NFIB Special Operations
Cyber Monthly Threat Update – March 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 – 31st March 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

Contents:

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

Key Findings

- Cyber Crime reporting figures have increased in March by 2%. An increase is not surprising as last March also had an increase of 12%.

- NFIB52C (Hacking – Social Media and Email), continues to be the most prolific fraud type, accounting for 66% of cyber reporting. This is followed by NFIB52B (Hacking – Personal) – 21%, consistent with the previous 3 months.

- Social Media Hacking (SMH) reported to Action Fraud has increased by 10% in March 2024 compared to February 2024. Over the last 13 months, SMH reporting is starting to stabilise, with the trendline increasingly level month-to-month. SMH reporting accounted for 43% of overall cybercrime reporting in March 2024, a slight rise from the 40% in February. Notably, this percentage has been decreasing in the first quarter of 2024, while SMH is remaining consistent. This is indicative of an increase in non-SMH cybercrime reporting. Analysis is currently taking place to understand further the impact of non-SMH.

- WhatsApp OTP vishing remains the most prevalent single attack type within SMH reporting, rising in March. Continuing previous trends, the WhatsApp groups being impacted by this MO are primarily group chats for religious groups and work group chats.

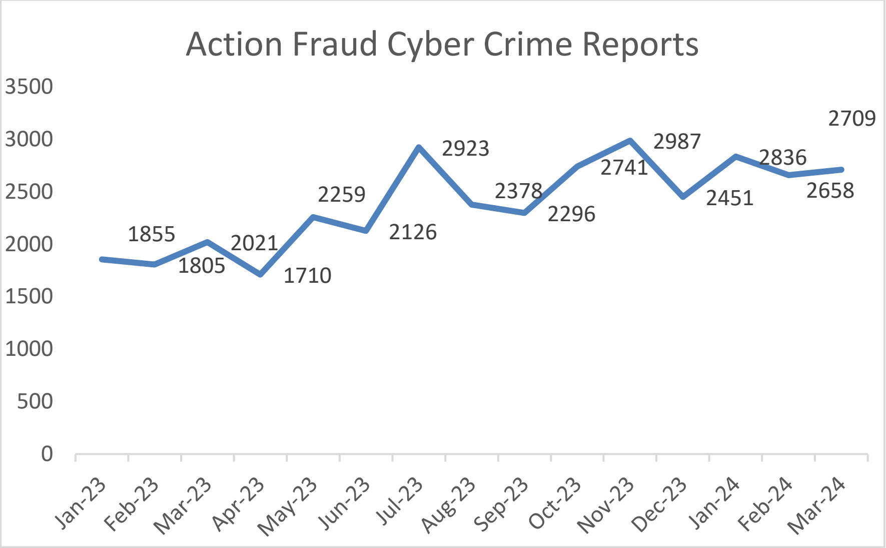
- In March 2024, there has been a 35% rise in reporting of Facebook accounts being compromised and then being used to advertise fraudulent ticket sales. This methodology continues to present a growing risk to UK users, as the ticket fraud itself is highly convincing because of the use of a hacked account.

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

- Four new variants, “BlackSuit”, “Mirror”, “Ebaka” and “Null” were identified in March 2024 Action Fraud reporting.

- In March, two Phishy Friday alerts were published. The first was in relation to recipients being notified that they have won an item from DeWalt and were asked to click a link to complete a survey to claim the items. The second Phishy Friday alert was offering recipients a coffee machine and to follow the link to claim it.

Overall Reporting



61% (1,664) of reports were classified as cyber-dependent, with 14% (370) classified as cyber-enabled.[1]

Compared to February 2024, there has been an increase of 2% in reporting. NFIB52C (Hacking – Social Media and Email), continues to be the most prolific fraud type, accounting for 66% (1,785) of cyber reporting. This is followed by NFIB52B (Hacking – Personal) – 21% (580 reports). This follows the same pattern as the previous three months and these findings are also consistent with March 2023 with social media hacking accounting for 60% followed by personal hacking at 17%.

Organisations

Organisations made 198 cyber reports to Action Fraud in March 2024, a 4% decrease on the 207 reports made in February 2024.

Hacking was the most reported incident in March with 92 reports made by Organisations, 46% of cyber reporting. BEC was second with 58 (29%), followed by Ransomware, with 24 reported incidents (12%). Hacking has risen back to expected levels and BEC has also dropped back down to Dec23 levels reflecting the typical split for these types of incidents.

Social Media accounts were the most commonly hacked resource of businesses in March 2024, occurring in 19% of reports, followed by Email (10%), which has seen an (18%) drop since February.

Invoice fraud was again the most common form of BEC reported, remaining stable at 21% of reports, with no change from February. The number of onward phishing reports has fallen once more to just 4%, down from 13% in February.

The attack vector was reported in fewer than 30% of reports. Where the mode of ingress is identified the most reported methodology for March was Insider Threat, accounting for only 13% of incident reports. Phishing Email and Sharing of OTP came in at joint second both with 10% only and

[1] The other 25% of reports were classified as the following: 9% were classified as 'Other'. 12% were disseminated for victim care purposes. The small remaining number were not yet classified by the time the data was downloaded.

all other categories at less than 9%. Micro businesses continued to report the most offences in March 2024 (35%), a minor decrease from February's 38%, followed by Small Businesses (17%). This is a continuing trend, following the same pattern as previous months.

In March, Other Service Activities and Education reported the most cyber incidents – both accounting for 12% of reports. 11% of reports did not disclose a sector.

