NFIB Specialist Operations
Cyber Monthly Threat Update – November 2022

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 November 2022.

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

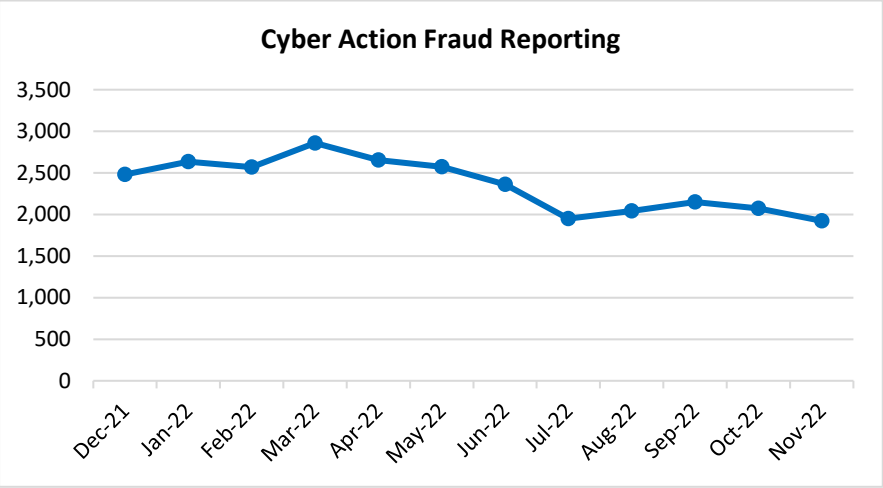
Overall Reporting	ECRS	Situation Updates	Subject Areas	Horizon Scanning

Contents:

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

CITY OF LONDON POLICE

Overall Reporting



- The total number of crime reports submitted to Action Fraud under the cyber codes were 1,923. This is a 7.2% decrease when compared to October 2022, where there were 2,073 reports.
- NFIB52C (Hacking – Social Media and Email), continues to be the most prolific fraud type, accounting for 52.5% of the reporting. This is followed by NFIB52B (Hacking – Personal) with 20.7%.
- Cyber dependent reporting accounted for 55.8% of the triaged incidents, while 21.2% were defined as enabled and 4.1% were disseminated under victim care[1].
- The highest number of reports were in the Metropolitan Police Force area, accounting for 18.6%. This is followed by Greater Manchester Police with 6.8%.

[1] The other 2.8% and 16.2% are classified as 'Pending' and 'Other' respectively.

Information Reports:

- 67 Information reports have been submitted to Action Fraud in October.
- The majority of these (65.7% - 44 reports) were defined as NFIB50A (Computer Viruses/ Malware/ Spyware), followed by NFIB52C (17.9% - 12 reports).

Enhanced Cyber Reporting Service (ECRS)

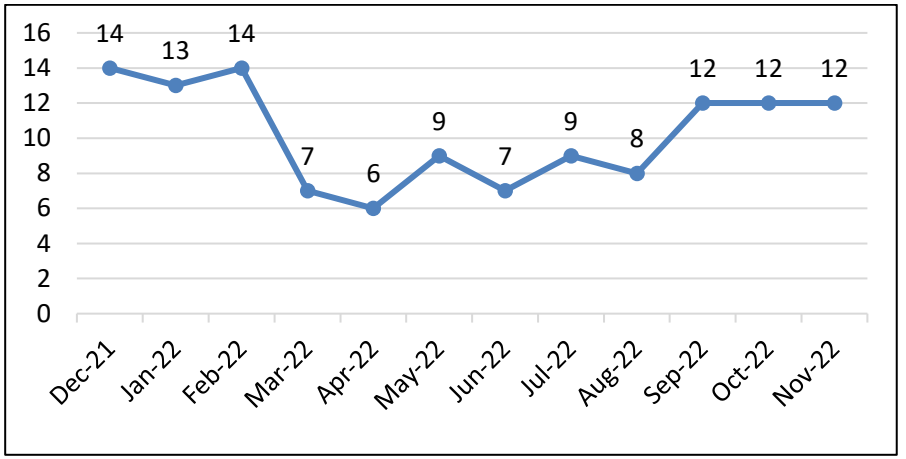
- There were 142 cybercrime reports from organisations in November 2022. This is an 8.3% increase from October 2022.
- Reports from SMEs made up 87.3% (124) of total reporting, with Micro (Sole Traders & 1-9 employees) businesses making up 52.4% (65) of SME reporting.
- The top reporting sector, outside of Other Service Activities, was Retail & Trade (16).
- Organisations that reported their sector under 'Other Service Activities' were manually assigned a sub-sector. Of these sub-sectors, Consultancy made up 31.2% (5) of the reports.
- 35.2% (50) of reports related to Business Email Compromise, making BEC the most commonly reported cybercrime. BEC incidents were broken down further to identify what type of BEC was committed. 44% (22) of these reports were identified as Invoice Fraud.
- In reports where a secondary cybercrime incident was reported, Insider Threats made up 75% (6) of reporting.
- Attack vectors were only identified in 6.3% (9) of reports, with phishing emails reported in 100% (9) of those reports.

