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 February 2024 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.

Contents

Looking Back

Contents

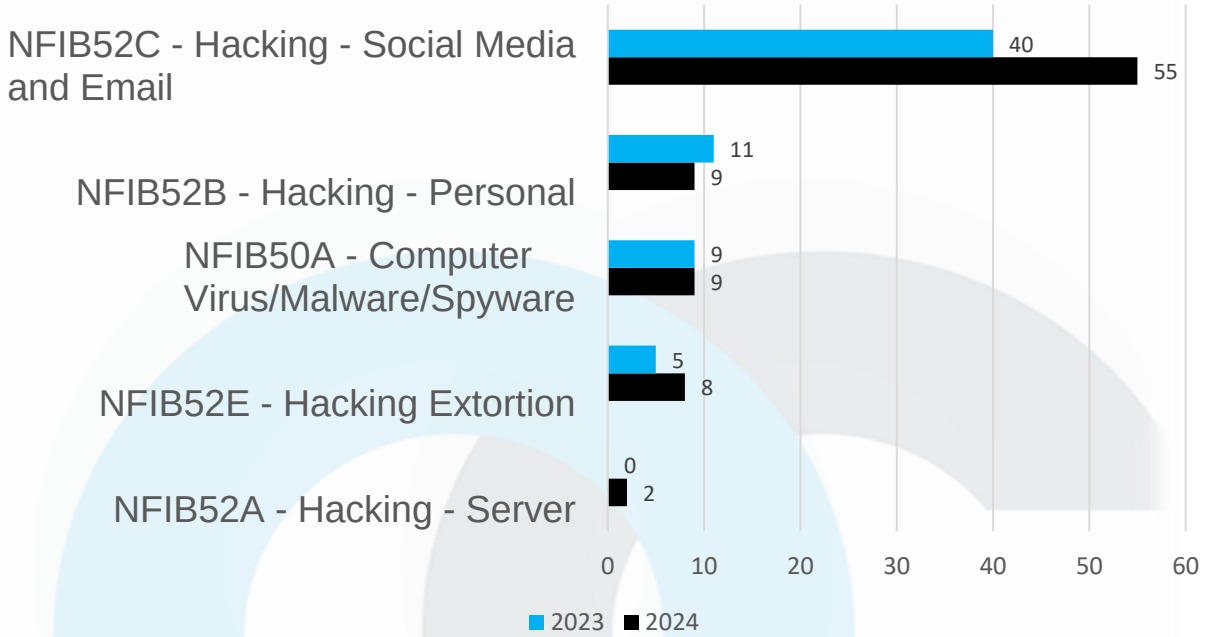
Looking Forward

Cyber Dependent North East Victim Reports

Total Reports: Feb 23: 65 Feb 24: 83 ↑ 27.7%

This data represents the number of reports received from Action Fraud with a Cyber category selected. In February 2024 there was a total of 83 Cyber reports, in comparison, there were 65 reports in February 2023, an increase of 27.7%. In February 2024, the highest reported category was ‘Hacking- Social Media and Email’ with 55 reports.

Cyber Categories February 2024 & 2023



Fraud Category
North East Victim Reports

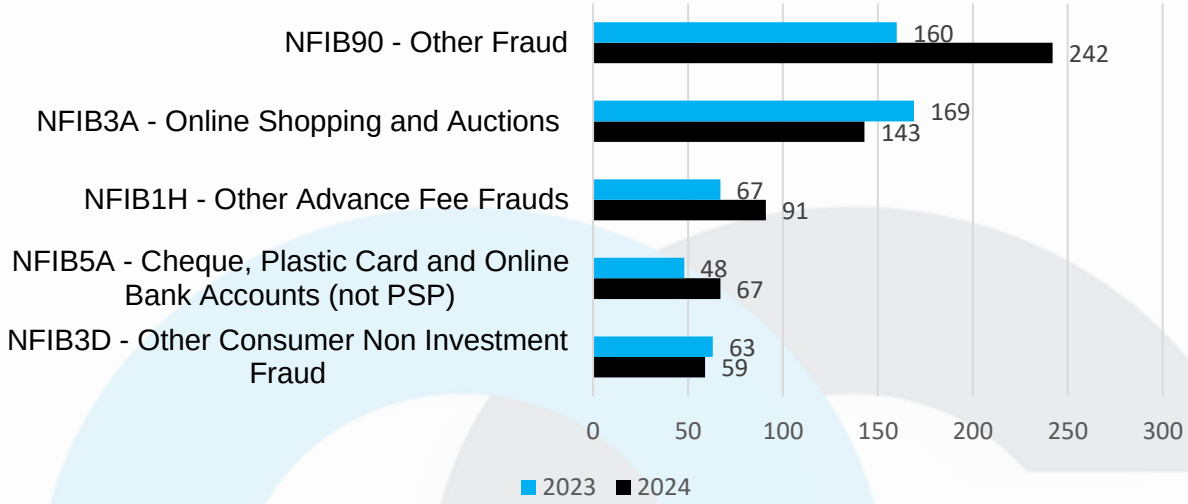
Total Reports: Feb 23: 507 Feb 24: 602 ↑ 18.7%

