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 March 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

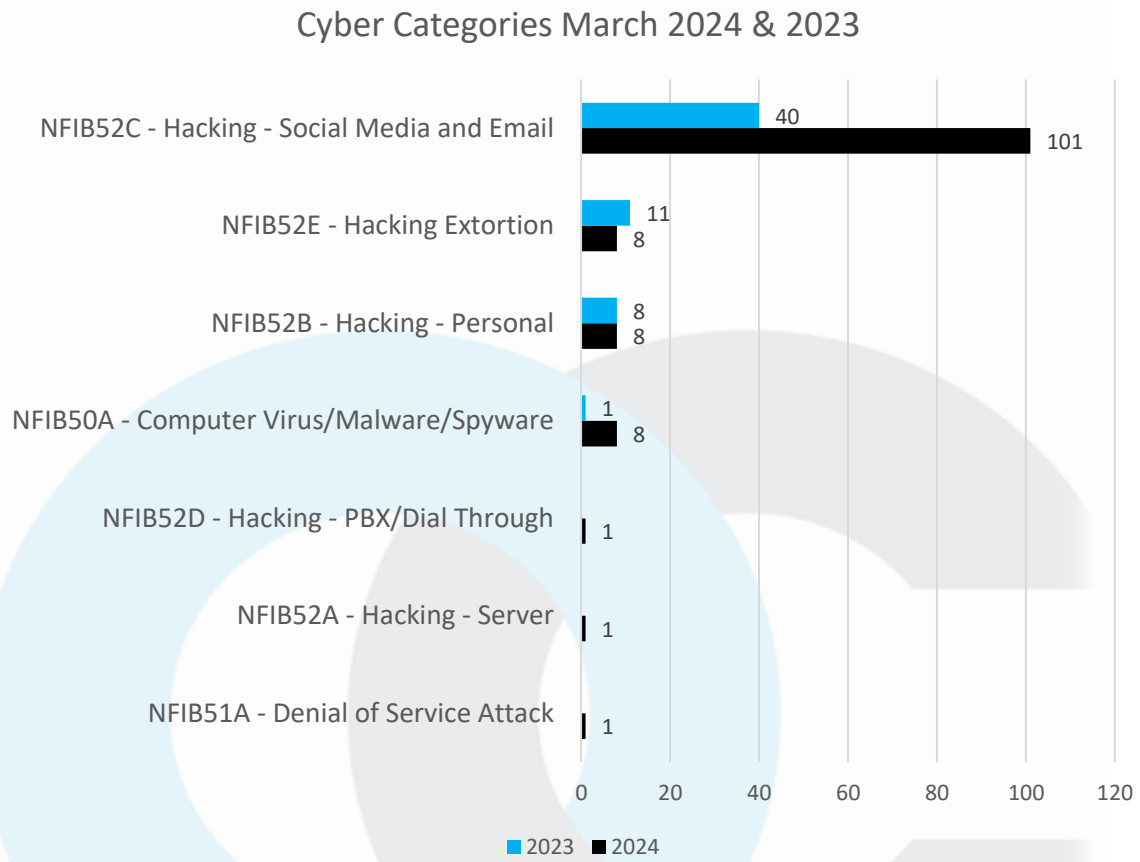
Cyber Dependent North East Victim Reports

Total Reports: Mar 23: 60 Mar 24: 128 ↑ 113%

This data represents the number of reports received from Action Fraud with a Cyber category selected. March 2024 there was a total of 128 Cyber reports, in comparison, there were 60 reports in March 2023, an increase of 113%. In March 2024, the highest reported category was 'Hacking- Social Media and Email' with 101 reports.

Phishing emails continue from scammers and one MO detected this month was an increase in the lure of offering recipients Paddock Club passes to the Silverstone Formula One. Nationally victims reported substantial losses, ranging from £2,300 to £10,000.

Another MO targets senior company employees 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 organization's email addresses have been compromised, and 132 reports using this methodology identified nationally since March 2023.



