NFIB Specialist Operations
Cyber Monthly Threat Update – January 2023

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 January 2023.

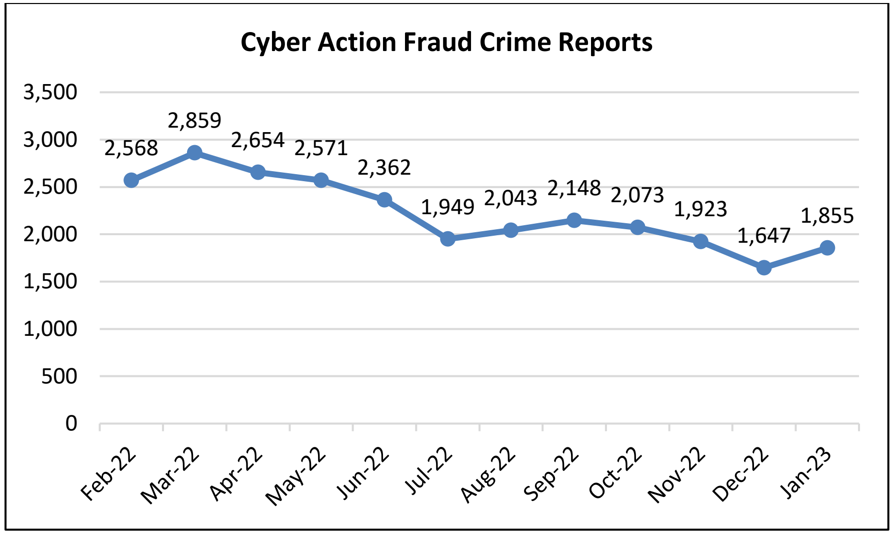
Contact: If anyone has any information they wish to put forward to be considered for this document, please contact the Cyber Intelligence Team on: NFIB Cyber Intel NFIB-CyberIntel@cityoflondon.police.uk

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

Overall Reporting



- The total number of Crime Reports submitted to Action Fraud under the cyber codes were 1,855. This is a 12.6% increase when compared to December 2022, where there were 1,647 reports.
- NFIB52C (Hacking – Social Media and Email), continues to be the most prolific fraud type, accounting for 53.4% (991 reports) of the reporting. This is followed by NFIB52B (Hacking – Personal) with 23.7% (440 reports).
- Cyber dependent reporting accounted for 48.2% (894 reports) of the triaged incidents, while 24% (446 reports) were defined as enabled and 10.1% (188 reports) were disseminated under victim care[1].
- The highest number of reports were in the Metropolitan Police Force area, accounting for 15.5% (287 reports). This is followed by Kent Police with 6.7% (124 reports).

Information Reports:

- In January, a total of 113 Information Reports were submitted to Action Fraud, the majority of which continue to be identified as Computer Viruses/ Malware and Spyware (NFIB50A), with 48 reports.

Enhanced Cyber Reporting Service (ECRS)

- There were 194 cyber-crime reports from organisations in January 2023. This is an 30.2% increase from December 2022.
- Compared to January 2022 (184), there was a 5.4% increase in reporting.
- Reports from SME's made up 62.3% (121) of total reporting, with Micro (Sole Traders & 1-9 employees) businesses accounting for 51.2% (62).
- The top reporting sector was *Public Admin and Defence/ Compulsory Social Security* (41). This sector made up 21.1% of all reports.
- Outside of *Public Admin and Defence/ Compulsory Social Security* and *Other Service Activities*, the *Information and Communication* sector made up the most reports (17). This sector is heavily targeted by threat actors, due to the potential wealth of information they hold as they can often act as an IT third party for other organisations.
- Organisations that reported their sector under *Other Service Activities* were manually assigned a sub-sector. Of these sub-sectors, *Automotive* and *Cleaning Activities* made up 14.2% (4) of the reports each.

[1] The other 2.6% and 15% are classified as 'Pending' and 'Other' respectively.