This data represents the number of reports received from Action Fraud with a Fraud category selected. There has been a total of 602 reports in February 2024, an increase of 18.7% compared to February 2023. Throughout February 2024, the most reported category remains 'Online Shopping and Auctions' with 143 reports but it is worth noting that this has reduced by 15.4%.

Fraudsters are encouraging victims to purchase gift cards and provide them with the cards or codes. £15,000 worth of cards were supplied to fraudsters by victims in the North-East last month. Cards were mainly for Apple and Amazon. In some instances, the gift cards were used as payment for items that do not appear or in advance fee frauds. One victim spent over £5000 with gift cards to pay taxes to obtain a community grant following a hacked message from a family member.

Fake text or whatsapp messages from family members requesting urgent financial help have continued into this reporting period. 14 victims have reported such messages to Action Fraud in February. In most cases the victim did not believe the message was real. In some, victims report losses within a range of £1600 to £6800.

Fraud Categories February 2024 & 2023



Messages from EVRI requesting the victim click on a link to rearrange a parcel delivery or additional delivery fees are on the increase. After submitting card details, several victims then reported contact from their banks' fraud team stating their accounts had been compromised and to transfer funds into another account belonging to the fraudster. In some instances, victims were encouraged to open Revolut accounts to keep their funds safe.

Engagement Events

Below is just some of what the team have been up to this month…

The RECCC have been to Windsor this month with UKFIU (UK Financial Intelligence Unit) and YHROCU (Yorkshire and Humber Regional Organised Crime Unit) to give an input at the Flywire annual conference.

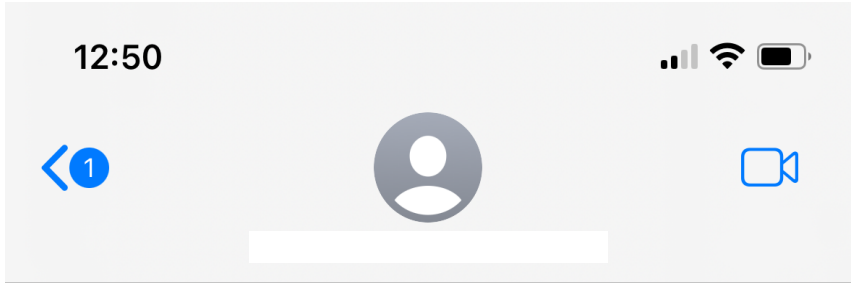
Durham University Criminology students received an input on money muling along with a Fraud Awareness stalls for student money week.

Our ongoing Fraud awareness (Operation Lazio) sessions with cadets have taken place at Newcastle College this month.

The RECCC attended ICAEW (The Institute of Chartered Accountants, England and Wales) annual conference and gave an input on economic crime.

Our Fraud Roadshow continued with Northumberland Libraries and Ponteland Library was visited this month for a drop-in session for public and staff.

STEMfest (Science, Technology, Engineering and Mathematics) was held in Darlington for KS2 students and school staff, the RECCC hosted a stall where pupils were able to take part in an interactive session.



iMessage
Today 12:50

EVRI mail package in the process of transportation, due to damage to the outer package, address information is lost, can not be delivered. Please be sure to update the delivery address information in the link within 12 hours.

https://evri-uk.motorcycles/uk

(Please reply Y, then exit the SMS, re-open the SMS activation link, or copy the link to open in Safari)

The EVRI team wishes you a great day!

The sender is not in your contact list.

Report Junk

11 reports in the North East

EVRi

There has been an increase in Fraudulent Evri delivery texts similar to the one pictured (left).

When victims reply ‘Y’ and receive a link they are taken to a page that looks similar to the Evri website, the website requests personal information and requests the victim to card details.

- Do not reply to the text and do not click any links.
- If you have entered any personal details, contact your banks Fraud team immediately by dialling 159.
- Forward any suspicious texts to 7726 to be investigated.

If you think you have been a victim of Fraud, contact Action Fraud at www.actionfraud.police.uk or call **0300 123 2040**.

Man Arrested For Fraud And Money Laundering

As a result of the police activity, a 39-year-old man was arrested on suspicion of Fraud by false representations and money laundering. The man has since been released on police bail while enquiries continue.

