North East ROCU
Regional Organised Crime Unit Network

Monthly Threat Update

North East Economic & Cyber Crime

Welcome to the Monthly Threat Update (MTU) from NEROCU. This document provides an overview of Economic and Cyber crime trends within the North East and UK.

This document contains July 2023 data with a forward outlook.

Please contact the Regional Economic Crime Coordination Centre (RECCC) if you have any questions: **RECCC@durham.police.uk**

Reading Time 5-10 minutes.

North East RECCC Regional Economic Crime Coordination Centre

NERCCU North East Regional Cyber Crime Unit

Contents

Looking Back

Contents

Looking Forward

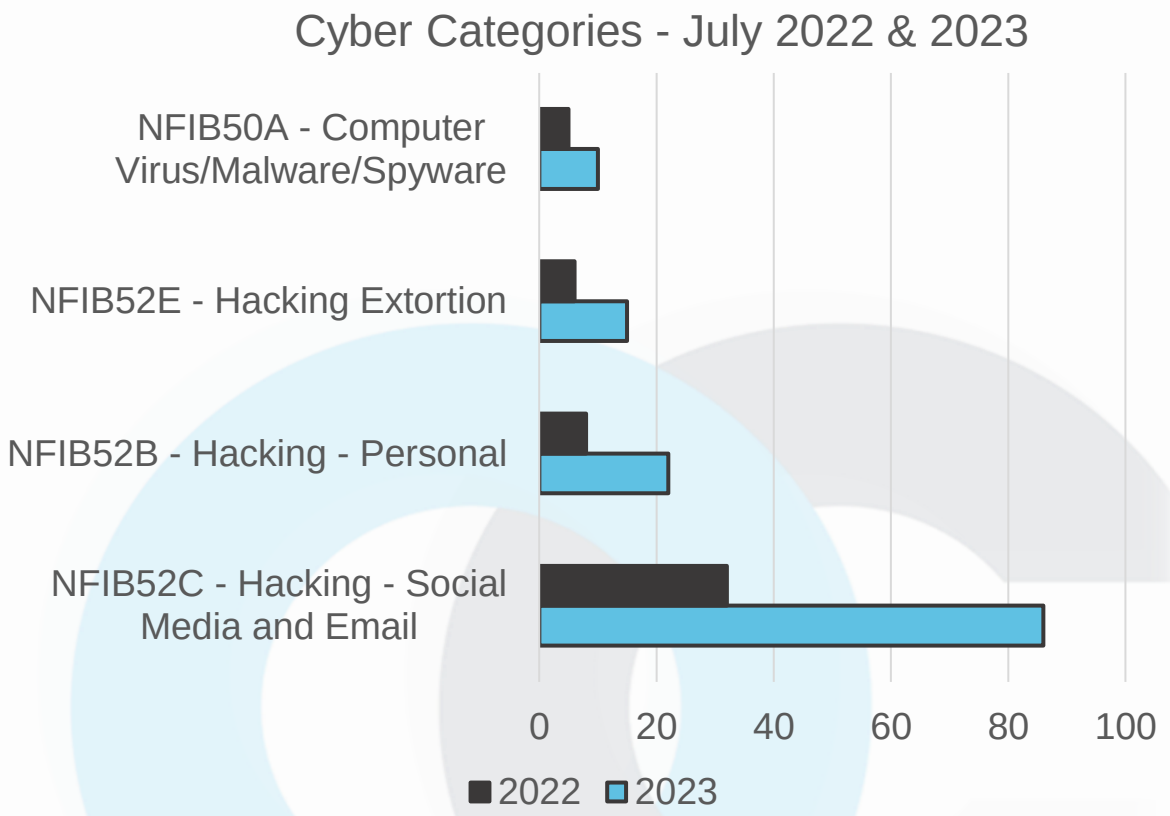
Cyber Dependent North East Victim Reports

Total Reports: July 22: 51 July 23: 123 160%

This data represents the number of reports received from Action Fraud with a Cyber category selected. In July 2022 there were 51 total Cyber reports. In comparison, there has been 133 reports in July 2023, this is a large increase of 160%. Through July 2023 the highest reported category was NFIB52C Hacking of social media and email. In 2023 there were 83 reports of NFIB52C, a 168% increase from the 2022 level of 32 reports.

