

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 May 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



- [Action Fraud: Regional Cyber Summary](#)
- [Action Fraud: Regional Fraud Summary](#)
- [Engagement Events](#)

Contents

Looking Forward



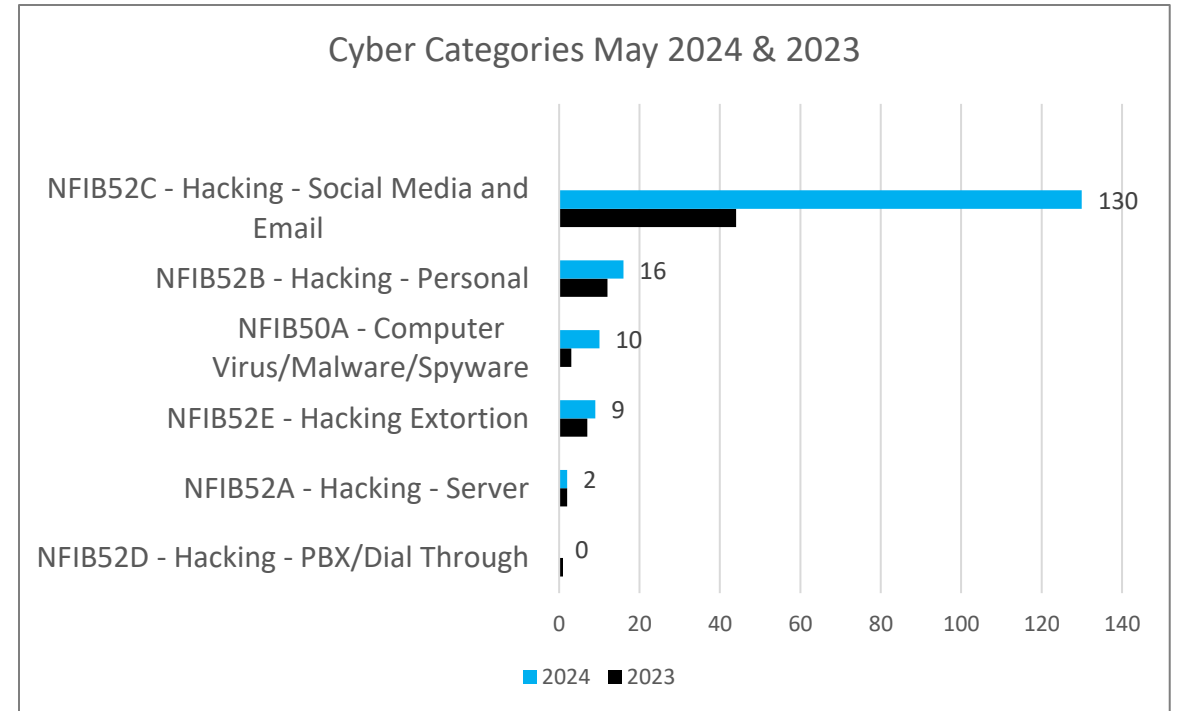
- [Horizon Scanning](#)
- [What's Happening Next](#)

Cyber Dependent North East Victim Reports

This data represents the number of reports received from Action Fraud with a Cyber category selected. In May 2024 there was a total of 167 Cyber reports, in comparison, there were 69 reports in May 2023, an increase of 142%. The highest reported category was 'Hacking – Social Media and Email' with 130 reports. The age category 31-40 reported the most 'Hacking – Social Media and Email' reports, followed by the 18-30 age category.

A broadband Cyber Fraud trend was identified in the region this month, 68% of these victims reported a total loss totalling £12,571. Victims have received phone calls claiming to be from their broadband suppliers, informing the victim they are suffering from poor connection and speed, and they will be able to assist. The victim is asked to download a specific app which allows the caller to gain remote access to their device. The caller highlights they have identified numerous viruses and will be entitled to a refund. The caller asks the victim to make a small payment of £2.99 to verify their details to arrange a refund, this leads to the caller attempting to use the card for further transaction, amounts of up to £3000 have been reported by victims. Similar motives have also been used where a small payment is required to book an appointment for an engineer to attend to the broadband problem. This has led to the victims Amazon account being accessed and numerous transactions for gift cards purchased.

