

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 August 2024 data with a forward outlook.

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

Reading Time 5-10 minutes.

# Contents

Looking Back



- [Action Fraud: Regional Cyber Summary](#)
- [Action Fraud: Regional Fraud Summary](#)
- [Action Fraud: Cleveland](#)
- [Action Fraud: Durham](#)
- [Action Fraud: Northumbria](#)
- [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 August 2024 there was a total of 132 Cyber reports, a 60% increase from August 2023.

Consistent with national reporting, 'Hacking-Social Media and Email' was the most reported category with 100 reports.

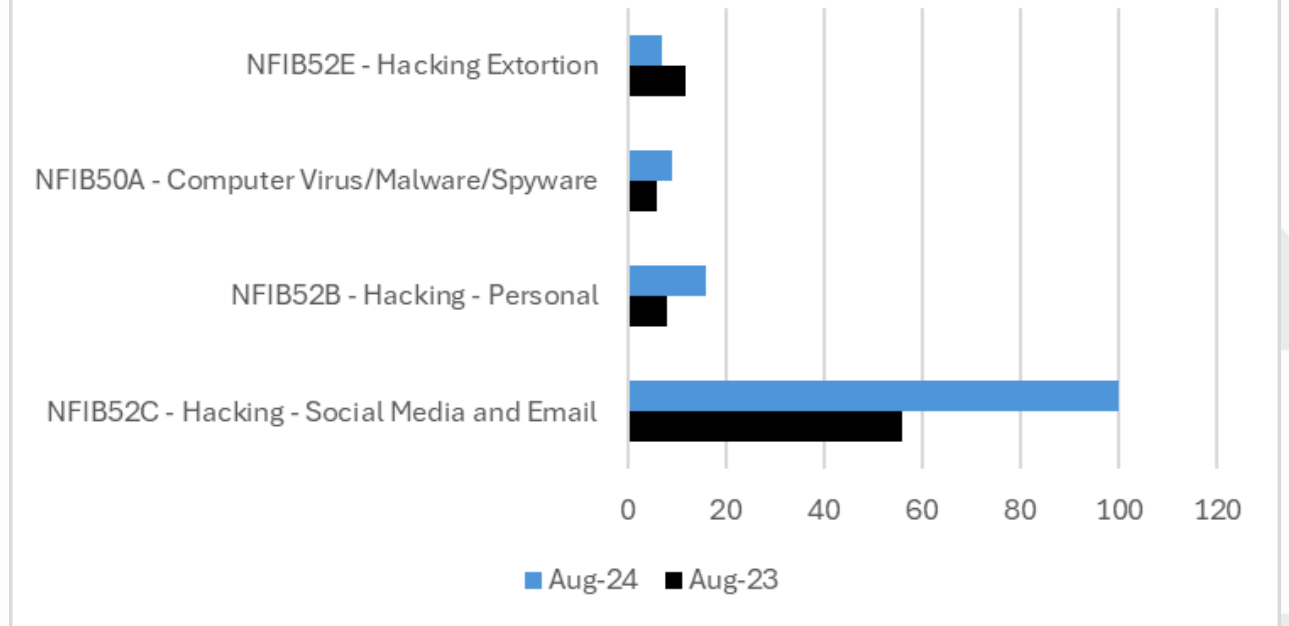
Within the 'Hacking-Social Media and Email' category, there has been an increase in 'Sim-Swap' reports across the region. 'Sim-Swapping' is where fraudsters can gain control of your mobile phone number by convincing the phone provider to transfer the service to a SIM in their possession.

**(See slide 15 for further information about SIM-Swapping')**

There have been 13 Sim-Swap reports in the North East in August. One victim reported a 'Sim-Swap' incident, which resulted in further accounts being hacked including their Klarna account. The offender debited a total of £2371 and applied for a credit card on the account. Another victim reported their social media accounts hacked. Their banking app was also hacked resulting in a £2000 loss.