Reports of NFIB50A Computer virus/malware/spyware have doubled this month from five reports in July 2022 to 10 in July 2023. This code refers to any intrusive software developed by cyber criminals to steal data, covertly monitor behaviour or damage and destroy computers and their systems.
In order to protect systems and computers from these types of attacks make sure to:

- Install an up-to-date anti-virus software and a firewall on your devices
- Ensure all browsers are set to the highest level of security
- Always install the latest software and app updates on all devices



Fraud Category
North East Victim Reports

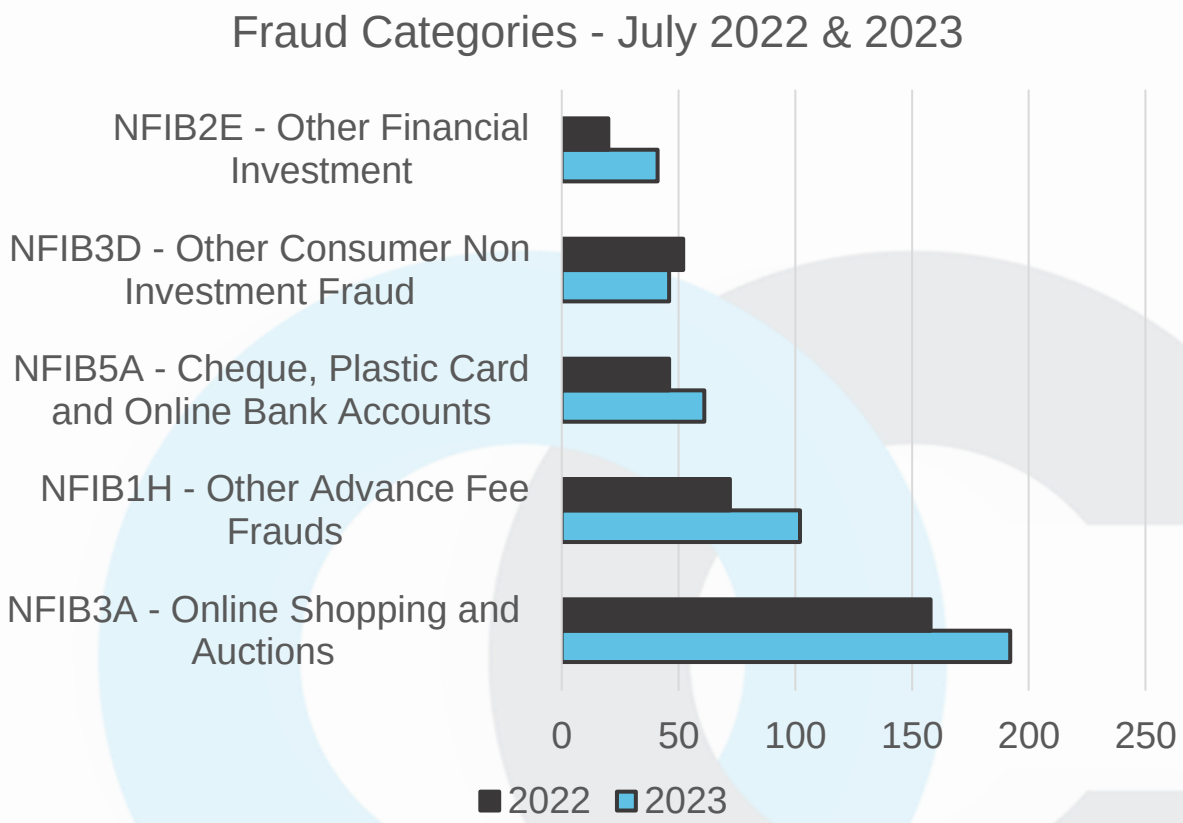
Total Reports: July 22: 658 July 23: 811 ↑ 23%

This data represents the number of reports received from Action Fraud with a Fraud category selected. There has been an increase in reports of 23% in July 2023 compared to July 2022. Throughout July 2023 the most reported category remains ‘Online shopping and Auctions’ with 192 reports in July 2023 compared to 158 reports in July 2022.

Since January 2020 there have been 646 reports featuring the keywords ‘gift card’. 97 of these reports are from 2023, this is a 15.5% increase from the same point in 2022 suggesting an increase in this Fraud and/or reporting. Gift cards such as iTunes, Steam Cards or Amazon are good targets for Fraudsters as they don’t require the physical gift card to redeem the value. Instead, the victim can read out the serial code on the back over the phone or pass it on via message/email for the Fraudster to gain the funds.