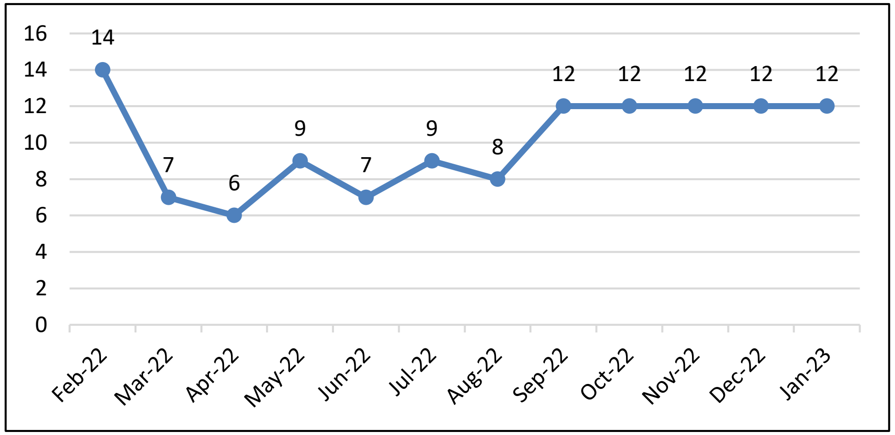
- 40.7% (79) of reports were related to Business Email Compromise, making it the most reported cybercrime. These incidents were broken down further to identify what type of BEC was committed. Of these, 41.8% (33) were identified as Invoice Fraud.
- Attack vectors were only identified in 4.6% (9) of submissions, with phishing emails accounting 88.8% (8).
- ECRS was specifically mentioned in 18.5% (36) reports. This is an 89.4% increase from December 2022.

Primary Incident	No. of Reports	%
Business Email Compromise	79	40.7%
Hacking	37	19.1%
Other	27	13.9%
Ransomware	19	9.8%
Insider Threat	10	5.2%
DDoS	5	2.6%
Malware	4	2.1%
Hacking Extortion	4	2.1%
Data Breach	3	1.5%
Extortion - Data Breach	3	1.5%
Phone Hacking	3	1.5%
Total	**194**	

Spotlight – Business Email Compromise:

- In January 2023, there were 79 reports of Business Email Compromise. This is a 75.5% increase when compared to December 2022 (45 reports). This is largely due to an influx of reports from the National Crime Agency.
- Of those reports, 41.8% (33) specifically reported Invoice Fraud as the form of BEC used.
- The second most reported type Email Account Compromise, which made up 34.2% (27) of BEC reporting.
- The *Construction* sector was the most targeted with 12 reports. This sector made up 15.1% of all reporting.
- Most reports were submitted by Micro businesses (Sole traders and organisations with 1-9 employees) making up 37.9% (30).
- SMEs made up 73.4% (58) of reporting.
- Of those reports which identified the attack vector used by the offender, 100% (3) stated that a phishing email was used to enact the offence.

Live Cyber Reporting



- 11 of the 12 incidents reported into the Live cyber service were disseminated out to a force in January.
- Reporting into the Live Cyber service has remained steady for the past

five months.

- Of these, NFIB50A was the most reported fraud type, accounting for 7 reports.
- Of interest within the 6 ransomware incidents reported an organisation's onsite backups were deleted, with all remaining data encrypted. This really emphasises the importance of businesses storing their backups on an external servers.
- Organisations identified as a 'business' sector, were the most highly reported from, with 4 reports identified.

Subject Areas

Ransomware

- 20 ransomware reports were identified in January 2023, which is a 41.1% decrease compared to December 2022, which stood at 34. Only 9 reports had enough information to identify the variant responsible for the attacks.
- This large decrease could be attributed to ransomware gangs going through a 'winding-down' and reconnaissance phase. December saw an increase in reporting due to the Christmas period and the increased effect that downtime on an organisation would have. Whilst operational downtime will have devastating effects throughout the year, it is more so during the holiday season when even one day out of operation can have huge financial effects. January is likely to be a period where ransomware gangs are looking ahead to the next target (this is especially true for big game hunters), and ways in which they can maximise the effect of an attack to ensure a ransom is paid.
- 1 new variant was identified, named Mario.
- Outside of *Other Service Activities*, both the *Information and Communication* sector and the *Manufacturing* sector were the most likely to report a ransomware attack with 3 reports each.
- Businesses with 50 – 249 employees were most highly reported from, making up 30% (6) of reporting.
- 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.
- Both 'Royal' and 'Lockbit 3.0' were also highly reported from ransomware variants with 3 reports (15%) each, making up 30% of the total reports made to Action Fraud in January 2023.