Total Reports: August 23: 82 August 24: 132  60%

### Cyber Categories August 2023 & 2024



# Fraud Category North East Victim Reports

Total Reports: August 23: 903

August 24: 590 ↓ 34.7%

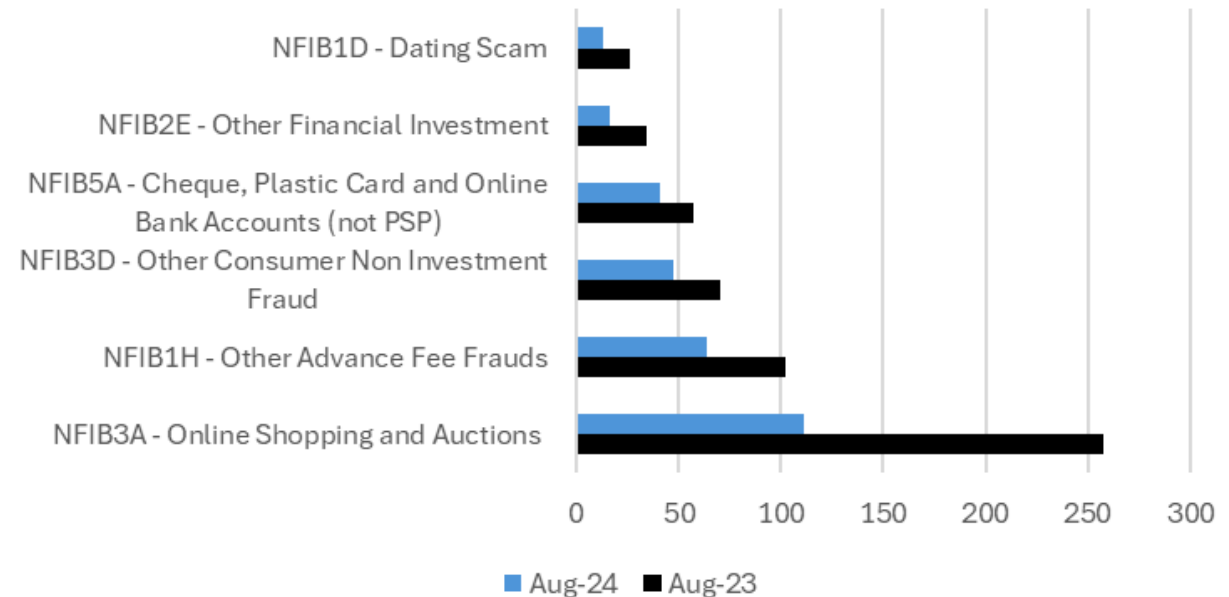
This data represents the number of reports received from Action Fraud with a Fraud category selected. In August 2024 there was a total of 590 Fraud reports, a reduction of 34.7% against the previous year.

Throughout this month, the most reported category remains 'Online Shopping and Auctions' with 117 reports but it is worth noting that this has reduced by 54%.

With the start of the football season, there has been a rise in Frauds reported when buying tickets for Newcastle United matches. Generally, more concert and match goers are joining Facebook groups to obtain tickets. One victim joined a group for Newcastle United tickets and managed to arrange tickets through the group's administrator from a 3<sup>rd</sup> party. Before receiving the ticket, the group disappeared from social media. Research has identified that Facebook groups exist dedicated to obtaining tickets for all North East football clubs and many are legitimate. There are also groups for concert tickets for Oasis and other popular musicians.

Phishing messages about missed parcel deliveries from EVRI have continued this month with victims asked to enter credit card details to make a small payment. Within a few hours, the victim receives a phone call from their bank (scammer) reporting fraudulent activity on their account and are asked to transfer funds to a Revolut account temporarily. Victims have lost a total of £9184 this month.

### Fraud Categories August 2023 & 2024



There are reports of an advert on Facebook for HMV selling off low priced stock of Blue ray players and DVD players from HMV stores closing in Europe (DVD players & blue ray players). The website followed through the link is fake and products are never received.

# **Three men jailed after stealing over £50,000 from North East victims by claiming to be from bank's 'Fraud Squad'**

**Following a Courier Fraud investigation by NEROCU Adam Rankin, 32, Paul Brown, 27, and Irfan Yousaf, 41, were jailed for a combined total for 12-and-a-half years.**

**Between May and August 2022, the three men contacted vulnerable and often elderly victims by telephone claiming to be from their Bank's 'Fraud Squad. They claimed their savings were at risk and needed to be safeguarded. They used manipulative tactics to convince victims to transfer money into other bank accounts and leave cheques for 'couriers' to collect.**

**They also stole the victim's personal information and used it to take out loans and credit cards in their name.**

**We are urging the public to speak to elderly relatives and explain the dangers of Courier Fraud. Please see the next page for information on how to protect yourself and others from this type of Fraud.**







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

# Courier

# Fraud

**The police or your bank will:**

- Never contact you to withdraw cash or transfer money to help secure your account.
- Never phone and ask you for your PIN or banking information.
- Never ask to send cash or other expensive goods via post for safekeeping.

**Report to Action Fraud**

If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online or by calling 0300 123 2040.

# Engagement Events

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

Barclay's Northumberland Street hosted two sessions in their branch, one interactive for their customers and one for staff.

International students received a Fraud Awareness session as Josephine Butler College Durham.

Staff at Alzheimer's Society Northumberland received a Fraud awareness input.

The team have been to North East Pensioners Association to give a basic Fraud awareness interactive session for members.

The RECCC have revisited Optimum Skills to deliver a workshop and also delivered an online training session to Durham Carers.

As students return to classes it signals the start of freshers events across the region, so far we have been to Bede Sixth Form, Redcar and Cleveland College, Prior Pursglove College and Middlesbrough College.