It is important to note that businesses or government departments will never ask for payment in the form of gift cards. Don’t share sensitive, personal or financial information in exchange for gift cards.

IF IT SOUNDS TOO GOOD TO BE TRUE IT PROBABLY IS!




£10
Gift Card Fraud
AF
#STAYTUNEDTOFRAUD
Cold calls, text messages and emails
£10
ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk
CITY OF LONDON POLICE
No genuine organisation will ask you to pay taxes, bills or fees using gift cards, or any other type of voucher. If you're contacted by anyone that asks you to do this, you're very likely the target of a scam.
Visit www.actionfraud.police.uk/giftcardfraud
for further advice on how to protect yourself

As car insurance premiums rise, drivers are being urged to watch out for bogus motor insurance deals on social media. More people could be targeted by criminals amid the cost-of-living crisis.

Colin Jemide from City Of London Police's Insurance Fraud Enforcement Department (IFED) tells us how we can protect ourselves from becoming a victim of 'Ghost Broking'.

CITY OF LONDON POLICE
Insurance Fraud Enforcement Department

What is 'Ghost Broking'?

Individuals or groups, known as 'Ghost Brokers', pose as middlemen for well-known insurance companies, claiming they can offer you legitimate car insurance at a significantly cheaper price. It is typically carried out by one of three ways: they will either forge insurance documents, falsify your details to bring the price down, or take out a genuine policy for you, before cancelling it soon after. For more information visit IFED | City of London Police.

Exclusive YouGov research reveals only one in six people (17%) are currently aware of Ghost Broking scams, despite its prevalence on popular sites like Facebook and Instagram.

£1.5m worth of losses from 'Ghost Broking' Frauds were reported to Action Fraud in the past year, according to City of London Police.

The data shows that males were most likely to use the services of a 'Ghost Broker' or be defrauded by them. The most susceptible group were those aged 20 to 29 years, followed by 30 to 39 years.

Live IFED investigations into 'Ghost Broking' have a total reported loss of £1,904,000 averaging £38,000 per investigation.

How do you know if you have been a victim of ‘Ghost Broking’?

You won’t realise you don’t have genuine cover unless you get stopped by police or make a claim. If you are not sure about the broker, check on the Financial Conduct Authority or the British Insurance Brokers’ Association website for a list of authorised insurance brokers: **register.fca.org.uk and biba.org.uk**. You can also check to see if your car is legitimately insured on the Motor Insurance Database website: **ownvehicle.askmid.com**.

How can people avoid becoming a victim of ‘Ghost Broking’?

If you need car insurance, be wary of heavily discounted prices on the internet or cheap prices you are offered directly. ‘Ghost Brokers’ often advertise on student websites or money-saving forums, university notice boards and marketplace websites such as Gumtree. They may also try to sell insurance policies to you through adverts in pubs, clubs or bars, newsagents and car repair shops.

- You can contact the insurance company directly to verify the broker’s details
- Be wary of brokers using only mobile phone or email as a way of contact. ‘Ghost Brokers’ have even been reported using messaging apps, including WhatsApp, Snapchat and Facebook. Fraudsters don’t want to be traced after they’ve taken money from their victims

How can I report any insurance fraud?

If you think that you’ve been a victim of a ‘Ghost Broker’, you can report your concerns to Action Fraud at actionfraud.police.uk or on 0300 123 2040.

You can also report insurance scams to the IFB CheatLine (powered by CrimeStoppers) on **0800 422 0421** or online.


HOW MUCH WOULD BUYING A GHOST BROKING POLICY COST YOU?
Liable for claim costs
£300 fixed penalty notice
6 points on your licence
Car seizure
Purchase of valid insurance policy
£150 minimum to retrieve impounded vehicle
Possible vehicle destruction
Initial purchase of invalid insurance policy

Amazon Scams

Amazon have been sending customers emails warning of two ways which criminals have been using to try and obtain victims money and personal data.

Prime Membership Scam
Customers have been contacted via text or phone call by criminals purporting to work for Amazon, they then tell them there is a problem with their membership. They will be asked to provide details or make a payment to resolve this issue.

Account Suspended Scam
Criminals use calls or texts to contact customers and tell them that their account will be suspended unless they take immediate action. They then send a Fraudulent link that will request sensitive information.

