients to participate in a loyalty programme to claim the newest model of "KitchenAid". The second Phishy Friday alert was regarding a lure which notified recipients that their subscription service had expired and offered them the chance to extend their membership for free as part of a loyalty scheme. The emails all included the same "90 Days" wording for various subscription services, such as Netflix, Hulu, Peacock and Amazon Prime.

Emerging Trends:

This month saw an increase in emails purporting to be from the DVLA, whereby recipients were asked to update their profile and input "valid and official information" to avoid termination of their motoring licence. There were 1,468 emails reported which used this MO between 1 April 2024 and 30 April 2024 and will continue to be monitored.

There was also an increase in Keto related emails in April. 757 emails were detected which promoted the Keto diet compared to 405 in March. These included the offer of gummies, challenges to see if recipients could "commit to Keto" for 28 days, and discounts or special offers. With the lead up to summer, it is assessed that weight loss phishing emails will increase, and fraudsters may try to lure potential victims in with easier methods of losing weight.

Hacking: Social Media and Email



Statistical overview:

Social Media Hacking (SMH) reported to Action Fraud has marginally decreased in April compared to March, decreasing by 2.9% to 1,141 reports. Over the last 14 months, SMH reporting is starting to stabilise, with the trendline increasingly level month-to-month.

SMH reporting accounted for 42.3% of overall cybercrime reporting in April 2024, a very minor decrease from 43.4% in March. SMH therefore remains the most highly reported single cybercrime type within Action Fraud reporting.

Spotlight – Delivery account takeovers:

In the first four months of 2024, there have been 68 reports of social media hacking within which the victim has also had online delivery accounts compromised. This most frequently occurs as a result of a compromise of the victim's email address, leading to all accounts linked to this being taken over.

Notably, once the suspect has taken control of the delivery account, they are frequently attempting to use the victim's saved financial details to purchase items, such as food deliveries or clothing, to an address.

Not all reports specify the location of this address, however it is evident that a portion of these deliveries are to UK addresses. Whether this UK address corresponds to a UK suspect involved in the account takeover is unknown based on the limited information contained in the initial report.

Ongoing trends:

Action Fraud have published an alert on the WhatsApp OTP vishing attacks following analysis by the Cyber Intelligence team over the last four months. This attack type continues to remain the single most prevalent attack type within all SMH reporting.

Reporting of ticket fraud following account takeovers continues to remain a significant issue for the UK public, attracting substantial media interest at the start of May[2]. Notably, offenders have started to utilise different scams after hacking a Meta account: ticket fraud on Facebook; cryptocurrency investment fraud on Instagram.

[2] Taylor Swift Eras tour: 'Facebook did nothing about ticket scam' - BBC News

Distribution List

Organisation	Department / Role	Name
PUBLIC		

Protective Marking	Official – Public
FOIA Exemption	No
Suitable for Publication Scheme	No
Version	Final
	Cyber Intelligence Team
Purpose	Provide an overview of key themes affecting individuals and enterprise. The information contained within this report has been based upon content within Action Fraud reports and open source which have not been verified as true and accurate accounts.
Owner	CoLP
Author	Cyber Intelligence Team
Reviewed By	Cyber Intelligence Team

CITY OF LONDON POLICE