NFIB Special Operations
Cyber Monthly Threat Update – December 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 December 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

CITY of LONDON POLICE

Key Findings

- Cyber Crime reporting figures have significantly decreased in December, falling by 17.9%. This is likely to be due to delayed reporting over the holiday period, as seen in previous reporting trends. In the first week of January 2024, reporting increased by 72.6% compared to the last week of December.

- Whilst reporting for most cybercrime codes fell, there was an increase in NFIB50A reporting. This was largely driven by a spike in HMRC impersonation emails where the recipient was asked to click on a link to input personal and financial information.

- Social media hacking continues to account for almost half of the cybercrime reported to Action Fraud. Reporting in December did decrease. However analysis indicates that it has since dramatically increased in the first week of January.

- Consistent with the decrease in overall cybercrime reports, reporting from organisations decreased by 18%. Incidents of Business Email Compromise (BEC) unsurprisingly decreased likely due to the reduced number of working days in December.

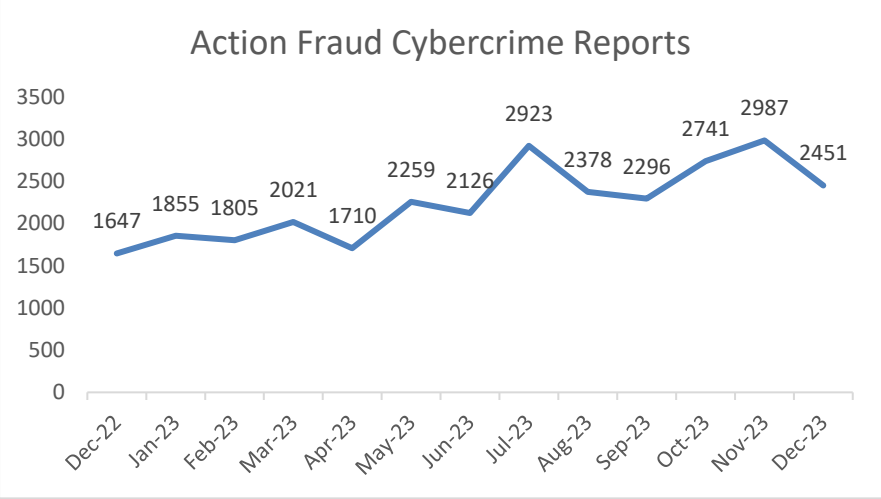
- There was an increase in ransomware reports compared to November's Action Fraud reported data. This was due to significantly lower reporting levels seen in November..

- Black Basta was the most identified strain with three new variants; 'DragonForce', 'Gyza' and 'Mimic' identified in December 2023.

- In December, the Cyber Intelligence team published two alerts. Firstly, a Phishy Friday which was regarding package deliveries, whereby recipients were notified that a package was awaiting delivery and provides a link to track the delivery. The team then also worked alongside the NCA to issue an alert regarding extortion emails purporting to be from the NCA.

- In December, a variation in payment diversion fraud was detected by the NFIB. These emails claim the sender has laryngitis and is therefore only able to communicate through email. This is an attempt to prevent the recipient from contacting the true owner of the email via the phone, which would therefore lead to the fraud being detected.

Overall Reporting



57.3% (1,405) of reports were classified as cyber-dependent, with 21% (537) classified as cyber-enabled.

Compared to November 2023, reporting has decreased by 17.9%. This is in part due to the large decrease in reporting over the Christmas period; 420 reports made for the last week of December, compared to 725 for the first week of January. While a decrease in reporting in December is consistent with previous years, overall reporting in December 2023 remained higher than the previous December. Despite decreases across overall cyber reporting figures there were increases seen in NFIB50A – Computer Viruses, Malware & Spyware. This was due to an increase in HMRC impersonation emails which are discussed later in this document.

Enhanced Cyber Reporting Service (ECRS)

Organisations made 164 cyber reports to Action Fraud in December 2023, a 18% decrease from the 200 reports made in November.

The most reported fraud type by organisations was Hacking, accounting for 31% of reports. This is a change from last month where Business Email Compromise (BEC) was the most common, which now sits as the second most reported this month, with 29% of reporting, followed by Ransomware, 21%. BEC saw a fall in reporting in December, likely due to the decrease in business days over Christmas providing fraudsters with fewer opportunities for this type of fraud.

The most common form of hacking continues to be social media, accounting for 33% of hacking reports, followed by internal systems (22%). Invoice fraud was the most common form of BEC reported, occurring in 85% of reports.

The attack vector was not reported in most instances in December, which is a continuing trend seen in previous months. When it was, insider threat has moved up the list as the most common attack vector (28%). In times of financial hardship insider fraud grows, the ongoing cost of living crisis and the financial pressures around Christmas likely exacerbated the insider threat issue.

Micro businesses continued to report the most offences (54%), followed by Small Businesses (18%). This is a continuing trend, following the same pattern as previous months.