Retail/Trade was the highest reported in Feb at 12% with Arts, Entertainment and Recreation and Other Service Activities in joint second with 11% of reports. Education came in at 10% so just a small increase from Feb there. All reports in Feb disclosed a sector.

Subject Areas

Ransomware

- 29 ransomware reports were identified in March 2024, this is a 25% decrease compared to February's Action Fraud reported data (39).
- Four new variants, "BlackSuit", "Mirror", "Ebaka" and "Null" were identified in March 2024.
- Unlike previous months, there has been a significant decrease in Akira attacks, from six reports in January and February to only one report in March, the reason for the fall in Akira attacks is not known.
- In March, LockBit 3.0 was the most reported ransomware variant, with 4 reports.

Victims:

- 83% (24) of reports were made by organisations. Organisations continue to be the most likely to report themselves as victims of ransomware, however – 83% is an unusually low proportion compared to previous months and this will continue to be monitored to identify any potential changes in MO.
- In March, 'Education' was the most targeted sector, with 7 reports.
- Businesses with 50 – 249 employees were the most likely to report a ransomware attack making up 31% of reporting with 9 reports which is a drop from 41% in February.

Phishing

Alerts:

In March, two Phishy Friday alerts were published. The first was in relation to recipients being notified that they have won an item from DeWalt and were asked to click a link to complete a survey to claim the items. The second Phishy Friday alert was offering recipients a coffee machine and to follow the link to claim it.

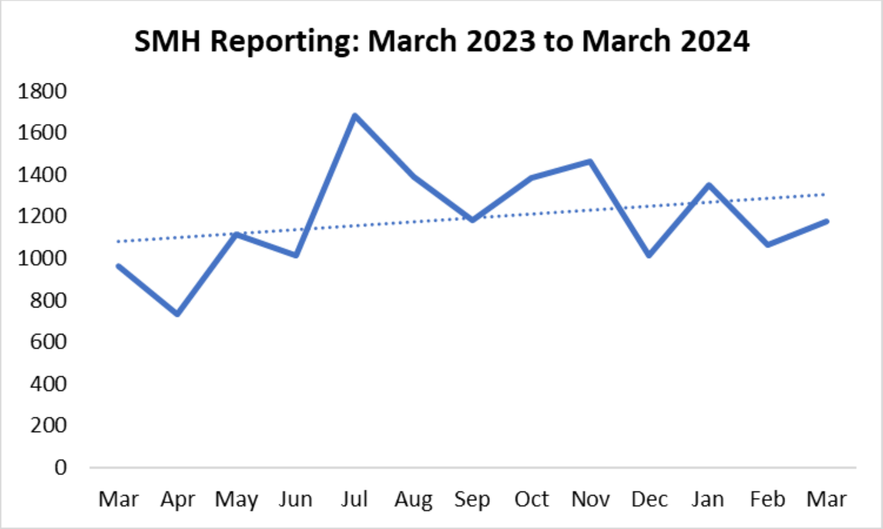
An alert was created in March in relation to the "sad news" emerging trend which was identified in the February CMTU. Recipients were receiving emails, purporting to be from a contact they knew, with the subject "sad news", followed by the sender's name. The email asks recipients to click a link to view an old photo to conjure up memories, and it is thought that clicking on the link may lead to a request for personal details or download malware onto the recipient's device.

Emerging Trends:

There has been a spike this month in emails promoting Ozempic, using language such as “unlock the power of Ozempic” and “lose weight, gain confidence”. With it now being in the lead up to summer, and Ozempic being popular in the mainstream media, individuals may be susceptible to clicking on links if they believe they are getting a good deal to help manage their weight. This MO will continue to be monitored.

There has also been a recent increase in reports surrounding DVLA information requests. The email states that a routine check has found some irregularities in the recipient’s profile, indicating that their information is not up to date. The email notes that recipients much update their profile with their “valid and official information” to avoid termination of their motoring licence.

Hacking: Social Media and Email



Statistical overview:

Social Media Hacking (SMH) reported to Action Fraud has Increased by 10% in March 2024 compared to February 2024.

Over the last 13 months, SMH reporting is starting to stabilise, with the trendline increasingly level month-to-month.

SMH reporting accounted for 43% of overall cybercrime reporting in March 2024, a slight rise from the 40% in February. Notably, this percentage has been decreasing in the first quarter of 2024, while SMH is remaining consistent. This is indicative of an increase in non-SMH cybercrime reporting.

Spotlight – Ticket fraud on Facebook:

In March 2024, there has been a 35.4% rise in reporting of Facebook accounts being compromised and then being used to advertise fraudulent ticket sales. This methodology continues to present a growing risk to UK users, as the ticket fraud itself is highly convincing as a result of the use of a hacked account.

Consistent with earlier trends, the method of takeover is likely to be the use of brute forcing or utilising leaked credentials to target a victim's email address, and from this their social media accounts.

Notably, victims are continually reporting how they have suffered an account takeover up to six months previously, but only now is their account being used for this fraudulent purpose. This is potentially indicative of a threat actor who is purchasing compromised accounts. However, this cannot be confirmed based on this limited intelligence, and there are other reasons for delaying the use of a hacked account.

Ongoing trends:

WhatsApp OTP vishing remains the most prevalent single attack type within SMH reporting, rising substantially from 110 reports in February to 157 reports in March. Continuing on previous trends, the WhatsApp groups being impacted by this MO are primarily group chats for religious groups and work group chats.

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

Copyright © City of London Police 2021 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. Any use of the information or other material contained in this document by you signifies agreement by you to these conditions.