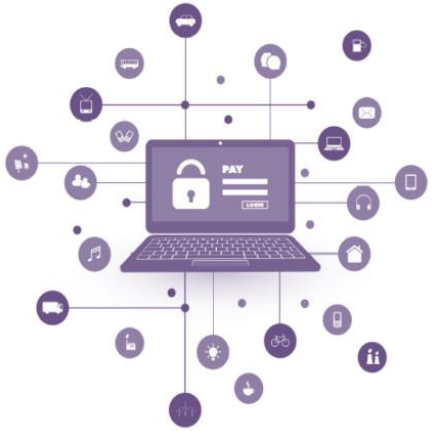
Monthly Threat Update - MTU Public– April 2022

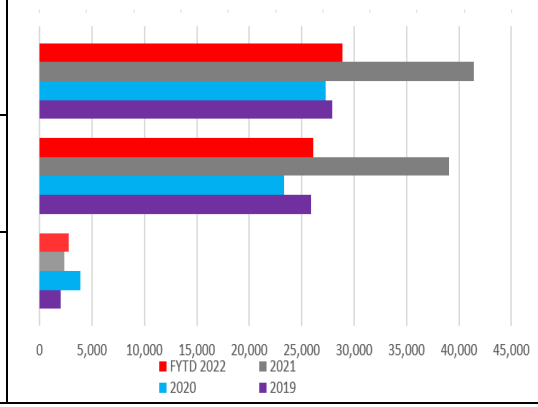
Welcome to the new Monthly Threat Update (MTU) for the City of London Police. This document provides an overview of Fraud and Cyber dependant crime trends using Action Fraud data for the period 1st -30th April 2022.



Contents:

Crime Trends Summary

Action Fraud Crime Reporting Volumes in April 2022		
	Reports	Direction
Total	28,899 -6%	↓
Fraud	26,114 -6%	↓
	2,785 -6%	↑↓



Explanation of Figures: The columns above on the left show the crime reports (excluding information reports) received for April 2022 and the percentage change from the previous month, broken down by all reports, fraud reports and cybercrime reports. The graph on the right-hand side shows the Action Fraud crime reports received for each financial year to date, broken down by all reports, fraud reports and cyber reports.

- Fraud and cybercrime reports to Action Fraud have slightly fallen in April by 6% to 28,899.

- When looking at the financial year to date (April 2022 only) as shown in the graph above, reporting figures overall are significantly below the same period in 2021 for fraud (during covid restrictions), however, the reporting volumes are more than then were during the same period in 2019 and 2020. This pattern is also shown when looking at fraud reporting specifically. When examining cybercrime reporting, the figures show that reporting is higher in the financial year to date compared to 2021 and 2019 but are below the figures for the same period in 2020. These comparisons to previous years will continue to be examined in subsequent MTU's.

- **Both crime and information reports received for fraud**[1] have slightly decreased in February from 41,501 to 43,793. For both crime and information reports, 15 out of 54 fraud types showed an increase in reporting compared to the previous month, whilst 17 out of 54 fraud types showed an increase in reporting compared to the same time last year.

- **Cyber-crime and information reporting** has dropped by 6% after the rise in March and is now 15% higher than 2021 average. Apart from slight increases in Denial-of-Service Attacks and Hacking – Server, all other cyber types show a drop in reporting in April. Hacking – Social Media and Email continues to be remain the most prolific cyber-crime type.

- **After a drop the previous month, Other Advance Fee frauds (crime and information) have risen once more from 2990 reports in March to 3110 in April.** However, figures are still relatively low compared to previous months.

- **Telecoms Industry Fraud (crime and information) has been steadily increasing,** with some slight variants, from a low in April 2020. Reporting is now the highest since February 2019.

[1] Crime reporting relates to reports where there has been a loss, whereas information reports relate to cases where fraud could have occurred but did not.

- **Dating Fraud:** Reporting increased 5% in March. Figures continue to drop from a high in August 2021 and they are now 11% lower than the previous year's average. However, figures are still higher than pre-pandemic.

