NFIB Special Operations
Cyber Monthly Threat Update – January 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 January 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 significantly increased in January, rising by 15.7%. This is likely to be due to delayed reporting over the holiday period, as seen in previous reporting trends. As mentioned in the December CMTU, in the first week of January 2024 reporting increased by 72.6% compared to the last week of December. This follows a steady increase in reporting seen since September 2023, when discounting the dip in December 2023 due to underreporting over the holiday period.

- Reporting for NFIB50A, computer viruses, malware and spyware fell this month, decreasing by 30%. It is likely that this is due to a reduction in the HMRC impersonation emails seen in December following the online tax return date passing.

- Social media hacking continues to account for almost half of the cybercrime reported to Action Fraud. Reporting in January significantly increased; however, this is due to increased reporting after the new year.

- WhatsApp OTP phishing attacks continue to rise, with it being the most frequently reported attack type, and fraudsters have increasingly targeted local mosques and Islamic groups.

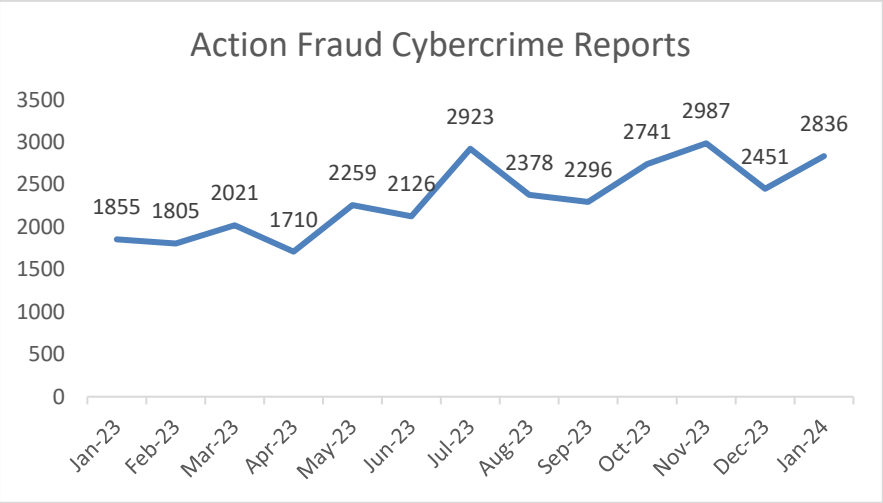
- LockBit was the most identified ransomware variant this month. A new variant was detected called 'Hunters International'.

- In January, two phishing alerts went out from NFIB relating to TV Licences as well as a competition to win a Tupperware set.

- An emerging phishing lure seen in January related to DocuSign phishing attacks, whereby fraudsters utilise a link to a false DocuSign login page and ask recipients to enter personal credentials or infect systems with malware. Searches on the Suspicious Email Reporting Service (SERS) and Action Fraud show that this has been a successful tactic, with high reporting numbers for this particular MO.

- There were increasing numbers seen in several phishing MO's this month, in both Action Fraud and SERS reporting. These include offering Paddock Passes to the Formula One race at Silverstone, an evolving phishing methodology using senior company employee's compromised emails, and life insurance phishing scams.

Overall Reporting



Compared to December 2023, there has been an increase of 15.7% in reporting. This is due to the decrease in reporting over the Christmas period. As predicted, the reporting figures have significantly risen in January. In comparison to January 2023, reporting volumes have increase by 52.8%. This is likely due to the continuing increase of reports of social media hacking.

Enhanced Cyber Reporting Service (ECRS)

Organisations made 168 cyber reports to Action Fraud in January 2024, a minor increase of 2% increase from December 2023.

The most reported fraud type by organisations was Hacking, accounting for 42% of reports, followed by Business Email Compromise (BEC), 33%, and Ransomware, 17%. Both Hacking and BEC saw a relative increase in reporting in January whilst Ransomware decreased, this is likely a knock-on effect of the disruption work by law enforcement against ransomware groups undertaken at the end of 2023, along with high profile group NoEscape apparently ceasing operations.[1]

Social media and email hacking both accounted for 25% of business reports in January 2024, with Internal Systems just behind occurring in 24% of reports.