Total Reports: May 23: 69 May 24: 167 ↑ 142%



Fraud Category North East Victim Reports

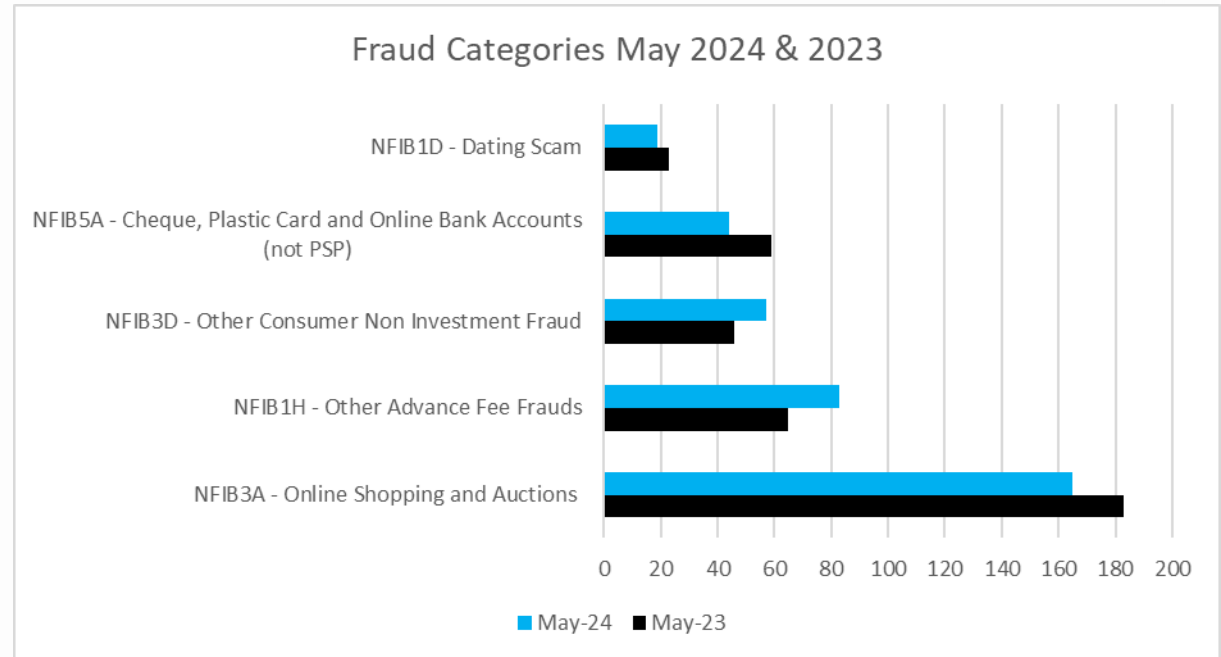
Total Reports: May 23: 696 May 24: 656 ↓ 5.75%

This data represents the number of reports received from Action Fraud with a Fraud category selected. Although the number of Frauds reported in May 24 (656 reports) is higher than April's level, there has been a reduction of 5.75% compared to May 2023.

Throughout this month, the most reported category remains 'Online Shopping and Auctions' with 165 reports but it is worth noting that this has reduced by 9.8%.

A warning has been issued nationally to holidaymakers looking to book flights as there has been a rise in scams involving fake social media accounts impersonating airlines on X, formerly known as Twitter.

According to the consumer association Which?, fake X accounts have been found impersonating major UK airlines, including British Airways, easyJet, Jet2, Ryanair, Tui, Virgin Atlantic, and Wizz Air. Scammers ask customers to send personal data or direct them to phishing websites to steal their card details. Holidaymakers are urged to report fake social media accounts and are reminded to never disclose personal or financial details via these channels



This month victims have lost £7300 in Ticket Frauds. Frauds were for flights and concert tickets. 7 victims lost an average of £400 purchasing last minute Taylor Swift Tickets for her Eras tour. Tickets were advertised on TikTok and Facebook. Some of the accounts used by sellers had been hacked previously by scammers.

Engagement Events

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



Students at Hartlepool College have received multiple Fraud Awareness inputs including advice and information on money muling.

Barclay's hosted a staff awareness workshop with us for their colleagues to discuss the impact of banking staff submitting Suspicious Activity Reports (SARs) and the Banking Protocol.