Primary Incident	No. of Reports	%
Business Email Compromise	50	35.2%
Hacking	29	20.4%
Other	25	17.6%
Ransomware	25	17.6%
DDoS	4	2.8%
Data Breach	3	2.1%
Hacking Extortion	3	2.1%
Phone Hacking	2	1.4%
Malware	1	0.7%
Total	**142**	

Spotlight – Business Email Compromise:

- In November 2022, there were 50 reports of Business Email Compromise. This is a 35.1% increase on BEC reports from October 2022 (37 reports).
- Of those reports, 44% (22) specifically reported Invoice Fraud as the form of BEC used.
- The second most reported form of BEC was Email Account Compromise, which made up 38% (19) of BEC reporting.
- Outside of Other Service Activities, the Financial and Insurance Activities, Retail and Trade, Education, and Information and Communication sectors were the most targeted with 5 reports each coming from these sectors.
- Micro businesses (Sole traders and organisations with 1-9 employees) made up 42% (21) of reports.
- Of those reports which identified the attack vector used by the offender, 100% (4) stated that a phishing email was used to enact the offence.
- There has also been a marked jump in the number of personal victims reporting a personal account compromise leading to emails being sent to friends requesting financial assistance. In October 2022 there were two such cases but in November this has increased to 11. We will monitor how this MO develops.

Live Cyber Reporting



- All 12 of the reported incidents into the Live cyber service were disseminated out to a force in November.
- Reporting into the Live Cyber service has remained steady for the past three months.
- Of these, NFIB52C and NFIB50A were the most reported fraud types with 3 reported incidents identified each.
- Six ransomware incidents have been reported, although no specific variants have been noted.
- Manufacturing and 'Business' activities are the sectors most reported

from, with 3 reports identified each.

Situation Updates

Situation Updates related to the Cost-of-Living Crisis are disseminated every 2 weeks by the Cyber Team.

11/11 – 25/11 (Most Recent):

- Cost-of-living related Action Fraud reports (including all keywords[2]) have decreased in the past 2 weeks, with a total of 26 reports identified. This is a 40.9% decrease when compared to the 28/10 – 11/11 Situation Update. This decrease could largely be due to the lack of coverage in the media over the last few weeks regarding the cost of gas and electricity, with more attention given to the recent budget that was released.
- In contrast to the previous week, where victims aged 50-59 were the most prolifically targeted by threat actors, those aged between 30-39 were more likely to be targeted, making up 26.9% of reporting.
- NFIB5A (Cheque, Plastic Card and Online Bank Accounts (Not PSP) was the most highly reported fraud and cyber code, accounting for 30.7% of reports.
- 6 reports were specifically identified under the "Energy Rebate" key word search. This is a decrease of 40% when compared to the last report, where 10 incidents were identified.
- Cost-of-living related Action Fraud reports continue to be most likely identified under the keyword "Energy Bill", with 38.4% of those identified containing this keyword specifically.