Invoice fraud was again the most common form of BEC reported, occurring in 68% of reports, although this is a reduction on December's numbers in relative terms when Invoice fraud was responsible for 85% of reports. There were more reports of onward phishing then we normally see (17% of reports) open-source research suggests that one explanation may be that fraudsters are currently low on supply of compromised accounts.

The attack vector was not reported in most instances in January; however, Insider Threat was again the most common reason identified and reported (22%).

[1] LockBit ransomware now poaching BlackCat, NoEscape affiliates (bleepingcomputer.com)

Micro businesses continued to report the most offences (42%), followed by small businesses (23%). This is a continuing trend, following the same pattern as previous months.

In January, Human Health & Social Work Activity reported the most cyber incidents – accounting for 11% of reports. Education, Arts, Entertainment and Recreation and Financial and Insurance Activities were all joint with 10% of reports. This has once again shifted from the main reporting sectors in December, where Human Health & Social Work Activity was joint fifth and Financial and Insurance activities wasn't in the top eight. It is unclear why such fluctuations occur.

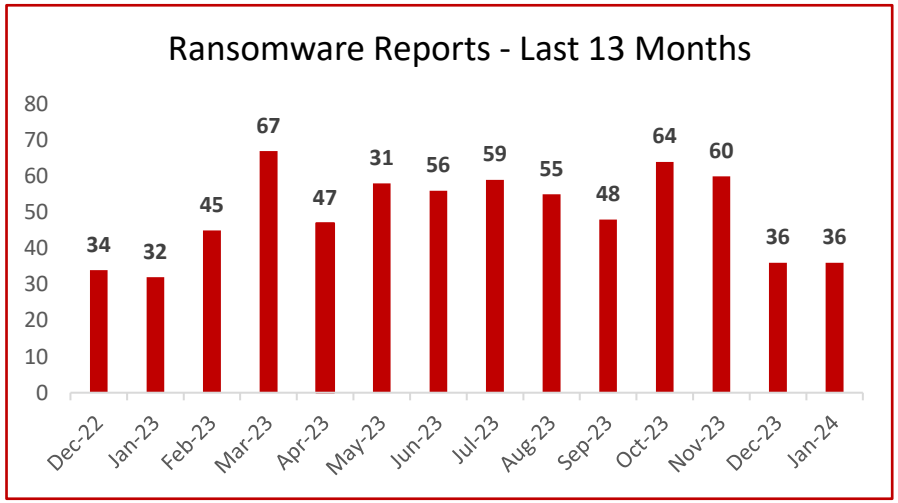
Subject Areas

Ransomware

- 36 Action Fraud reports relating to Ransomware were identified in January 2024, this is the same as December.
- One new variant, 'Hunters International', was identified in January 2024.
- Lockbit was the most frequently reported variant in January.

Victims:

- 86.11% (31) of reports were made by organisations. Organisations continue to be the most likely to report themselves as victims of ransomware.
- In January, 'Financial and Insurance activities' was the most targeted sector in terms of reporting numbers.
- Businesses with 50-249 employees were the most likely to report a ransomware attack to Action Fraud making up 42.3% of organisation reporting with 11 reports and is the same as December 2023.



Phishing

In January there were 1,030,520 emails were reported to the Suspicious Email Reporting Service (SERS), an increase of 5.3% from December. This is the highest monthly reporting figure known to date and follows the trend month on month that more people are reporting suspicious emails to SERS. The most frequently reported known email address in January used a variety of lures, including being selected to complete surveys to win a variety of items such as Stanley tumblers and Le Creuset items, as well as warning recipients that devices have been infected with viruses.

Alerts:

In January, two Phishy Friday alerts were published. The first was regarding TV licences, whereby several lures were used, including but not limited to recipients being asked to either update their details to stay licenced, or set up a pre-authorised debit. The second Phishy Friday published was related to recipients being noted that they have won or could win a "36 Piece Tupperware Set".