Fraud Category
North East Victim Reports

Total Reports: Mar 23: 748 Mar 24: 689 ↓ 7.8%

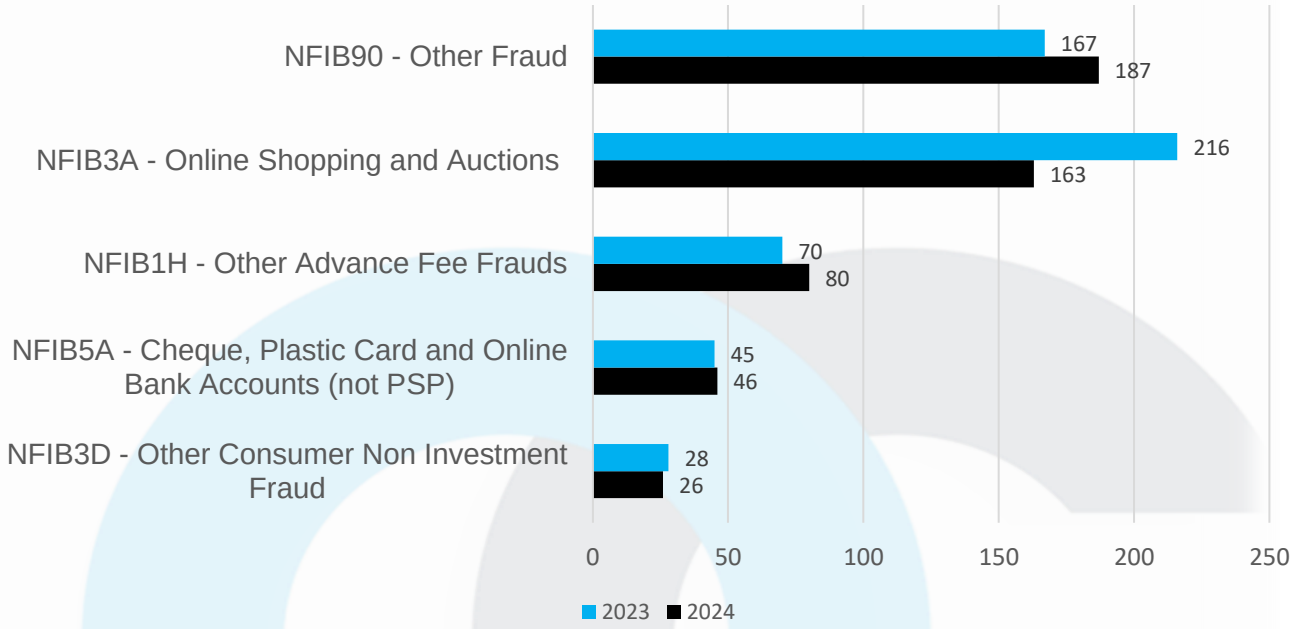
This data represents the number of reports received from Action Fraud with a Fraud category selected. There has been a total of 689 reports in March 2024, a reduction by 7.8% compared to March 2023. Throughout March 2024, the most reported category remains 'Online Shopping and Auctions' with 163 reports but it is worth noting that this has reduced by 25.5%. Of note:

- £23,500 has been lost by victims in the North East when buying cars online this month. Most of this was in relation to deposits paid to secure cars sold on Facebook Marketplace, Gumtree or Ebay.

- Fake adverts have been circulated on Facebook marketplace for caravan holiday rentals in Berwick. Victims have paid deposits and then been unable to contact the company. With the holiday season approaching it is likely that there will be more scams of this nature.

- Victims report meeting buyers face to face to sell items such as phones with payment via bank transfer. Despite the seller showing the victim payment has gone through on their banking app, payment is never received.

Fraud Categories March 2024 & 2023



This month, 4 North East Vinted sellers report losing a total of £1400 after clicking on a link to retrieve funds following a transaction. When the transactions did not work, victims report speaking to a Vinted chatbot (fake) and being advised that as certain banks cannot be used to retrieve funds so the best solution would be to open a new account with Revolut bank and to transfer an amount in to receive their money. The scammers then remove all funds from the Revolut account.

Engagement Events

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

This month was the end of our Northumberland Libraries Fraud Roadshow we have covered Bedlington, Hexham, Cramlington, Ashington, Ponteland and Alnwick spending the morning speaking to staff and members of the public at each library.

We have held an information session on Fraud awareness for staff at North Star housing who provide supported housing for vulnerable young people in Norton.

Our quarterly meeting at ‘Let’s Connect’ Hartlepool gave us a chance to do an input to staff and clients about the rise in Gift Card Fraud in the area.

Fraud Awareness workshops delivered at Middlesbrough College over the course of a week reaching over 400 students and staff.

We attended Lyynfield pensioners group to give an input on Fraud Awareness and did the final few sessions with Police Cadets which you can find on the next page ….

12

Fraud workshops and awareness sessions held.

Fraud awareness training delivered to cadet leaders and cadets.

Operation Lazio

North East RECCC Regional Economic Crime Coordination Centre

North East Police Cadets

120+

Cadets and cadet leaders involved in sessions across all three North East Police Forces.

Delivery of Fraud awareness sessions by cadets to local communities.

Op Lazio is an engagement operation across the 3 North East Police Forces involving Police Cadets; the theme is Building Resilience Against Fraud; the cadets/cadet leaders take part in a combination of presentations and workshops designed to increase awareness of Fraud and provide a solid foundation for the cadets and cadet leaders to deliver their newfound knowledge into communities.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

ABTA
The Travel Association

ATOL PROTECTED

Be safe online

Use 3 random words to create a strong password for your email that's different to all your other passwords. If 2-step verification is available, always enable it.