[2] Key words used include: "Cost-of-Living", "Energy Rebate", "british gas", "e.on", "npower", "edf", "gas bill", "energy bill", and "energy prices".

MOs of Interest:

- Vishing and smishing attacks have become more prevalent as the Christmas shopping period has begun and consumers are increasingly looking for the best deals.
- Offenders continue to call victims impersonating energy companies and offering 'deals' on bills and equipment installation.
- Several victims received a call claiming to be from their phone provider and stating that they could receive a discount on their phone bill due to cost-of-living hardships. They were then asked a series of questions designed to take their personal information.
- Victims have received phone calls and texts claiming to be from the government and different departments, including DWP, and claiming they need to fill in a form for cost-of-living assistance.

Subject Areas

Ransomware

- 33 ransomware reports were identified in November which is an 120% increase compared to October reporting figures. This increase can be attributed to offenders targeting businesses in the run-up to the Christmas period. During this period, the cost and impact of an organisation being out of operation for any amount of time is even greater, therefore increasing the likelihood of an organisation paying a ransom to ensure they can get back online quicker.
- 3 new variants were identified in November 2022. These were Elbie, ZATP, and VENUS.

- In November 2022, outside of *Other Service Activities* (4), *Professional, Scientific and Technical Activities* (3), *Construction, Retail & Trade* (3), *Education* (3), and *Manufacturing* (3) were the most common sectors to report.
- SMEs continued to be the most likely to report a ransomware attack with Micro (1-9 employees) and Small (10-49 employees) making up 42.4% of reporting (7 reports each).
- No losses were reported in November 2022, but one organisation did report their intention to pay a ransom – this amount was not disclosed in the report.
- Outside of unknown, Vice Society, Black Basta, Deadbolt, Elbie, and Lockbit 3.0 were the most commonly reported ransomware variants.
- 48.4% (16) of reports contained enough information to identify the ransomware variant.

Variant	No. of Reports
Vice Society	2
Black Basta	2
Deadbolt	2
Elbie*	2
Lockbit 3.0	2
ZATP*	1
VENUS*	1
Checkmate	1
VVWQ	1
Quantum Locker	1
Royal	1
Total	**16**

Phishing

Weekly phishing alerts disseminated in November 2022:

Energy bill rebate payment scams - updated alert and circulated via social media platforms, which was republished mid-November:

- A total of 392 reports were made into Action Fraud between the reporting period of 1st September and 13th November connected to the energy bills rebate smishing scam. Of these total reports, 299 consisted of crime reports and the remainder, 93 reports, consisted of information reports. Reporting numbers for this specific scam in November dropped significantly compared to September and October.
- Offenders are purporting to be from the UK Government and are sending out SMS text messages telling people that they need to apply for the £400 energy rebate.
- These messages claim the following lines: "GOV.UK: You are eligible for a discounted energy bill under the Energy Bills Support Scheme. You can apply here."
- There is a URL link contained within the SMS text message (https://energybill-rebate.com), which directs users to a fake Energy Bills Support Scheme page, and users are urged to share personal information, i.e. name, date of birth, phone number, address, as well as bank details, which can be used for PII and credential harvesting, and used for follow-up frauds or/and facilitate identity fraud.
- As of 14th November, a total of 37 victims incurred financial losses to this specific smishing scam and MO. Total financial losses of £156,401 have been reported by these victims.
- The highest financial loss reported by a victim was £29,920.

Royal Mail Phishing Scam – An estimated 400 emails identified between Monday 14th November and Monday 28th November 2022:

- Circa 400 reports for the above reporting period were sent to recipients purporting to be from Royal Mail and seeking to tempt members of the public into following links within the email or paying fees to release parcels.
- Most of the emails have come from the same address – royal-mail0@ya.ru which manifests as "*Track&Trace*". The subject line seems to use the known identifier for the potential victim followed by "*You have (1) package waiting confirmation*" and then a reference number. The body of the email relates to "*Track and Trace International Delivery*".
- The email offers the recipient the opportunity to track their order. As this is a mass phishing scheme, the tracking number is the same in every email.
- Other emails invite the recipient to pay a small fee to release a parcel that is due to be delivered. They are more aligned to genuine Royal Mail communications, using appropriate colour schemes and insignias. The standard of English varies from poor to broadly what would be expected, depending on the email.