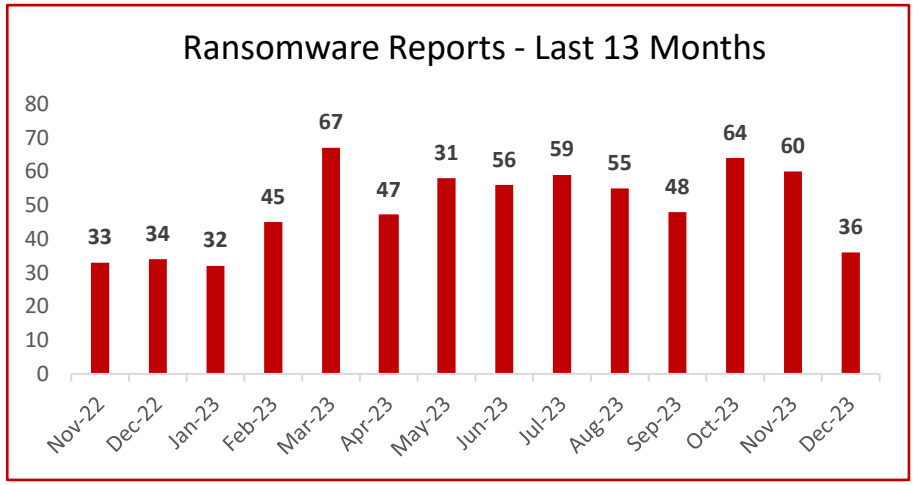
As with last month, Micro, Small and Medium businesses (SMEs) all reported BEC as the most common cyber-crime type, followed by

Hacking. However, for large companies the most reported cyber-crime was Ransomware.

In December, four sectors shared the top spot for most incidents - Education, Manufacturing, Arts, Entertainment and Recreation and Retail and Trade (7%). Last month's highest reporter, Construction, made 5% of reports, as did both Information & Communication and Human Health & Social Work Activity.

Subject Areas

Ransomware



January 2023 to November 2023 has been updated with NCCU statistics to augment our own reporting.

There were 36 ransomware reports identified in December 2023, this 28.6% increase compared to November's Action Fraud reported data (28). Although overall reporting has fallen, ransomware reporting has increased, however this is due to a significantly low number of reports seen in November.

Three new variants 'DragonForce', 'Gyza' and 'Mimic' were identified in December 2023.

In December, Black Basta was the most reported variant, with 4 reports.

20 out of 36 (56%) reports received in December contained enough information to identify the ransomware variant. Through either victim naming the variant, linked suspect contact details, or linked file extensions.

Variant	No. of Reports
Black Basta	4
Akira	2
Lockbit	2
Rhysida	2
INC	2
Black Cat	2
MedusaLocker	1
Phobos	1
Dragonforce	1
Mimic	1
Lockbit 3.0	1
Gyza	1
Total:	20

Victims:

94.4% (34) of reports were made by organisations. Organisations continue to be the most likely to report themselves as victims of ransomware.

In December, 'other service activities' was the most targeted sector, with 7 reports. This differs from last month, where the legal sector was the most targeted sector.

Businesses with 50 – 249 employees were the most likely to report a ransomware attack making up 25% of reporting with 9 reports, closely followed by 250+, 8 reports.

Phishing

In December there were 978,164 emails reported to the Suspicious Email Reporting Service (SERS), an increase of 4.5% from November. The most frequently reported known email address in December used a variety of lures, including package delivery emails, protection from malware and Christmas deals.

In December, two phishing alerts were shared publicly. The first was regarding package deliveries, whereby recipients were notified that a package was awaiting delivery and provides a link to track the delivery.

The second alert that was submitted in December was for an emerging trend regarding NCA impersonation phishing emails, whereby fraudsters were accusing recipients of accessing and viewing indecent images of children or other illegal content and asks recipients to 'justify their

actions' in a response to the email. In addition to the emails reported to SERS, numerous Action Fraud reports were also made. [1]

There was a large spike in emails using the term "HMRC" in December, with 1,460 emails reported, an increase of 201% from November (485 reports). The phishing campaign impersonated HMRC and aimed to encourage the recipients to follow a link to enter sensitive personal and financial information. Several Action Fraud reports have also been made in relation to this scam, which were identified after a significant increase in the NFIB50A cybercrime code was detected. Analysis of NFIB50A reporting indicated that the increase was a consequence of the emergence of this HMRC phishing campaign.

Additionally, as expected and mentioned in the previous CMTU, there was a steady amount of weight loss related phishing lures throughout December, including the promotion of Keto, however there was no significant peak found.

Emerging Trends:

December was the peak month for reports of payment diversion fraud where the suspect claimed to have laryngitis in an attempt to prevent the recipient from contacting the sender by phone. This fraud uses a compromised email account to request payment, usually in the form of a gift card, to be sent to a relative of the sender who allegedly has cancer. A total of 70 reports were identified between 1st July 2023 and 10th January 2024, and December has been the peak month of reporting. It is likely that the initial compromise of the email account is achieved through large scale phishing campaigns impersonating the recipient's email provider.