- **The retailer is reminding customers that the company will never ask people to provide payment information for products or services over the phone and people should check the URL of links they are sent before clicking.**

- **Legitimate websites will include ‘amazon.co.uk’ or ‘amazon.co.uk/support’ in the URL.**

- **Those who do wish to speak to a customer service agent, either with an issue of their own or to verify an email or text they’ve been sent, should go through the Amazon app on smartphones or through the website to obtain the correct contact information or links.**

Engagement Events

A busy month for the team with a lot of events due to the summer holidays. Below is just some of what the team have been up to…

The whole team attended the FinTech conference in Newcastle, Detective Inspector Paddy O'Keefe gave an input around risk.

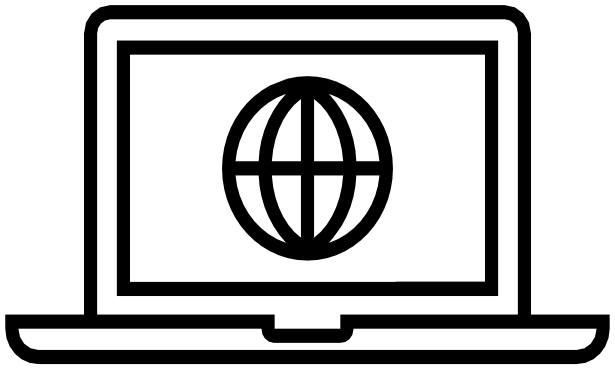
Luckily the rain stopped when we attended Chester Le Street activity week along with Durham Constabulary Cyber Crime Team and the EID fusion event at Stockton Park.

An event was held at Barclay's Middlesbrough branch with Victim Care and Advice Service to speak with customers and give out Fraud advice.

International students at Josephine Butler College in Durham attended an input around Fraud awareness delivered by the RECCC.

Horizon Scanning

Monitoring Threats



If you are going on holiday abroad this summer be wary of taking photos of boarding passes and uploading them to social media. Boarding passes contain personal data that can be stolen by criminals and used in identity Fraud if it is uploaded online for all to see.

It can lead to targeted phishing attempts with malicious links to try and obtain more sensitive data. The boarding pass also contains details of flight numbers, flight departure and arrival times and the travel company you are flying with, this information could lead them to contact you claiming to be the travel company.

If you do take an airport photo before you fly, ensure that the barcode and any other personal information is not on show.

What's Happening Next?

It has been reported that 'debt help' ads on social media are targeting vulnerable people who are finding themselves in financial difficulties. The ads promise to write off up to 85% of debt for those struggling by signing them up to an Individual Voluntary Arrangement which is a court approved debt solution. Although it is marketed as an 'easy fix' of consolidating debts, the companies advertising are neglecting to tell those signing up that it affects their credit score and can carry large amounts of fees for the service. The companies make false claims and even pose as charities to lure people in. The Citizens Advice Service have found a number of the adverts to be misleading and even fail to mention that the person signing up will be entering into an Individual Voluntary Arrangement.

This also offers criminals the opportunity to exploit the fact that these advertisements are on social media platforms and claim to offer a 'debt help' company. Ensure that if you are using this service that you fully understand the agreement and try to establish that the company you are using is legitimate.

With a disappointing rainy summer almost over, last minute holiday bookings are on the rise for people in the search of nicer weather. Due to the surge in demand, it may cause people to look for last minute deals online. We can do the following to keep ourselves safe :

- Don't reply to unsolicited emails, texts, social media or calls with holiday offers. Links and attachments in emails may lead to malicious websites or download viruses.
- Book a holiday directly with an airline or hotel, or through a reputable agent. Check whether they're a member of the Association of British Travel Agents.
- If you decide to deal directly with the property owner or a letting agent, ask them questions about the booking, room, location and area. Don't book on websites that don't have a padlock icon (https) in the address bar and be extra cautious if you're asked to pay using bank transfer or cash; pay by credit or debit card if you can.

Handling Instructions

Distribution List
NEROCU
North East Police Forces

Provenance: Available upon request.

Protective Marking	**Official – Law Enforcement**
Version	**Final**
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	**NEROCU**
Authors	**Megan Turner – Engagement Officer** **Olivia White – Intelligence Analyst**
Reviewed By	**D/Inspector Paddy O'Keefe**

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 NEROCU in confidence and may not be shared other than with the agreed readership/handling code without prior reference to NEROCU. 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.