Community groups in Hexham have received a Fraud Awareness input.

The team have been to Saltburn Library with Barclay's to speak with customers, staff and members of the community while visiting the pop-up branch.

Redcar and Cleveland Council Apprentices took part in a Fraud Foundation workshop, participants were based in a variety of different roles within the council where they can feed in their newfound knowledge of Fraud.

We delivered a Fraud Foundation input to learners and staff on the construction course at Optimum Skills.

Other organisations that have received workshops and inputs are County Durham Parish Council, Horden Together Community Group and Eaglescliffe Computer Club.





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.

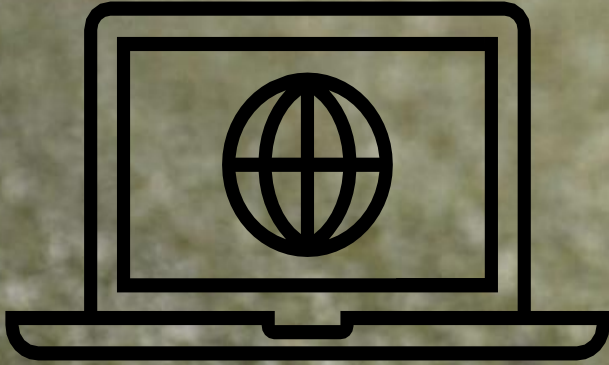
BOOK NOW

#StopHolidayFraud



Horizon Scanning

Monitoring Threats



The Euro's are now underway – fans are advised to be wary of ticket resales.

- It is expected that there will be a rise in Fraudulent ticket sales on social media and resale sites.
- There may be a rise in sales of fake merchandise, people should remain vigilant when purchasing good online or on online marketplaces.
- Where possible purchase tickets directly from UEFA rather than resale sites and individual sellers.
- When purchasing from a website, ensure the website is secure and check the web address.
- Watch out for fake website URLs.
- Do not purchase merchandise or tickets using social media as this leaves you highly vulnerable to being the victim of Fraud.

COURIER FRAUD




Criminals targeting vulnerable people pretending to be a police officer, bank official or figure of authority.

If you have suspicions, hang up & call them back on a trusted number from a website or bank statement.



If you're a victim report it to Action Fraud & your bank immediately.



The Fraud often starts with the **criminal contacting the victim outside of the group via a call**. They have a fake profile picture and name, so it appears they are a legitimate member of the group.

They then state they will send the victim a **one-time passcode** to access or join an upcoming group call. The victim is asked to share the passcode to 'register' for the call. The passcode is used to access the victim's WhatsApp account and register it to a new device preventing the victim from accessing it.

Messages are then sent to group members, contacts, friends and family **requesting them to send money** urgently.

WhatsApp group chat members are being warned they could be targeted by criminals, as Action Fraud reveals it has received **636 reports from victims of the messaging app this year**.


How to protect yourself:

- Do not engage with anyone outside the chat where possible if they are unknown to you.
- Forward any suspicious messages to 7726.
- Do not send one-time passcodes to **ANYONE**, even known or trusted people.

actionfraud.police.uk/mulletover


Spotted a **suspicious** text message?



 Suspicious text messages should be forwarded to **7726**. This enables your provider to investigate the origin of the text and take action, if found to be malicious.

 **7726**

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

Cyber
Aware 

 TO STOP FRAUD™

What's Happening Next?



GOOD NEWS FOR O2 CUSTOMERS

Phone company O2 are implementing a brand-new call identification system for millions of customers. It will reach Android users first and the plan is to roll it out to other devices in the coming months.

The filter will display the details of the company or person calling and display the organisations details on the screen and the AI technology can determine if it suspects the call to be a scam, the system will note the behaviour and notify anyone else receiving a call from the number.

What does this mean for me?

By doing this O2 hope to give their customers confidence in knowing who is calling and minimise scam calls. O2 already use AI technology to detect spam text messages, this has prevented 83 million spam texts from reaching customers in 2023.

Great news for anyone who has an O2 sim and it looks like you won't have to wait long as it is expected to roll out in the next few months.





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.



Emails

Forward Fraudulent emails to
report@phishing.gov.uk



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.



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 its 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– Economic Threat Desk Analyst Sarah McCluskey –Cyber Threat Desk 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.