Black Friday SERs Searches: 18/11/22 – 24/11/2022 –

- In total there was 2,402 reported emails during the above time period.
- The number of malicious reports sits at 869 – which is 36.17% of the total.
- The majority of these phishing emails state that the recipient is a 'Black Friday Winner' or that they have won black Friday deals, gift cards etc.
- The email bodies contain links where the recipient in encouraged to click in order to claim these prizes.

[3] World Cup and Black Friday being exploited by scammers (yahoo.com)

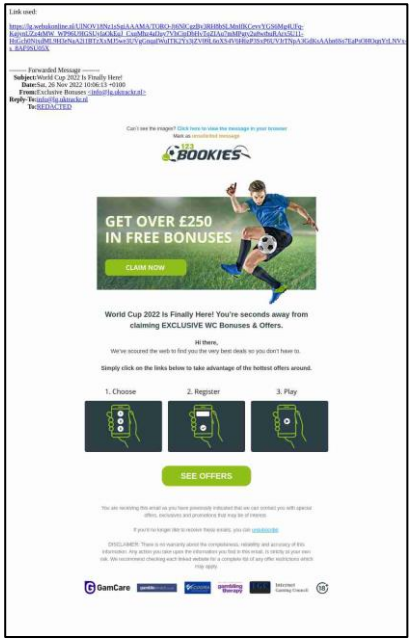
- Example phishing email below:

World Cup Exploited by Scammers[3]:

A sharp rise in ticketing scams was recorded by CIFAS during the start of the World Cup gets under way. CIFAS stated that the scams they are seeing include fake ticket lotteries offering cash prizes, or "hospitality packages" distributed through phishing texts and emails. Clicking on the links included in these emails could lead to the downloading of malware designed to steal personal and financial information.

World Cup-related SERs Searches: 25/11/22 – 27/11/2022 –

- There were 26 reports on SERs, which is a decrease from the previous week's checks which stood at 50. These 26 reported emails had a malicious reporting level of 46.15%, which is an increase from last weeks of 30%.
- Most of the reported emails are non-nefarious and follow no threat pattern or MO, as they tend to be single spam emails. However, there was an email that appeared 9 times.
- This email was sent from the email address: info@lg.uktrackr.nl and is titled "World Cup 2022 Is Finally Here!" and appears to be an offer from a betting site (see below).



Hacking: Social Media and Email

Overall:

689 reports of social media hacking (SMH) have been received by Action Fraud in November. This is a small increase of 8 reports when compared to October.

Suspect Takeover Motive:

- The percentage of reports with no identified motive has continued to decrease, falling from 20% in October to 18.7% of overall reporting. This means our overall dataset is becoming slightly more accurate.
- Within the investment fraud takeover MO, there is a repeated trend where victims are asked to provide a copy of their driving licence in order to verify their identity before they can enter the 'investment'. This enables the suspect to do two things: firstly, attempt the social media providers account recovery process to take over the victim's account; secondly, use the victim's document to prove their identity when using the victim's account to further promote the fraud.

Suspected Attack Vectors:

- 42.8% of overall SMH reporting having no identified method of takeover.
- The methods of takeover remain consistent, with email takeover, phishing, leaked credentials, and chain hacking methods being the most persistently reported.
- A notable change is that the use within chain hacking of the account recovery link hook has decreased. The social media site used by victims in these reports does include on the link a message for this not to be shared, which was cited by one victim as preventing them from screenshotting the link.

CITY of LONDON POLICE

- The number of reports in which malware was likely to be involved in the takeover has doubled in November compared to October. Reports involving this method often relate to sextortion attempts and Cyber domestic abuse (spyware). In two of the sextortion reports, separate victims likely downloaded the same malware from an advertisement seen on the same social media site. One notable report indicates that a victim downloaded a malicious file and lost control of their social media account shortly after. IIOC were then posted on to the account. This is the first instance in which malware has been used in an IIOC takeover.