Variant	No. of Reports
Royal	3
Lockbit 3.0	3
Mario*	1
Avos Locker	1
Play	1
Total	**9**

Phishing

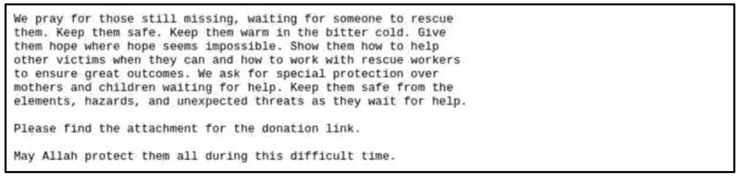
Overall SERs Figures - January 2023:

- Between 00:00:00 on 01/01/2023 to 23:59:59 on 31/01/2023, 624,136 emails were reported on the SERs platform.
- 15.8% were deemed to be malicious.
- 2.6% were deemed to be suspicious.
- The most frequently reported known email address was reported 2,618 times. 98% of emails from this address were deemed malicious

and all 2,618 emails were sent in the last eight days of the month. There were a range of MOs sent from this email address, including an "IPS" delivery scheme, prize give-aways and horoscope readings. All of them encourage you to click a link contained within the email, although it is unclear for what purpose.

Turkey/ Syria Earthquake:

- The Cyber Intelligence Team is monitoring the impact of the Syria/ Turkey earthquake, and how it can be exploited by threat actors in a variety of ways.
- Between 06/02/2023 – 14/02/2023, there have been 7 reported emails referencing the earthquake.
    - 4 request assistance via a donation link within the email body.
    - 1 requests donations straight into a bank account.
    - 2 state that the donation link is attached on the email.



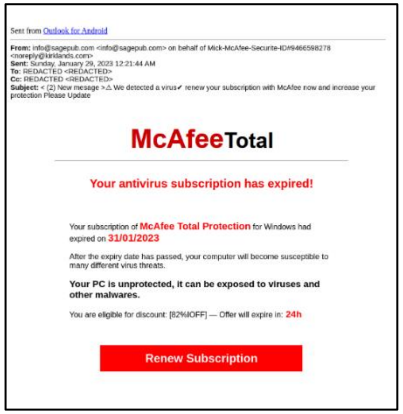
```
We pray for those still missing, waiting for someone to rescue
them. Keep them safe. Keep them warm in the bitter cold. Give
them hope where hope seems impossible. Show them how to help
other victims when they can and how to work with rescue workers
to ensure great outcomes. We ask for special protection over
mothers and children waiting for help. Keep them safe from the
elements, hazards, and unexpected threats as they wait for help.

Please find the attachment for the donation link.

May Allah protect them all during this difficult time.
```

Figure 1: Example Email Using Turkey/ Syria Earthquake Lure.

Phishy Friday Alerts:

McAfee - 16th January 2023 and 30th January 2023:

- The Suspicious Email Reporting Service has received over 2,200 reports pertaining to be from McAfee. There is more than one specific email being used but nearly all of them warn recipients of expired, or expiring, antivirus software and vulnerabilities to their PC that can be exploited.
- The Suspicious Email Reporting Service (SERS) has deemed nearly 45% (956) to be malicious, with the vast majority of those within the past week. Since the 25th January there have been 1,245 (57%) emails reported, 774 (62%) of which SERS has deemed malicious.
- Two examples of the emails seen are:
    - The email subject warns that the recipient's McAfee account will be deleted today, with devices left unprotected. The body of the email offers an "Introductory offer" that is "Including VPN!" and can "Protect yourself and your family from the latest malware, viruses, ransomware and spyware threats". There is a link to "Get it here now".
    - The email subject simultaneously alerts the recipient that a virus has been detected and renew the subscription. The body of the email warns that the "antivirus subscription has expired", although the date of expiry is often in the future. The account holder is offered a renewal at a significantly reduced rate and a link to "Renew Subscription" is provided.