BOOK NOW

#StopHolidayFraud

Impersonation Fraud

Impersonation Fraud happens when you're contacted by someone you believe you can trust. Your bank, HMRC, the police, or even a family member. They may ask you for personal or financial details, invent reasons to ask you for money, or convince you that your bank account is at risk.

Your bank will never ask you to transfer money to a 'safe account', HMRC will never pressure you or threaten you with arrest, and the police will never ask you to withdraw money to assist with an investigation.

Criminals use messaging apps to pose as a family member stating they have lost their phone, asking for money. Once they get a reply, they'll invent a reason for needing money. This could be money for bills, rent, a new phone contract etc. If you get a message like this, always speak to the person over the phone or face to face before parting with your money or personal details.

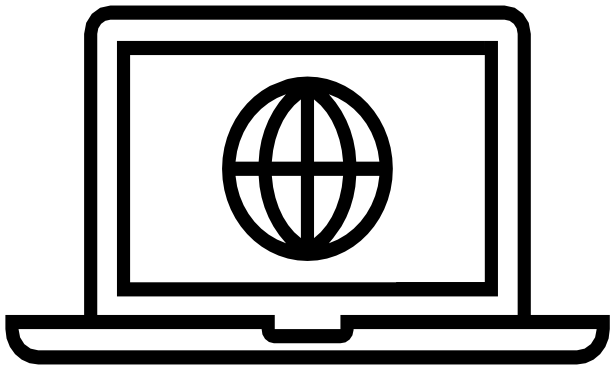
✋ **STOP: Take a moment to think before you reply.**

👊 **CHALLENGE: Ask yourself, could this be fake?**

👍 **PROTECT: If you think you've been scammed, contact your bank immediately.**

Horizon Scanning

Monitoring Threats



There has been an increase in reports of sellers on Vinted being sent a link to set up an online bank account to receive their funds. On setting up the account they are talking to a chatbot through messages and are told to deposit £200 to get started.

The victim then can't retrieve their money and this is usually when they realise they have been scammed.

How to protect yourself

- Do not share personal details, bank account details or email addresses on Vinted.
- Do not buy or sell anything out of the app, for example if someone is encouraging you to use WhatsApp or text.
- Try not to leave the app i.e. don't click any links that take you out of the Vinted app.

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, victims 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**.

DO NOT SHARE TWO STEP VERIFICATION CODES OR ONE TIME PASSWORDS

THEY ARE IN PLACE TO PROTECT YOUR ACCOUNTS AND ARE NOT TO BE SHARED WITH ANYONE, NO MATTER HOW TRUSTED.

CRIMINALS ARE USING HACKED WHATSAPP AND SOCIAL MEDIA ACCOUNTS TO POSE AS FRIENDS AND FAMILY ASKING FOR CODES AND ONE TIME PASSWORDS.

What's Happening Next?

Planning on buying second hand tickets this summer?

With Summer around the corner it is expected that social events will naturally start to increase. As a result those who wish to attend concerts, music festivals and other events and have missed out on ticket sales will look to purchase them from ticket resale sites or often use Facebook.

The total lost in the North East to Ticket Fraud in 2023 was

£109,150.47

What should you do?

- Buy tickets from reputable sellers, try to avoid buying from random people on social media.
- Use a credit card where possible for better protection under Section 75.
- Try to use the box office site, official website or reputable ticket seller when purchasing tickets.
- Avoid paying directly into someone's bank account.

You should report to Action Fraud online or by calling 0300 123 2040 or online at actionfraud.police.uk

North East RECCC
Regional Economic Crime Coordination Centre

North East ROCU
Regional Organised Crime Unit Network

For more information search 'nerccu police'

Scan to visit our website

BUILDING RESILIENCE AGAINST FRAUD

How to report

Police

All Fraud in the UK is reported to the police at Action Fraud by phone or online:
0300 123 2040
www.actionfraud.police.uk

Action Fraud is the central reporting point for all reports of fraud, your local police force will be informed by Action Fraud.

Banks

Dial 159 (Stop Scams UK Anti-Fraud Hotline)
An automated line which Takes you through to your Bank's Fraud team .

For alternative ways of contacting your bank only use the contact details on your bank card or the official website.

Emails

Forward Fraudulent emails to
report@phishing.gov.uk

Phone Numbers

Forward phone numbers Sending you Fraudulent Messages or calls to **7726**

Handling Instructions

Distribution List
NEROCU
North East Police Forces

Copyright © NEROCU 2023 Disclaimer: While every effort is made to ensure the accuracy of the information or material contained in this document, it is provided in good faith on the basis that NEROCU and it's staff accept no responsibility for the veracity or accuracy of the information or material provided and accept no liability for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any information or material herein. The quality of the information and material contained in this document is only as good as the information and materials supplied to NEROCU. Should you or your police force hold information, which corroborates, enhances, or matches or contradicts or casts doubt upon any content published in this document, please contact NEROCU. Any use of the information or other material contained in this document by you signifies agreement by you to these conditions.

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 – 3P** **+-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.