Phishing is a type of Social engineering. Criminals send emails with links that take you to an address that encourages you to reveal personal or financial information.

# CRIMINALS LIKE TO PHISH FOR YOUR INFO.

## HOW TO PROTECT YOURSELF:

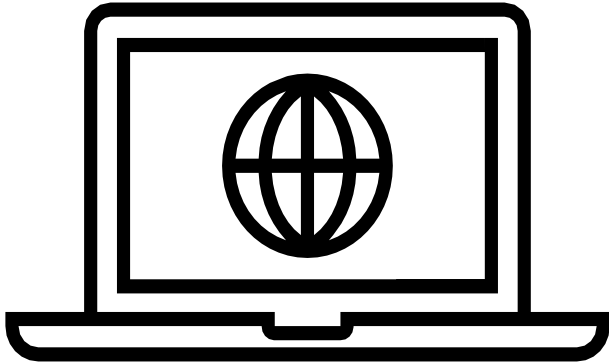
- Avoid clicking on links in emails
- If they're trying to rush or panic you into making a payment, ask yourself why?
- Don't give out any of your personal or financial information
- If you think you might have been scammed, contact your bank immediately and report it to Action Fraud.





# Horizon Scanning

## Monitoring Threats



### Online Shopping?

As the highest reported Fraud in the North East, it is important to remain vigilant when making purchases online.

There has been an increase in victims reporting they have paid a large deposit or the full amount for goods they have never received.

When using sites such as Facebook Marketplace, avoid paying without seeing the item first.



There has been an increase in scams on Facebook involving caravan holiday rentals. Victims have paid a deposit for a caravan holiday via a Facebook advert and the holiday never comes to fruition.

There have been 6 reports from victims in the North East in August.

Try to use official holiday booking sites where possible.



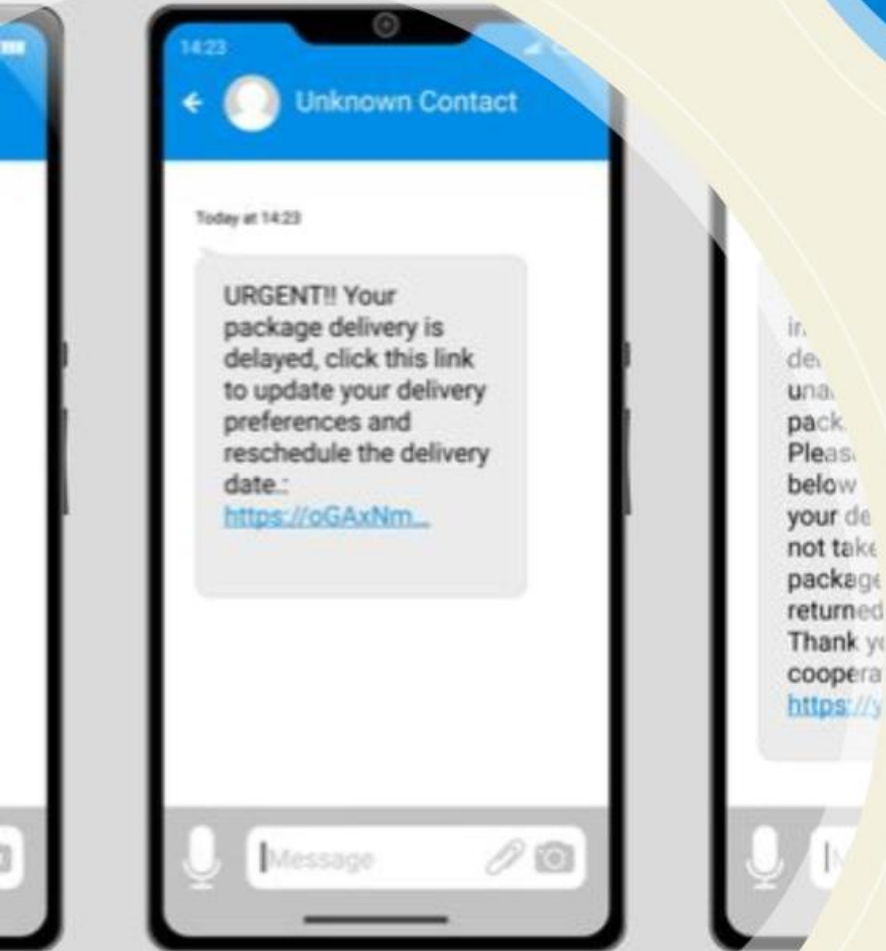


**EVRi**  
delivery made for you



## What to do if you receive a scam text

- If you do receive a suspicious text, do not click on the link provided. Instead, report the message by forwarding it to the free scam reporting service at 7726 and block the number.
- If you have clicked on a suspicious link and think you may have given your details away to a scam, you should contact your bank immediately and report to Action Fraud , 0300 123 2040



# Student guide to

# FRAUD

**Our new  
'Student guide to FRAUD'  
booklet has now been launched.**

We will be visiting Colleges and Universities across the region over the coming months to speak with students and staff.