Sent from Outlook for Android

From: info@sagepub.com <info@sagepub.com> on behalf of Mick-McAfee-Securite-ID#9466598278 <noreply@kirklands.com>
Sent: Sunday, January 29, 2023 12:21:44 AM
To: REDACTED <REDACTED>
Cc: REDACTED <REDACTED>
Subject: < (2) New mesage >⚠ We detected a virus✔ renew your subscription with McAfee now and increase your protection Please Update

McAfeeTotal

Your antivirus subscription has expired!

Your subscription of McAfee Total Protection for Windows had expired on 31/01/2023

After the expiry date has passed, your computer will become susceptible to many different virus threats.

Your PC is unprotected, it can be exposed to viruses and other malwares.

You are eligible for discount: [82%IOFF] — Offer will expire in: 24h

Figure 2: Example McAfee Phishing Email.

Health Supplements - 26th December 2022 and Monday 9th January 2023:

- An estimated 315 reports were made to SERS in the stated period, seeking to tempt members of the public into follow links within the email. This type of lure has historically been used to harvest credentials and obtain payment details.
- There are several different emails, all encouraging recipients to click on a link to either read up on an easy way to lose weight or buy allegedly highly effective dietary or health supplements.
- Many offered unrealistic weight loss targets or espoused the urgent need to order products immediately, these are hooks often used in fraudulent schemes to lure in victims. Similar fraud schemes in the past have seen victims receive products that do not assist weight loss, no products at all or even items that could be hazardous to some people's health
- This MO has been reported previously so we know that it is a common scam that people fall victim to.

Hacking: Social Media and Email

Overall:

Overall reports of social media hacking (SMH) have marginally increased in January compared with December, rising by 3.7% to a total of 567 reports. This however remains substantially lower than the 689 reports from November.

Suspect Takeover Motive:

- The proportion of reports in which the motive for the takeover could not be identified in the text has remained consistent, with 26.6% of reporting having no identifiable motive.
- For the first time in the 8 months that this review has been ongoing, the primary motive for SMH has not been to promote a fraudulent investment, but instead to impersonate the victim of the takeover to claim an emergency and demand money from a victim's friends and followers. This should not however be taken as indication of a substantial change of method, as suspects will always exploit a victim's account for any possible financial opportunity. This means that frequently they will aim to commit both various forms of fraud as well as extort the original owner of the account and, depending on the privileges (such as unlimited access to a victim's camera roll on their phone) and content on the victim's account (private messages sent to a partner), potentially 'sextort' the victim as well.

Suspected Attack Vectors:

- In 59% of January reports there was insufficient detail within the report text to ascertain how the victim lost access to their account(s). This is a slight increase from 50% in December.
- The methods used within SMH have not significantly changed in January other than the increase previously identified in vishing attacks using WhatsApp.
- One hook that has continuously been used in SMH has been reported slightly more than usual in January. This hook advertises a simple riddle or puzzle on posts on either of Meta's main platforms. A financial reward is promised as a reward for solving the riddle. However, once the users respond to this riddle the suspect will attempt will, as part of claiming this 'prize' engineer the victim into sharing or changing critical account details. This MO, reported 7 times in January, is almost always used as the first compromise within what goes onto to be a chain hack compromise; the victim's compromised account is used by the suspect to take over the accounts of a victim's friends and followers. Alongside enabling a chain hack, this MO will also attempt to defraud a victim via

tricking a victim into transferring money in order to 'claim' a larger financial reward.