Spotlight – Organisations and Social Media Hacking (SMH):

- There has been a slight increase (7 more reports) in businesses reporting SMH in November. Business accounts continue to represent a minor fraction of overall reporting – 9.3%.
- IIOC motivated takeovers are the most impactful for businesses. With businesses accounting for 35.5% of victims within this MO. This is almost certain to be the result of businesses being intentionally targeted by suspects as business accounts provide suspects with the best opportunity to monetize the takeover as they intend (paid advertisements).
- This takeover method also has substantial impacts on business due to their customers being involuntarily exposed to child sexual abuse, which can lead to reputational damage. Financially, businesses suffer loss of earnings and advertisement revenue and can lose capacity to contact their clients.
- As with October, business social media accounts are overwhelmingly targeted by taking over a linked email account (48.6% of identified takeover methods), closely followed by spoofed login's sent to the victim in a phishing email (20% of identified methods). The spoofed log-in method is tailored to business accounts, using a claim of copyright breach or need to verify a business account as the hook to target the victim.

Spotlight – Impersonation and Social Media Hacking:

- One of the most useful assets that a suspect acquires after taking over a victim's social media account is the friendship this victim may have with other users on the site. This gives the suspect an audience that trusts in and cares for the social media account that the suspect now controls.
- It is not therefore surprising that the second most frequently reported motive for account takeover within the last six months is to exploit this privilege to commit fraud and additional account takeovers (chain hacking). This is referred to as the 'impersonation' MO as suspects impersonate the victim on the victim's account.
- Initial access to the victim's account is acquired via either compromise of the linked email account, or a chain hack (the suspect is using a hacked account of the victim's friend) that engineers a victim into sharing a One-Time-Passcode (OTP) for their account.
- With access to the account, the suspects will attempt to commit mandate fraud against the contacts of the account as well as to further the chain hack, usually at the same time. The mandate fraud is premised on some form of emergency that the caller has found themselves in.
- This form of takeover varies significantly depending on the platform being used, with WhatsApp takeovers using large group messages for initial access, and Facebook takeovers using private messages.

Vulnerabilities

Cyber Domestic Abuse Profile – Published 02/11/2022:

Key Findings:

- 295 reports were identified as 'Cyber Domestic Abuse' (CDA).
- Where victim gender was known, 78.3% of victims were female.
- Where suspect gender was known, 75.7% of suspects were male.
- In 233 reports (80%), CDA was initiated following a break-up within the relationship between victim and suspect.
- 13.2% (39) of reports indicate that CDA occurred within the context of a legal process involving the victim and the suspect.
- Direct physical control was the means used to commit CDA in 13.2% of reports. This refers to reports where the suspect has been in possession of the victim's devices and used this to commit CDA.
- Only 7.1% of reporting indicates that the suspect was aiming to locate the victim through CDA.
- Social media was the primary avenue for committing CDA, with 34.2% of reports indicating that the suspect has used social media to harass, stalk, or abuse the victim, either through account takeover or abusive posts.
- 85 reports were categorised as a case of 'digital identify theft'. This refers to instances in which the suspect uses knowledge of the victim's personal identifying information (PII), including addresses, emails, and phone numbers, to create online financial, insurance, or Government accounts in the victim's name. This leads victim's to be in significant debt and in some cases be blacklisted for fraud and unable to gain financial independence. Victim's email accounts were targeted in 68 reports. Emails are a particular vulnerability for those victims in legal proceedings with the suspect or having recently fled the suspect. This is due to the sensitive information contained within our email accounts, as well as the addresses likely to be visible on correspondence to the victim.
- Malware was potentially deployed in a small minority of reports (8.1%). It is likely that the true scope of malware based CDA is far more significant than this figure suggests, as the purpose of CDA based spyware is to remain undetected by the victim. Some reporting under this category indicates that the use of spyware had a 'gaslighting' impact on the victim, as the victim feels no one will believe them and questions their own sense of reality.
- Internet of Things (IoT) was explicitly mentioned in only 4 reports.

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