Emerging Trends:

There has been an increase in DocuSign phishing attacks seen in January. DocuSign is a platform which allows businesses and individuals to sign documents electronically. Fraudsters are sending out phishing emails with a false DocuSign login page attached. The login page is thought to request personal credentials or infect computer systems with malware[2]. Searches on SERS and Action Fraud reporting indicates that this has been a successful tactic, with over 300 reports on SERS in January, and a small number of Action Fraud reports – some of which were known to lead onto an attempted mandate fraud. This MO will continue to be monitored.

Another MO that was detected this month was an increase in the lure of offering recipients Paddock Club passes to the Silverstone Formula One. In January, 187 of these emails were reported to SERS, and there were several reports to Action Fraud, whereby multiple victims reported substantial losses.

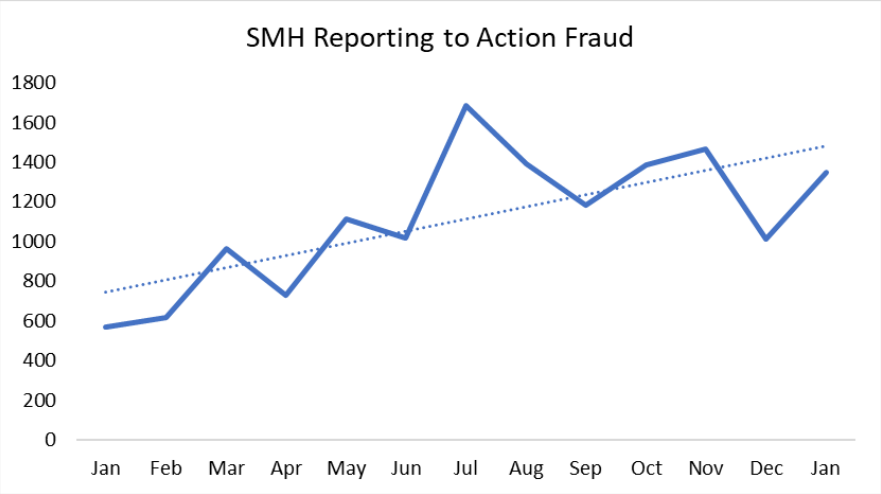
Finally, an evolving phishing methodology has been identified this month. Senior company employees are being targeted with a phishing email from a senior employee of another company. The sender of the email is known to the recipient, and the email address used is legitimate, however it has been compromised to send out the email. The email asks the recipient to follow a link to open a document, and upon clicking the link the recipients are prompted to input email login credentials. Shortly after, the recipient's email is then compromised, and used to send the same phishing email that they received. An escalating number of organisation email addresses have been compromised, and 132 reports using this methodology have been identified since March 2023.

Ongoing Trends:

Life insurance phishing scams are continuing to be on the rise. Between 1st January and 31st January, there were over 1,500 emails reported to SERS which relate to large amount of life insurance coverage, compared to 422 in December. However, reports of this nature are still not being made into Action Fraud.

[2] Lookout for DocuSign Phishing Scams | AmTrust Insurance (amtrustfinancial.com)

Hacking: Social Media and Email



Statistical overview:

Social Media Hacking (SMH) has increased dramatically in January 2024, rising by 33% compared to December, with 1,348 total reports. This figure is artificially high compared to December, as several SMH victims did not report offences that occurred during the holiday period until the start of the new year.

In January, SMH incidents accounted for 47.5% of overall cybercrime reporting to Action Fraud.

Spotlight – SMH leading to ticket fraud:

In January, Action Fraud received reports which indicated that the victim had initially suffered a Facebook account compromise from between six – twelve months ago, but had their account reactivated in January and used to advertise fraudulent tickets.

Using a compromised account to commit ticket fraud is continuing to drive increased demand for compromised accounts. These accounts are compromised via phishing attacks, leaked credentials, and brute forcing.

Of particular concern in January were reports in which a victim of social media hacking was subjected to harassment and threats from individuals who were defrauded by the suspect now in control of the hacked account. There is an ongoing risk to SMH victims, where the suspect shares the victim's address as the location to pick up non-existent tickets.

Ongoing trends:

The single most frequently reported attack type continues to be WhatsApp OTP phishing, with 185 reports in January, a substantial rise from the 99 in December. Notably, WhatsApp groups for local mosques and Islamic pilgrimage groups have started to be increasingly targeted relative to church groups, which were already targeted.

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