Spotlight – Businesses and Social Media Hacking:

- Businesses continue to account for a minority of overall SMH reporting (7.1% in January) which is consistent with overall under-reporting from business victims. This amounts to only 40 total reports regarding business accounts.
- For the first time since this review was initiated in June 2022, the primary motive of takeovers of business accounts has not been the indecent images (IIOC) MO. Instead, a novel form of extortion specifically targeting businesses has started to be reported.
- This MO targets businesses with a spear-phishing email advising them of a need to verify their social media accounts via following a link to log-in. This itself is not new, as this is a common method used in IIOC takeovers. There are other similarities with the IIOC MO, as victims have reported their accounts being deactivated, however no actual indecent imagery has been reported.
- Instead, victims have reported receiving an extortion demand via a WhatsApp message very soon after losing control of their account. Out of the limited reports of this MO (5), none have paid a ransom.
- Alongside this form of business-specific extortion, there have been two instances in which individuals have been victims of an IIOC takeover and have in fact received a ransom message specifically mentioning the content posted onto their accounts and threatening to post more if money is not received, or to remove the content already posted. This is a change in the MO, and potentially an attempt to better monetise this takeover considering the relatively low (16%) success rate that suspects have had posting advertisements onto accounts compromised using the IIOC takeover method.
- Businesses must be sure to ensure they pay close attention to emails purporting to be from social media providers and must also ensure their own email provider is able to identify emails sent from spoofed domains.

Spotlight – WhatsApp Vishing:

- In December 2022, and now also in January 2023, a resurgent method of WhatsApp account takeover has been reported in increasing numbers to Action Fraud. This method of SMH is almost unique from all others as it uses a vishing WhatsApp call, not a smishing/phishing attempt which were previously more prevalent. Reporting has increased in January compared to December, rising from 5 to 12 reports to Action Fraud.
- The victims of these takeovers will receive a phone call from someone claiming to represent an organisation the victim is part of. Initially, these organisations were all Christian religious communities with WhatsApp groups. However, in January this has expanded to target other (non-religious) community groups with WhatsApp groups. The suspect will explain that they will send a text to the victim which is needed to access some form of content that is linked to the group of which the victim is part. However, this code is in fact an authentication code to link the victim's WhatsApp account to a new device. Once shared with the suspects, they will use this to impersonate the victim in messages to other members of this group requesting financial assistance.
- An almost identical (smishing not vishing) method of takeover has previously been identified as specifically targeting WhatsApp users with a family connection to India. This is not the case currently. Limited suspect information suggests that Nigerian phone numbers are sometimes being used to contact victims with the vishing call.

- WhatsApp's two-factor authentication (2FA) option would likely disrupt this method of takeover as the suspects would have to alter their vishing script to target the 2FA key as well as the SMS sent to the victim's phone. They are currently not doing this, so 2FA is highly likely to be effective to prevent this form of takeover.

Vulnerabilities

- There has been a 77.3% increase of reports referred for victim care from December 2022 (106 reports) to January 2023 (188 reports). This could be due to an increase in vulnerability around the Christmas period.
- 68% (128) of reports related to NFIB52B – Hacking Personal.
- 68% (128) of reports were referred as victim care due to the report coming from a repeat victim. Repeat victims can either be individuals who are consistently targeted or, in some cases, those that are suffering from mental health issues and consistently report to Action Fraud.
- Using a range of keywords ("sextortion", "Revenge", "revenge porn", "rape", "abuse", "domestic", "sex", "images", "threat", "hurt", "assault", and "consent"), we were able to identify the most common themes that were likely to come up in a report from a vulnerable victim. "Sex" was the most common keyword mentioned in reports, with it included in 12.7% (24) of reports.
- 86.7% (163) of victims reported through the Action Fraud website. This preference for reporting through the website isn't necessarily unique to vulnerable victims but this method of reporting might be utilised for vulnerable victims due to the nature of the crimes they are reporting.
- 71.2% (134) of victims identified as female, and 25.5% (48) of victims identified as male.
- Victims between the ages of 50 – 59 continue to be the most likely to be referred as victim care with 64.3% (121) of victims reporting themselves as between these ages.

Distribution List

Organisation	Department / Role	Name
PUBLIC		

Handling Instructions

This report may be circulated in accordance with the protective security marking shown below and caveats included within the report. The information contained in this report is supplied by the City of London Police in confidence and may not be shared other than with the agreed readership/handling code without prior reference to the City of London Police. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 2018.

The cover sheets must not be detached from the report to which they refer.

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.