This month, officers from our Economic Crime Team targeted an address on Clarendon Road in Thornaby. The strike day which was carried out as part of the national OpHenhouse activity.

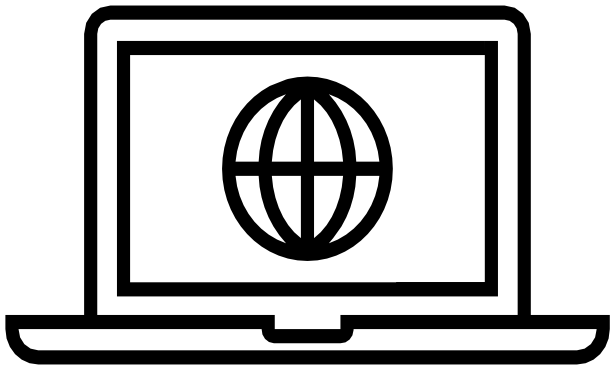
This success has been the result of some outstanding partnership working and a clear example of the robust activity we'll take against anyone looking to defraud members of the public.

The operation came after intelligence was received from Cleveland Police (UK) about reports of fraud in their force area.

Organised criminality of any kind will not be tolerated in our region's communities, and we will always look to identify those responsible for such offences and bring them to justice.

Horizon Scanning

Monitoring Threats



There has been an increase in businesses being targeted by Impersonation Fraud. Businesses, along with individuals are receiving phone calls impersonating the banks Fraud team.

If you receive a call claiming to be from the banks Fraud team and are in any doubt about this. Hang up and use another phone if possible, to dial 159 or a number known to you to check this out.

Reports have been received that phishing emails claim the recipient could receive a free “36 Piece Tupperware Set” with the email body saying, “Answer & Win” or “You’ve been chosen!” with instructions for a short survey to be completed to win the prize. The email also shows a photo of a Tupperware set along with a logo of either Asda, John Lewis or Costco. The use of well-known and trusted brand logos attempts to add a layer of authenticity to the scam. It is believed that once the survey link is clicked it will lead to either a request for financial/personal details or will download malicious malware.

Make sure to be vigilant when receiving emails and remember … if it sounds too good to be true, it probably is!

ALWAYS TRUST YOUR INSTINCTS

NOT THE CALLER

NOT THE TEXTER

NOT THE EMAILER

If you don't think they are who they say they are, always take time to stop and think.

takefive-stopfraud.org.uk

TAKE FIVE

TO STOP FRAUD™

Gift Card Fraud

How to protect yourself :

- **The police, banks and other reputable organisations will never ask you to purchase a gift card.**
- **Avoid giving out any details or PINs from gift cards.**
- **Be aware of people online striking up relationships and requesting you to purchase gift cards.**
- **If you receive an email from a work colleague, check it out with them in person where possible.**

Members of the public and sometimes businesses/employees are targeted with 'Gift Card Fraud'.

The criminal (often presenting as the victim's colleague/manager or organisations such as the police, bank, DVLA and HMRC) asks the victim to purchase gift cards, usually from supermarkets.

Methods that have been used are phone calls, emails (even emails purporting to be from the victim's place of work, requesting the gift voucher for a colleague) and messages on social media or emails.

Once purchased, victim's are asked to pass over details from the gift card.

Gift cards are popular with criminals to launder money as they are difficult to trace compared to bank transfers.

£15K
lost in the North East throughout February

If you think you have been a victim of Fraud, contact your bank immediately and report to Action Fraud at www.actionfraud.police.uk or call **0300 123 2040**.

Did you know?

In just one year, 1 in 17 adults were victims of fraud

Source: Crime Survey for England and Wales, year ending September 2023

The government have launched the STOP! THINK FRAUD campaign.

You can access the campaign here : [Stop! Think Fraud - How to stay safe from scams (stopthinkfraud.campaign.gov.uk)]

Access advice on how to protect yourself from Fraud, information on how to report Fraud and steps to recover if you have been a victim.

What's Happening Next?

Planning a holiday in 2024?

Summer is fast approaching which means prime holiday season is looming. Fraudsters are likely to use this to scam people.

Spot the signs of Holiday Fraud

- You're contacted out of the blue by a travel agent or company you've never spoken to before, offering a holiday at a very low price.
- The details, pictures or address of the property or hotel on offer look suspicious, or independent website reviews aren't favourable or don't exist.
- You're asked to pay using bank transfer or cash; pay by credit or debit card if you can for extra protection.

What should you do?

- 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 (ABTA).

- 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** **Claire Hardy– Intelligence Analyst**
Reviewed By	**T/Sgt Brian Collins**

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.