- **Mandate Fraud:** Crime reporting has risen by 13% from the previous month. It is now 15% lower than the previous year average. Reporting is lower than pre-pandemic.

- **Computer Software Service Fraud:** Crime reporting has increased by 3% from the previous month. Reporting is now 32% below the previous year average. Figures remain low compared to the previous year and pre pandemic.

Current Reporting Trends

April MO's

- Individuals have still been reporting advertisements on social media for tax rebates, clicking on the link and supplying personal and financial information. Some reports claim that the company then obtain tax refunds from HMRC but keep the money for themselves.

- There have been reports of people looking to renew their driving licence online and being directed to a fraudulent website, which asks for personal and financial information. The victims also report being at a financial loss.

- Text messages are still being sent stating that a delivery has been attempted but the recipient was not home. To reschedule a new delivery date the recipient is asked to click on a link which takes them to a website requesting personal and financial information. There have been previous variants of this type of message, including requests for payments of customs fees.

- Scams using the crisis in Ukraine as a hook continue to circulate. Although numbers have been falling, reports into the Suspicious Email Reporting system still show that people are still being targeted by malicious and increasingly sophisticated scams linked to the conflict. These include both charity scams as well as apparent investment opportunities. An alert was sent out from NFIB Cyber in relation to 454 Suspicious Email Reporting Service (SERS) reports linked to the header "The ongoing Ukraine Russia conflict is giving rise to big opportunities for investing in crypto". These emails adopt the same MO as previously observed. Additionally, a new subject header variation is likely to rise in the coming weeks, entitled: "Bitcoin Dips Below $44K, good news for people wanting to invest".

- Victims have reported that they have been contacted through the Telegram app regarding a data management part time job or an investment opportunity. With the job opportunity, the suspect explained that the victim would be paid to submit reviews and would be paid 1% of the value of the product reviewed. The victim was told that they needed to pay for each "mission" and then they would get the commission on the work done. The victim was told that they needed to complete 40 missions, after which they would be able to withdraw all the money spent on missions. In the investment opportunity, the victim was told that they would make an initial deposit and the investment scheme was based on a "mission" system, where money would be put into certain "mission packages" and that this would generate income leading to the victim receiving a 1% commission. Both MOs are scams and the money deposited is never

returned. The scam company appears to be impersonating a genuine global organisation.

So What? New MO's devised by fraudsters in order to trick victims into handing over personal and financial details.

Provenance: SAIP data

Horizon Scanning – Emerging Issues & Threats

Energy Scams

There have been several alerts in the press over the past few weeks that have been issued by various organisations regarding cold callers using the energy crisis to target potential victims. Energy scams has also been raised in previous MTU's as a potential emerging threat and something we could continue to see over the coming months, particularly as we move into the winter period and energy usage increases further.

There have been warnings issued about scammers purporting to be calling or texting from the council requesting bank details to process the £150 council tax rebate. In addition, Which? have issued a warning about the circulation of emails using the regulator Ofgem claiming to offer rebates, with links to a fake online portal where victims are urged to share personal and payment details in order to claim the refund. In relation to Ofgem phishing emails, NFIB have reported 750 reports in two days.

Action Fraud issued an alert after receiving 449 reports relating to fake emails purporting to be from E. ON, the utility company. The emails state that the recipient is owed a refund as they have been overcharged. The links in the email direct the user to a genuine looking website that requests personal and financial information.

So What? Energy scams continues to be a threat and is something we could continue to see over the coming months, particularly as we move into the winter period.

Provenance: Council warns of energy rebate scammers targeting homeowners in Coventry - CoventryLive (coventrytelegraph.net)

New initiative after rise in doorstep scams | Barrhead News

Protective Marking	PUBLIC
FOIA Exemption	No
Suitable for Publication Scheme	No
Version	Final
	CoLP Strategic R&A
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	Strategic R&A
Reviewed By	Senior Analyst Strategic R&A