# Student guide to

# FRAUD

## What are the top 'Fraud Types' to look out for as a student?

### 1. Investment Fraud :

Criminals will target students looking to make quick-wins with available cash through cryptocurrency or schemes with a promise of high return investment. They are targeted through social media and online where many investment schemes operate.

### 2. Employment Fraud :

Students looking for job opportunities can be targeted by Fraudulent adverts aimed at stealing personal information or money. Students might be asked for an upfront payment for a fake consultation or extra help finding a job.

### 3. Accommodation Fraud :

Criminals often target students looking for university accommodation. Fraudsters ask students to pay fees in advance without seeing a property first, and as a result they lose money as well as somewhere to live.

### 4. Online Shopping Fraud :



Often criminals will create fake websites or replicate legitimate online stores to get people to provide their personal and financial information for a purchase that isn't real. This can lead to those details being used for criminal activity.

### 5. Ticket Fraud :

Fraudsters will use opportunities, like highly in-demand events, to target students by selling fake tickets. Students looking for cheap deals for freshers' events can also be targets.







In recent months, we have seen an increase in the number of remote access tool scams. Remote Access Tool (RAT) scams will often begin a call from someone claiming to be your bank or service provider asking you to download software or an app so they can connect to your device. Regardless of the narrative, the goal of fraudsters using this tactic is to steal your money or access your financial information by tricking you into allowing them to remotely connect to your computer.

Broadband is an easy topic for scammers to try their luck on. Broadband scams tend to focus on technical faults, and prey on victims' lack of technical awareness with broadband terminology. Scammers try and gain access to your computer/smart phone to run checks on your broadband connection, they ask victims to install remote access desk sharing software which allows them to gain access to your device, often resulting in them making fraudulent banking transactions and accessing personal information.

## I think I've been scammed, what can I do?

- **Contact your bank immediately and change your online banking passwords.**
- **Enable 2FA (two-factor authentication) on all your log-ins.**
- **Run a virus check on your Computer/Smart Phone**
- **For mobile calls check your App store for Call Blocking Apps**
- **Report to Action Fraud**



**Action Fraud**  
National Fraud & Cyber Crime Reporting Centre  
0300 123 2040

#ProtectYourPension

# Have you felt pressured to make a quick decision about your pension?

Don't be rushed. Always seek independent advice first.





# Protect yourself from SIM Swap Fraud

SIM swapping is where a fraudster can gain control of your mobile phone by convincing the phone provider to transfer the service to a SIM in their possession. You may notice that your mobile is no longer connecting, and you are unable to make calls or texts.

The fraudster will have access to any incoming calls and text messages, including one-time passwords to gain access to your financial and social media accounts.

## What to do if you think your SIM card has been swapped?

- **Call your network provider immediately.** If you receive unsolicited texts or emails about your SIM being ported or a PAC request, or you unexpectedly lose phone service, you will need to notify your provider.
- **Inform your banks as soon as possible.** The fraudster may attempt to make a money transfer online or over the phone and therefore have been alerted for any attempt for unauthorised transactions. You can also record your details with Cifas, the fraud prevention service.



# What's Happening Next?



## Trying to bag yourself a bargain for the upcoming Oasis tour or another event?

Oasis have announced a reunion tour and have released tickets for various dates across the UK. With tickets in high demand it is likely that Ticket Fraud will be on the rise. Like with all other popular concerts criminals are likely to exploit this trying to sell fake tickets using social media or selling sites.

We are seeing a rise in reports for Ticket Fraud from people joining ticket sales groups for various events such as football and concerts on Facebook and having their money stolen and the group is deleted leaving victim's with no ticket.

## What can you do to protect yourself?

- **Be wary of any tickets being sold on social media or unofficial selling sites.**
- **Use well known and trusted reselling sites that offer protection.**
- **If it seems too good to be true, it probably is!**
- **Use strong passwords for any accounts you use to purchase tickets.**
- **Try to use official websites where possible, always check the website domain.**







 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](http://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](mailto: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

<b>Distribution List</b>
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.**



<b>Protective Marking</b>	<b>Official – Law Enforcement</b>
<b>Version</b>	<b>Final</b>
<b>Purpose</b>	<b>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.</b>
<b>Owner</b>	<b>NEROCU</b>
<b>Authors</b>	<b>Megan Turner – 3P Officer Claire Hardy– Economic Threat Desk Analyst Sarah McCluskey –Cyber Threat Desk Analyst</b>
<b>Reviewed By</b>	<b>T/Sgt Brian Collins</b>

## 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.