The Cyber Intelligence team is also monitoring ongoing life insurance phishing scams. There has been a recent increase in reports of individuals being told they qualify for life insurance and offering help to find the best life insurance policies. There have so far been 482 emails reported to SERS in the first two weeks of January, compared to 422 for the whole of December.

Open-source research has indicated that phishing MO's using Facebook accounts which have been taken over has evolved. The latest emergence of this trend uses the lure of displaying a link to a fake BBC news article, with the post caption "I can't believe he's gone. I'll miss him so much" to try and encourage readers to click on the link.[2] There have been no reports identified so far for this MO, so it will continue to be monitored.

Ongoing Trends Update:

Mentioned previously in the November CMTU was the Temu mystery box and pallets scam. An alert for this MO was published[3], however we are continuing to see this MO escalate. In December, there were over 15,000 emails reported for "Temu", indicating that this lure is continuing, and so monitoring will continue for this MO.

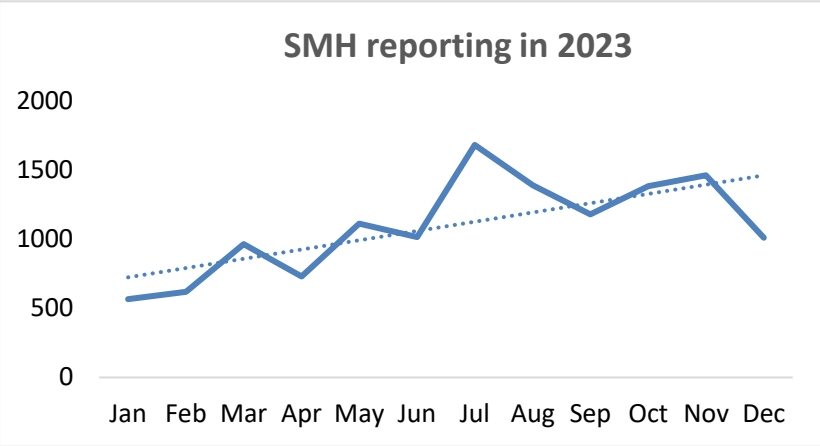
[1] Fraudsters impersonate NCA officers in 'child pornography' scam emails | Action Fraud

[2] Facebook users targeted with "I'll miss him so much" scam | Cybernews

[3] Action Fraud alerts UK public to surge in Temu scam emails | Deeside.com

Hacking: Social Media and Email

Social Media Hacking (SMH) continues to be the most prevalent cyber-dependent crime reported to Action Fraud. However, SMH reporting in December has decreased significantly from November. Falling by 31% to 1,012 total reports.



While a decrease in reporting in December is consistent with seasonal reporting patterns in previous years, the decrease in SMH was exceptionally sharp compared to the 18% fall in overall reporting.

It is almost certain that the decrease in reporting is not representative of a decrease in offending. Rather, the decrease in December is a consequence of delayed reporting during the holiday period. Within the first eight days of 2024, there has been a 47% increase in reporting when compared to the last eight days of 2023.

The most significant motives and methodologies within SMH in December 2023 were not distinct from previous months. accounts are continually compromised for the purpose of ticket or online shopping fraud; to advertise investment frauds; and to commit family and friends' fraud.

However, the WhatsApp vishing MO, the most frequently reported attack type in recent months, did decrease significantly. Decreasing by 60% to only 99 reports in December.

In December's reporting, there were five reports in which the victim was subject to a threat of doxxing, including "swatting".

Notably, there have been a small number of reports in which victims have described receiving positive action from the platform after having their account compromised and used for fraudulent purposes. These reports are still significantly outnumbered by failed takedown requests, including some reports in December of hacked accounts remaining active for months.

Vulnerabilities

Within social media hacking reports received in December, there were 21 reports identified as incidents of Cyber Domestic Abuse, often known as "tech abuse". This represents a notable decrease from November. This is consistent with the overall drop in social media hacking reports.

Consistent with previous trends, victims of domestic abuse and coercive control are especially susceptible to cybercrime because of the offender being an intimate or familial relation to the victim. Offenders exploit this proximity to commit cyber offences, such as through knowing the passwords a victim has used or being in control of a joint account. This is

known as “Abuse-Enabled” cybercrime, and there were 12 reports from December which were committed through these methods.

Within December’s SMH data, there were a small number of reports identified as incidents of cyber VAWG. These are incidents of targeted and gender-based harassment committed through cyber-enabled and cyber-dependent means.

Five incidents of social media hacking were likely linked to incidents of cyber-bullying occurring in schools or between young people.

Three separate reports were incidents of social media hacking in which a victim was also a victim of online child sexual abuse through sextortion.

28 reports of social media hacking led to an incident of sextortion against the victim of the hacking. This includes threats to use artificial intelligence to create synthetic content of the victim.

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

CITY of LONDON POLICE